МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

УТВЕРЖДАЮ
Ректор
_____Н.К. Криони
«29» 12 2016 г.

Основная профессиональная образовательная программа

Уровень подготовки
высшее образование – бакалавриат

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
Безопасность автоматизированных систем

Квалификация
бакалавр

Форма обучения
очная

Год начала подготовки – 2015

Разработана в соответствии с
ФГОС ВПО Приказ № 496
Дата утверждения 28.10.2009 г.

Актуализирована в соответствии с
ФГОС ВО. Приказ №1515
Дата утверждения 01.12.2016 г.

Уфа 2016

Разработчики:
Доцент кафедры вычислительной
техники и защиты информации В.А.Дуленко

Основная профессиональная образовательная программа обсуждена на кафедре
вычислительной техники и защиты информации
26 декабря 2016., протокол № 7.

Заведующий кафедрой
д-р техн. наук, профессор_____В.И. Васильев

Представители работодателя:

Директор ЗАО «Республиканский центр защиты информации» С.Н. Зарипов

ФИО, должность, наименование организации место печати

Основная профессиональная образовательная программа обсуждена и одобрена Научно-методическим советом по УГСН 10.00.00 Информационная безопасность
28 декабря 2016 г., протокол № 4.

Председатель НМС
д-р техн. наук, профессор_____В.И. Васильев

Декан факультета ИРТ_____Н.И. Юсупова

Основная профессиональная образовательная программа одобрена и утверждена Ученым советом УГАТУ
29 декабря 2016 г., протокол № 14

Начальник ООПБС_____Г.Т. Гарипова

СОДЕРЖАНИЕ

1. Общие положения

1.1. Основная профессиональная образовательная программа (определение)

Основная профессиональная образовательная программа высшего образования (далее – ОПОП ВО, программа), реализуемая в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Уфимский государственный авиационный технический университет» (далее – университет, УГАТУ) по направлению подготовки 10.03.01 «Информационная безопасность» и направленности (профилю) «Безопасность автоматизированных систем» представляет собой систему документов, разработанную на основе Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по соответствующему направлению подготовки, с учетом требований рынка труда, профессиональных стандартов и рекомендованной примерной образовательной программы (далее – ПрООП).

ОПОП ВО регламентирует цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника и включает в себя: учебный план, календарный учебный график, рабочие программы дисциплин (модулей), программы практик, программы научно-исследовательской работы обучающихся, а также методические материалы, обеспечивающие воспитание и качество подготовки обучающихся.

1.2. Нормативные документы для разработки ОПОП ВО

Нормативную правовую базу разработки ОПОП ВО составляют:

1. Федеральный закон Российской Федерации: «Об образовании в Российской Федерации» (от 29 декабря 2012 г. N 273-ФЗ);

2. Приказ Министерства образования и науки Российской Федерации от 19 декабря 2013 г. № 1367 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;

3. Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 «Информационная безопасность», утвержденный приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1515;

4. Письмо Министерство образования и науки от 22.01.2015 № ДЛ-1/05вн «Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов»;

5. Профессиональные стандарты: Специалист по защите информации в автоматизированных системах (06.033 Утвержден Приказом Минтруда России №522н от 15.09.2016), Специалист по технической защите информации (06.034 Утвержден Приказом Минтруда России №599н от 01.11.2016), Специалист по защите информации в телекоммуникационных системах и сетях (06.030 Утвержден Приказом Минтруда России №608н от 03.11.2016), Специалист по безопасности компьютерных систем и сетей (06.032 Утвержден Приказом Минтруда России №598н от 01.11.2016), Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности (06.031 Утвержден Приказом Минтруда России №611н от 09.11.2016);

6. Нормативно-методические документы Министерства образования и науки Российской Федерации;

7. Примерная основная образовательная программа, утвержденная УМО по направлению «Информационная безопасность» (носит рекомендательный характер);

8. Устав УГАТУ и другие локальные нормативные акты университета.

1.3. Общая характеристика ОПОП ВО

1.3.1. Цели ОПОП ВО

ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Безопасность автоматизированных систем» имеет своей целью развитие у обучающихся личностных качеств, а также формирование общекультурных-универсальных (общенаучных, социально-личностных, инструментальных) и профессиональных компетенций в соответствии с требованиями ФГОС ВПО по данному направлению подготовки.

В области обучения целью ООП ВО по направлению подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Безопасность автоматизированных систем» является формирование универсальных (общенаучных, социально-личностных, общекультурных и инструментальных) и профессиональных (общепрофессиональных и профильно-специализированных) компетенций, позволяющих выпускнику успешно работать в избранной сфере деятельности, быть социальной мобильным и устойчивым на рынке труда.

