

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«СЕРТИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ»

Уровень подготовки: высшее образование – магистратура

Направление подготовки

09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

(код и наименование направления подготовки)

Направленность подготовки

Безопасность и защита информации

(наименование программы подготовки)

Квалификация (степень) выпускника

магистр

Форма обучения

очная

Уфа 2017

1. Место дисциплины в структуре образовательной программы

Дисциплина «Сертификация систем защиты информации» является обязательной дисциплиной вариативной части ОПОП по направлению подготовки 09.04.01 Информатика и вычислительная техника, направленность: Безопасность и защита информации.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.01 Информатика и вычислительная техника (уровень магистратуры)», утвержденного приказом Министерства образования и науки Российской Федерации от "30" октября 2014 г. № 1420. Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Целью освоения дисциплины является получение обучающимися систематизированных теоретических знаний об организации мероприятий по информационной безопасности на объекте информатизации, об их правовом обеспечении, об основных понятиях и видах защищаемой информации в соответствии с законодательством Российской Федерации, о системе защиты государственной тайны, конфиденциальной информации, знания по вопросам организации системы государственного лицензирования в области защиты информации, сертификации и аттестации объектов защиты информации.

Задачи:

- изучить российское и международное законодательство в области защиты информации;
- формирование умения организации государственного лицензирования в области защиты информации;
- формирование навыков организации системы сертификации и аттестации объектов защиты информации.

Входные компетенции:

На пороговом уровне ряд компетенций был сформирован за счет обучения на предыдущих уровнях высшего образования (бакалавриат, специалитет).

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1.	Способность к профессиональной эксплуатации современного оборудования и приборов	ОК-8	Базовый уровень первого этапа освоения компетенции	Вычислительные системы; Методы анализа информационных рисков; Интегрированные системы безопасности объектов информатизации
2.	Способность анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических	ОПК-6	Базовый уровень первого этапа освоения компетенции	Вычислительные системы; Теория и методология информационной безопасности;

	обзоров с обоснованными выводами и рекомендациями			Системы защищенного электронного документооборота; Защита конфиденциальной информации;
3.	Способность разрабатывать и реализовывать планы информатизации предприятий и их подразделений на основе Web- и CALS-технологий	ПК-10	Базовый уровень первого этапа освоения компетенции	Информационно-аналитические системы безопасности

*- **пороговый уровень** дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

- **базовый уровень** позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

- **повышенный уровень** предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1.	Способность к профессиональной эксплуатации современного оборудования и приборов	ОК-8	Пороговый уровень первого этапа освоения компетенции	Научно-исследовательская работа
2.	Способность анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ОПК-6	Пороговый уровень первого этапа освоения компетенции	Государственная итоговая аттестация
3.	Способность разрабатывать и реализовывать планы информатизации предприятий и их подразделений на основе Web- и CALS-технологий	ПК-10	Пороговый уровень первого этапа освоения компетенции	Технологии разработки Web-приложений; Научный семинар

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1.	Способность к профессиональной эксплуатации современного оборудования и приборов	ОК-8	<ul style="list-style-type: none"> - нормативно-правовое обеспечение сертификации технических средств защиты информации; - нормативная база сертификации программных средств защиты информации 	<ul style="list-style-type: none"> - правильно применять полученные теоретические знания на этапе проведения сертификации и контроля 	<ul style="list-style-type: none"> - организационными и техническими способами защите информации на объекте информатизации;
2.	Способность анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ОПК-6	<ul style="list-style-type: none"> - основные угрозы информационной безопасности объекта информатизации и их классификацию; - классификацию мероприятий по защите информации; - правила лицензирования и сертификации в области защиты информации; - порядок проведения аттестации объектов информационной защиты; - типовые методики испытаний объектов информатики по требованиям защиты информации; - типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации 	<ul style="list-style-type: none"> - применять стандарты и другие нормативные документы при оценке, контроле качества и сертификации; - определять рациональные способы и средства защиты информации на объекте информатизации; - организовать мероприятия по защите информации на объекте информатизации. 	<ul style="list-style-type: none"> - схемами сертификации и правилами декларирования соответствия; - признаками обязательной и добровольной сертификации.
3.	Способность разрабатывать и реализовывать планы информатизации предприятий и	ПК-10	<ul style="list-style-type: none"> - возможности применения современных Web- и CALS-технологий; 	<ul style="list-style-type: none"> - использовать эффективность современных Web- и CALS-технологий; 	<ul style="list-style-type: none"> - средствами Web- и CALS-технологиями для решения конкретных задач профессиональной обла-