В области воспитания личности целью ООП ВО по направлению подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Безопасность автоматизированных систем» является укрепление нравственности, развитие общекультурных потребностей, творческих способностей, социальной адаптации, коммуникативности, толерантности, настойчивости в достижении цели, формирование выносливости и физической культуры.

1.3.2. Срок освоения

Срок освоения ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность» (очная форма обучения) – 4 года.

1.3.3. Трудоемкость

Трудоемкость освоения обучающимся данной ОПОП ВО за весь период обучения в соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» составляет 240 зачетных единиц и включает все виды аудиторной и самостоятельной работы студента, практики и время, отводимое на контроль качества освоения обучающимся ОПОП ВО. Трудоемкость остается неизменной при любой форме обучения, применяемых образовательных технологиях, использования сетевой формы, реализации программы по индивидуальному учебному плану, в том числе при ускоренном обучении.

1.3.4. Образовательные технологии

При реализации образовательной программы образовательные технологии, в том числе дистанционные образовательные технологии и электронное обучение, не используются. Образовательная программа не реализуется с использованием сетевых форм.

Методы и средства обучения и образовательные технологии реализации образовательной программы определяются исходя из необходимости достижения обучающимися планируемых результатов освоения образовательной программы, а также с учетом индивидуальных возможностей обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья.

1.3.5. Тип программы

Программа академического бакалавриата.

1.4. Язык реализации ОПОП ВО

Образовательная деятельность осуществляется на государственном языке Российской Федерации.

1.5. Требования к уровню подготовки, необходимому для освоения ОПОП ВО

Для освоения ОПОП ВО подготовки бакалавра абитуриент должен иметь документ государственного образца о среднем (полном) общем образовании или среднем профессиональном образовании.

2. Характеристика профессиональной деятельности

2.1. Область профессиональной деятельности выпускника

В соответствии с ФГОС ВО по данному направлению подготовки область профессиональной деятельности бакалавра с профилем подготовки «Безопасность автоматизированных систем» включает: сферы науки, техники и технологии, охватывающие совокупность про-

блем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

В число организаций и учреждений, в которых может осуществлять профессиональную деятельность выпускник по данному направлению и профилю подготовки ООП ВО входят:

– академические, ведомственные и частные научно-исследовательские и производственные организации, связанные с решением проблем, связанных с обеспечением безопасности компьютерных систем;

– учреждения системы высшего и среднего профессионального образования, среднего общего образования.

2.2. Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускника в соответствии с ФГОС ВО по данному направлению подготовки являются:

- объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;

- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

- процессы управления информационной безопасностью защищаемых объектов.

2.3. Виды профессиональной деятельности выпускника

В соответствии с ФГОС ВО по данному направлению подготовки выпускник с профилем подготовки «Безопасность автоматизированных систем» подготовлен к следующим видам профессиональной деятельности:

- эксплуатационная;

- проектно-технологическая;

- экспериментально-исследовательская;

- организационно-управленческая.

В соответствии с запросами рынка труда выпускник с профилем подготовки «Безопасность автоматизированных систем» подготовлен к:

- применению современных информационных технологий в профессиональной деятельности;

- обоснованному применению технологических решений при проектировании систем защиты информации;

- осуществлению контроля и диагностики состояния компонентов системы обеспечения информационной безопасности;

- использованию основных законов естественнонаучных дисциплин в профессиональной деятельности, применению методов математического анализа и моделирования, теоретического и экспериментального исследования;

- выполнению профессиональной деятельности.

В соответствии с профессиональными стандартами выпускник готов к видам деятельности:

- обеспечение безопасности информации в автоматизированных системах;

- техническая защита информации;

- защита информации в компьютерных системах и сетях.

2.4. Задачи профессиональной деятельности выпускника

Выпускник по направлению подготовки 10.03.01 «Информационная безопасность» (по профилю «Безопасность автоматизированных систем») должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности и профилем ОПОП ВО:

а) эксплуатационная деятельность:

– установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

– администрирование подсистем информационной безопасности объекта;

– участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

б) проектно-технологическая деятельность:

– сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

– проведение проектных расчетов элементов систем обеспечения информационной безопасности;

– участие в разработке технологической и эксплуатационной документации;

– проведение предварительного технико-экономического обоснования проектных расчетов;

в) экспериментально-исследовательская деятельность:

– сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

– проведение экспериментов по заданной методике, обработка и анализ их результатов;

– проведение вычислительных экспериментов с использованием стандартных программных средств;

г) организационно-управленческая деятельность:

– осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

– организация работы малых коллективов исполнителей;

– участие в совершенствовании системы управления информационной безопасностью;

– изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

– контроль эффективности реализации политики информационной безопасности объекта защиты.