их подразделений на основе Web- и CALS-технологий				сти; - средствами реализации задач профессиональной области.
---	--	--	--	---

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часов).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	2 семестр
Лекции (Л)	10
Практические занятия (ПЗ)	20
Лабораторные работы (ЛР)	8
КСР	4
Курсовая проект работа (КР)	-
Расчетно - графическая работа (РГР)	-
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	93
Подготовка и сдача экзамена	-
Подготовка и сдача зачета	9
Вид итогового контроля (зачет, экзамен)	зачет

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
		Аудиторная работа				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1.	<p>Основы законодательства РФ в области информационной безопасности и защиты информации</p> <p>Информация, как объект правового регулирования. Законодательство РФ в области информации и информационной безопасности. Международное право в сфере защиты информации. Понятие и виды информации, защищаемой законодательством РФ. Классификация информации по категориям доступа.</p>	2	2			13	17	<p>Р 6.1 №1</p> <p>Р 6.2 №2, гл.5</p>	<p>лекция классическая, лекция проблемная; при проведении практических занятий:</p> <p>- проблемное обучение</p>
2.	<p>Лицензирование деятельности в области защиты информации</p> <p>Общие положения. Организационная структура системы лицензирования. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.</p>	2	2	4		20	28	<p>Р 6.1 №4</p> <p>Р 6.1 №5</p> <p>Р 6.2 №2, гл.10</p>	
3.	<p>Сертификация средств защиты информации по требованиям безопасности информации</p> <p>Общие положения. Организационная структура системы сертификации. Порядок проведения сертификации и контроля. Требования к нормативным и методическим документам по сертификации средств защиты информации.</p>	4	8	4	4	26	46	<p>Р 6.1 №2</p> <p>Р 6.1 №3</p> <p>Р 6.2 №1</p> <p>Р 6.2 №2, гл.10</p> <p>Р 6.2 №3, гл.3,5</p>	
4.	<p>Аттестация объектов информатизации по требованиям безопасности информации</p> <p>Цель и задачи аттестационных проверок и испытаний. Условия и порядок проведения испытаний. Оформление отчетных материалов по результатам испытаний.</p>	2	8			34	44	<p>Р 6.1 №6</p> <p>Р 6.2 №2, гл.10</p> <p>Р 6.2 №3, гл.1</p>	

Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	2	Изучение порядка осуществления сертификации в области защиты информации	4
2.	3	Изучение порядка осуществления лицензирование в области защиты информации	4

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Законодательство РФ в области информационной безопасности	2
2	2	Изучение положений о государственном лицензировании деятельности в области защиты информации	2
3	3	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	2
4	3	Система сертификации средств криптографической защиты информации	2
5,6	3	Изучение положения о сертификации средств вычислительной техники и связи	4
7,8	4	Изучение положения по аттестации объектов информатизации по требованиям безопасности информации	4
9,10	4	Изучение особенностей аттестации помещений по требованиям безопасности информации	4

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации.
2. Положение от 27 октября 1995 г. N 199 О сертификации средств защиты информации по требованиям безопасности информации.
3. Типовое положение от 5 января 1996 г. N 3 Об органе по сертификации средств защиты информации по требованиям безопасности информации.
4. Постановление от 15 апреля 1995 г. N 333 О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.
5. Постановление от 3 февраля 2012 г. N 79 О лицензировании деятельности по технической защите конфиденциальной информации.
6. Положение от 25 ноября 1994 г. По аттестации объектов информатизации по требованиям безопасности информации.

6.2 Дополнительная литература

1. Положение от 25 ноября 1994 г. Об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации.

2. Семкин С.Н. Основы правового обеспечения защиты информации. Учебное пособие. – М.: Горячая линия-Телеком, 2007. – 238 с.

3. Гатчин Ю.А., Симоненко З.Г. Вопросы технологии сертификации средств защиты информации. Учебное пособие. – СПб ГУ ИТМО, 2008. – 120 с.

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки <http://library.ugatu.ac.ru/> в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Обучающимся обеспечен доступ к м электронным ресурсам и информационным справочным системам, перечисленным в таблице

Таблица

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателями
1.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	885 898 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №2255/0208-15 от 23.12.2015
2.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн. диссертаций и дипломных работ	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и Государственной публичной научно-технической библиотекой России (далее ГПНТБ России) Сублиц. договор №ProQuest/151 52/0208-16 от 02.06.2016
3.	СПС «КонсультантПлюс»	2007691 экз.	По сети УГАТУ	Договор 3К-2318/0106-15 от 30.12.2015
4.	СПС «Гарант»	6139026 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к	Договор 15\0208-16 от 15.03.2016

			ресурсу	
5.	ИПС «Технорма/Документ»	36939 экз.	Локальная установка: библиотека УГАТУ-5 мест; кафедра стандартизации и метрологии-1 место; кафедра начертательной геометрии и черчения-1 место	Договор № АОСС/914-15 № 989/0208-15 от 08.06.2015.
6.	Научная электронная библиотека eLIBRARY* http://elibrary.ru/	9919 полнотекстовых журналов	С любого компьютера, имеющего выход в Интернет, после регистрации в НЭБ на площадке библиотеки УГАТУ	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА». № 07-06/06 от 18.05.2006
7.	Патентная база данных компании Questel Orbit* http://www.orbit.com	55 млн. документов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор № Questel/151 46/0208-16 от 02.06.2016
8.	Научные полнотекстовые журналы издательства Taylor & Francis Group* http://www.tandfonline.com/	1700 наименов. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор № T&F/151 44/0208-16 от 02.06.2016
9.	Научные полнотекстовые журналы издательства Sage Publications*	790 наименов. журнал.	С любого компьютера по сети УГАТУ, имеющего	В рамках Государственного контракта от 17.02.2016 г.

	http://online.sagepub.com/		выход в Интернет	№14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/151 47/0208-16 от 02.06.2016
10.	Научные полнотекстовые журналы издательства Oxford University Press* http://www.oxfordjournals.org/	255 наимен. Журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OUP-151 43/0208-16 от 02.06.2016
11.	База данных Computers & Applied Sciences Complete компании EBSCO Publishing http://search.ebscohost.com	1000 наим. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №CASC/151 50/0208-16 от 02.06.2016
12.	Научный полнотекстовый журнал Science The American Association for the Advancement of Science http://www.sciencemag.org	1 наимен. журнала.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Science/151

				45/0208-16 от 02.06.2016
13.	<p>Научные полнотекстовые журналы Американского института физики</p> <p>http://scitation.aip.org/</p>	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	<p>В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России</p> <p>Сублиц. договор №АИР/151 48/0208-16 от 02.06.2016</p>
14.	<p>Научные полнотекстовые ресурсы Optical Society of America*</p> <p>http://www.opticsinfobase.org/</p>	9 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	<p>В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России</p> <p>Сублиц. договор №OSA/151</p> <p>49/0208-16 от 02.06.2016</p>
15.	<p>База данных GreenFile компании EBSCO*</p> <p>http://www.greeninfoonline.com</p>	5800 библиографич записей, частично с полными текстами	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	<p>Доступ предоставлен компанией EBSCO российским организациям-участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)</p>
16.	<p>Реферативная база данных INSPEC компании EBSCO Publishing</p> <p>http://search.ebscohost.com</p>	Более 11 млн. библиографич записей		<p>В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России</p> <p>Сублиц. Договор №INSPEC/151</p> <p>51/0208-16 от</p>

				02.06.2016
17.	<p>Архив научных полнотекстовых журналов зарубежных издательств* - http://archive.neicon.ru</p> <p>Annual Reviews (1936-2006)</p> <p>Cambridge University Press (1796-2011)</p> <p>цифровой архив журнала Nature (1869- 2011)</p> <p>Oxford University Press (1849–1995)</p> <p>SAGE Publications (1800-1998)</p> <p>цифровой архив журнала Science (1880 -1996)</p> <p>Taylor & Francis (1798-1997)</p> <p>Институт физики Великобритании The Institute of Physics (1874-2000)</p>	2361 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен российским организациям-участникам консорциума НЭИКОН (в т. ч. УГАТУ - без подписания лицензионного договора)