3. Требования к результатам освоения ОПОП ВО

3.1. Компетенции выпускника, формируемые в результате освоения программы

Результаты освоения ОПОП ВО определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

В результате освоения данной ОПОП ВО выпускник должен обладать следующими компетенциями:

Общекультурные компетенции:

1. Способность использовать основы философских знаний для формирования мировоззренческой позиции (**ОК-1**).

2. Способность использовать основы экономических знаний в различных сферах деятельности (**ОК-2**).

3. Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (**ОК-3**).

4. Способность использовать основы правовых знаний в различных сферах деятельности (**ОК-4**).

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

6. Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (**ОК-6**).

7. Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности **(ОК-7**).

8. Способность к самоорганизации и самообразованию (**ОК-8**).

9. Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (**ОК-9**).

Общепрофессиональные компетенции:

1. Способность анализировать физические явления и процессы для решения профессиональных задач (**ОПК-1**).

2. Способность применять соответствующий математический аппарат для решения профессиональных задач (**ОПК-2**).

3. Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (**ОПК-3**).

4. Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (**ОПК-4**).

5. Способность использовать нормативные правовые акты в профессиональной деятельности (**ОПК-5**).

6. Способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (**ОПК-6**).

7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (**ОПК-7**).

Профессиональные компетенции:

Эксплуатационная деятельность:

1. Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (**ПК-1**).

2. Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (**ПК-2**).

3. Способность администрировать подсистемы информационной безопасности объекта защиты (**ПК-3**).

4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (**ПК-4**).

5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (**ПК-5**).

6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (**ПК-6**).

Проектно-технологическая деятельность:

7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (**ПК-7**).

8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (**ПК-8**).

Экспериментально-исследовательская деятельность:

9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

(**ПК-9**).

10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (**ПК-10**).

11. Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (**ПК-11**).

12. Способность принимать участие в проведении экспериментальных исследований системы защиты информации (**ПК-12**).

Организационно-управленческая деятельность:

13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (**ПК-13**).

14. Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности (**ПК-14**).

15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (**ПК-15**).

Профессионально-специализированные компетенции (дополнительные компетенции):

1. Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (**ПСК-1**).

2. Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей **(ПСК-2**).

3. Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации (**ПСК-3**).

4. Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности (**ПСК-4**).

Требования к результатам обучения (знания, умения, владения) представлены в рабочих программах по дисциплинам (модулям) и программах практик и программе государственной итоговой аттестации.

3.2. Матрица соответствия дисциплин и компетенций, формируемых в результате освоения ОПОП ВО

Соответствие дисциплин и компетенций, формируемых в результате освоения ОПОП, указано в виде матрицы, представленной в приложении 1.

3.3. Матрица соответствия компетенций, предусмотренных ОПОП, разработанной в соответствии с ФГОС ВПО, компетенциям ФГОС ВО

Компетенции ФГОС ВПО		Компетенции ФГОС ВО	
Код	Наименование	Код	Наименование
ОК-4	Способность понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач	ОК-1	Способность использовать основы философских знаний для формирования мировоззренческой позиции

ОК-4	Способность понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач	ОК-2	Способность использовать основы экономических знаний в различных сферах деятельности
ОК-4	Способность понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач	ОК-3	Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма
ОК-3	Способность уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия		
ОК-1	Способность осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма	ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности
ОК-1	Способность осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма	ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
ОК-6	Способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность		
ОК-7	Способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовность и способность к активной состязательной деятельности в условиях информационного противоборства		
ОК-2	Способность осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм	ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия
ОК-5	Способность к кооперации с коллегами, работе в коллективе		
ОК-6	Способность находить организационно-управленческие решения в нестандартных ситуациях и готовно-		

	стью нести за них ответственность		
ОК-9	Способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии	ОК-7	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности
ОК-10	Способность к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного		
ОК-11	Способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства	ОК-8	Способность к самоорганизации и самообразованию
ОК-12	Способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков		
ОК-8	Способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления		
ОК-13	Способность к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	ОК-9	Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности
ПК-20	Способность применять методы анализа изучаемых явлений, процессов и проектных решений	ОПК-1	Способность анализировать физические явления и процессы для решения профессиональных задач
ПК-22	Способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов		
ПК-1	Способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности	ОПК-2	Способность применять соответствующий математический аппарат для решения профессиональных задач
ПК-11	Способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	ОПК-3	Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач
ПК-20	Способность применять методы анализа изучаемых явлений, процессов и проектных решений		
ПК-2	Способность понимать сущность и значение информации в развитии современного общества, применять	ОПК-4	Способность понимать значение информации в развитии современного общества, применять инфор-

	достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах		мационные технологии для поиска и обработки информации
ПК-3	Способность использовать нормативные правовые документы в своей профессиональной деятельности	ОПК-5	Способность использовать нормативные правовые акты в профессиональной деятельности
ПК-7	Способность использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий	ОПК-6	Способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности
ПК-32	Способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации		
ПК-8	Способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-11	Способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-15	Способность применять программные средства системного, прикладного и специального назначения	ПК-2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-16	Способность использовать инструментальные средства и системы программирования для решения профессиональных задач		
ПК-17	Способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности		
ПК-10	Способность администрировать подсистемы информационной безопасности объекта	ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты
ПК-29	Способность участвовать в работах по реализации политики информационной безопасности	ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-30	Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности		
ПК-6	Способность организовать проведение и сопровождать аттестацию объекта на соответствие требовани-	ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации

	ям государственных или корпоративных нормативных документов		по требованиям безопасности информации
ПК-27	Способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-13	Способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-18	Способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности		
ПК-20	Способность применять методы анализа изучаемых явлений, процессов и проектных решений		
ПК-14	Способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	ПК-8	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-19	Способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	ПК-9	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
ПК-24	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности		
ПК-28	Способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации		
ПК-21	Способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов	ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК-22	Способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов	ПК-11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
ПК-23	Способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	ПК-12	Способность принимать участие в проведении экспериментальных исследований системы защиты информации

ПК-4	Способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-5	Способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации		
ПК-9	Способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия		
ПК 12	Способность участвовать в разработке подсистемы управления информационной безопасностью		
ПК-25	Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью		
ПК-26	Способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью		
ПК-31	Способность организовать работу малого коллектива исполнителей с учетом требований защиты информации	ПК-14	Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности
ПК-33	Способность организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	ПК-15	Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПСК-1	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ПСК-1	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПСК-2	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	ПСК-2	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей

ПСК-3	Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	ПСК-3	Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации
ПСК-4	Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности	ПСК-4	Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности

4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ОПОП ВО

Содержание и организация образовательного процесса при реализации данной ОПОП ВО регламентируется учебным планом с учетом его направленности (профиля), календарным учебным графиком, рабочими программами дисциплин (модулей), программами практик, а также методическими материалами, обеспечивающими реализацию образовательных технологий.

4.1. Календарный учебный график

Последовательность реализации ОПОП ВО по годам (включая теоретическое обучение, практики, промежуточные и итоговую аттестации, каникулы) прилагается.

4.2. Учебный план

Учебный план прилагается.

4.3. Рабочие программы дисциплин (модулей)

Рабочие программы дисциплин (модулей) прилагаются.

4.4. Программы практик и научно-исследовательской работы

4.4.1. Программа практик

При реализации данной ОПОП ВО предусматриваются следующие виды практик:

1. Учебная практика. Тип – практика по получению первичных профессиональных умений и навыков. Способ проведения – стационарная, выездная.

2. Производственная.

2.1. Тип – эксплуатационная практика. Способ проведения – стационарная, выездная.

2.2. Тип – преддипломная практика для выполнения выпускной квалификационной работы. Способ проведения – стационарная, выездная.

2.3. Тип – научно-исследовательская работа. Способ проведения – стационарная, выездная.

Предприятия, учреждения и организации, с которыми вуз имеет заключенные договоры:

- ООО «УралСофтПроект», г. Уфа;
- ОАО НПП «Полигон», г. Уфа;
- ЗАО Центр системных исследований «Интегро», г. Уфа;
- ОАО «Международный аэропорт «Уфа»;
- ОАО «Агрегат», г. Сим Челябинской обл.;
- ООО НПФ «Пакер», г. Октябрьский;
- ОАО «БЭТО», г. Уфа;
- ОАО Нефтеавтоматика;
- Федеральное государственное унитарное предприятие «Приборостроительный завод» (ГК РОСАТОМ), г. Трехгорный Челяб. обл.;
- ОАО «Башнефтегеофизика», ООО НПЦ «Геостра», г. Уфа;
- ОАО «Уфимское научно-производственное предприятие «Молния»;
- ОАО «Башнефтегеофизика», ООО НПЦ «Геостра», г. Уфа;
- ПАО Башинформсвязь, г. Уфа;
- ООО «Компьютерная компания ФЕРМО»;
- ОАО УАП Гидравлика;