6.4. Методические указания к практическим занятиям

Практические занятия проводятся как в традиционной форме (т.е. в виде занятий, на которых решаются задачи и примеры из рассматриваемой предметной области), так и в форме семинаров, где обсуждаются и закрепляются базовые понятия, терминология, нормативные документы, постановки задач и методы их решения, рассмотренные преподавателем концептуально в лекционном курсе.

Особое внимание в ходе практических занятий уделяется получению профессиональных знаний о проблемах повышения эффективности защиты информации в области методов сертификации систем защиты информации, освоению прогрессивных технологий и технических средств, ГОСТов. Задачами изучения материалов являются: термины и определения по сертификации, сертификату соответствия, системе сертификации, стандарту, техническому регулированию, техническому регламенту, видам и типам государственных испытаний, а также усвоение магистрами основных законов и нормативной документации по сертификации средств защиты информации.

7. Образовательные технологии

При реализации дисциплины применяются классические образовательные технологии, а также интерактивные формы проведения практических занятий в виде анализа конкретных ситуаций.

При реализации ОПОП дистанционные образовательные технологии, электронное обучение, а также сетевое обучение не реализуется.

8. Методические указания по освоению дисциплины

Формы работы студентов: лекционные задания, практические занятия, написание рефератов, решение кейс-задач.

Дисциплина «Сертификация систем защиты информации» разбита на ряд отделов (модулей), представляющих собой логически завершённые части курса и являющихся теми комплексами знаний и умений, которые подлежат контролю.

Для оценки степени усвоения дисциплины рекомендуется проведение типовое задание и тестирование студентов по материалам лекций. Подборка вопросов для контрольных работ и тестирования осуществляется на основе изученного теоретического материала (см. раздел 5 настоящей рабочей программы).

В качестве организованной самостоятельной работы студентов рекомендуется использовать написания ими рефератов по выбранной тематике (см. раздел 5 рабочей программы). При написании реферата студент должен, в соответствии с требованиями к оформлению работ, сформулировать проблему, показать ее актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения данной проблемы.

9. Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации: 5-301, 5-314, 5-317.

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП с учетом направленности подготовки:

- 5-304 – компьютерный класс;
- 5-317 – компьютерный класс.

Вычислительное и телекоммуникационное оборудование и программные средства, необходимых для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

- компьютерная техника:
 - Intel Core i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb; серверы: CPU Intel Xenon E3-1240 V3 3.4GHz/4core/1+8Mb/80W/5GT ASUS P9D-C /4L LGA1150 / PCI-E SVGA 4xGbLAN SATA ATX 4DDR-III HDD 3 Tb SATA 6Gb/s Seagate Constellation CS 3,5” 7200rpm 64 Mb Crucia <CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11;
- программное обеспечение:
 - Программный комплекс – операционная система Microsoft Windows (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
 - Программный комплекс – Microsoft Office (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
 - Kaspersky Endpoint Security для бизнеса (лицензии 13C8-140128-132040, 500 users)
 - Microsoft Visual C++ 2010 Express (бесплатная версия, распространяется компанией Microsoft)
 - MPICH2, пакет реализации интерфейса MPI-2 от Аргоннской Национальной Лаборатории, США, вер. 1.4.1 (свободная версия для ОС MS Windows)
 - Intel® Threading Building Blocks (Intel® TBB) – библиотека многопоточной реализации циклов (демонстрационная версия).

10. Адаптация рабочей программы для лиц с ОВЗ

При обучении инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, обеспечивается возможность беспрепятственного доступа в учебные помещения и пункты питания и другие, необходимые для жизнедеятельности помещения, оборудованные пандусами, лифтами и иными средствами, облегчающими процесс передвижения. Для лиц с ограниченными возможностями здоровья по зрению предусматривается возможность доступа к зданию с собакой-поводырем.

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.