- ОАО Сбербанк России;
- УГАТУ, отдел информационных технологий в образовании;
- ОАО «БАНК УРАЛСИБ»;
- Институт математики с ВЦ УНЦ РАН;
- ОАО «Уфимское моторостроительное производственное объединение»;
- ОАО СОГАЗ;
- ФГБОУ ВО «Уфимский государственный авиационный технический университет», кафедра «Вычислительная техника и защита информации» (профессорско-преподавательский состав кафедры составляет 31 штатную единицу, доля преподавателей, имеющих ученую степень доктора или кандидата наук, в общем числе преподавателей кафедры составляет 76%, доля преподавателей, имеющих основное место работы в данном вузе, в общем числе преподавателей составляет 75%, на кафедре осуществляется научно-исследовательская работа по направлениям:
- Методы, алгоритмы и технические средства интеллектуальных систем управления сложными техническими объектами. Научный руководитель – д-р техн. наук, профессор Васильев В.И.
- Управление в социальных и экономических системах. Научный руководитель – д-р техн. наук, профессор Гузаиров М.Б.
- Интеллектуальные многоуровневые системы управления информационной безопасностью. Научный руководитель – д-р техн. наук, профессор Васильев В.И.
- Отказоустойчивые информационно-управляющие системы для автоматизации сложных технических систем. Научный руководитель – д-р техн. наук, профессор Фрид А.И.
- Методы обработки спектральной и оптической информации. Научный руководитель – канд. физ.-мат. наук, доцент Гараев Р.А.

Аудиторный фонд кафедры включает 3 дисплейных класса, 2 мультимедийные аудитории и 11 лабораторий).

Программа практик разрабатывается в соответствии Положением о практике студентов. Программа практик прилагается.

4.4.2. Программа научно-исследовательской работы

Программа научно-исследовательской работы прилагается.

5. Фактическое ресурсное обеспечение

Ресурсное обеспечение данной ОПОП ВО формируется на основе требований к условиям реализации ОПОП ВО, определяемых ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность».

5.1. Кадровое обеспечение

Уровень кадрового потенциала характеризуется выполнением требований к наличию и квалификации научно-педагогических кадров в соответствии с действующей нормативно-правовой базой.

Квалификация руководящих и научно-педагогических работников организации соответствует квалификационным характеристикам, установленным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, разделе «Квалификационные характеристики должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования», утвержденном приказом Министерства здравоохранения и социального развития Российской Федерации от 11 января 2011 г. №1н и профессиональным стандартам.

Доля научно-педагогических работников, имеющих образование, соответствующее профилю преподаваемой дисциплины (модуля), в общем числе научно-педагогических работников, реализующих образовательную программу составляет 80% (критериальное значение, предусмотренное ФГОС ВО – не менее 70%).

Доля преподавателей, имеющих ученую степень доктора или кандидата наук, в общем числе преподавателей, обеспечивающих образовательный процесс по ОПОП ВО составляет 88% (критериальное значение, предусмотренное ФГОС ВО – не менее 50%).

Доля преподавателей, имеющих основное место работы в данном вузе, в общем числе преподавателей, обеспечивающих образовательный процесс по ОПОП ВО составляет 94%

(критериальное значение, предусмотренное ФГОС ВО – не менее 50%).

Доля работников из числа руководителей и работников организаций, деятельность которых связана с направленностью реализуемой программы бакалавриата в общем числе работников, реализующих программу бакалавриата составляет 8% (критериальное значение, предусмотренное ФГОС ВО – не менее 5%).

Преподаватели систематически занимаются научной и/или научно-методической деятельностью по профилю преподаваемых дисциплин (модулей).

5.2. Учебно-методическое и информационное обеспечение

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к следующим электронно-библиотечным системам:

- ЭБС «Лань» http://e.lanbook.com;
- ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru;
- Консорциум аэрокосмических вузов России http://elsau.ru;
- Электронная коллекция образовательных ресурсов УГАТУ http://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus;
- ЭБС BOOK.ru - электронно-библиотечная система http://www.book.ru.

ЭБС содержат все издания основной литературы, перечисленные в рабочих программах дисциплин (модулей), практик, НИР и сформированы на основании прямых договорных отношений с правообладателями.

Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивают возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет, как на территории университета, так и вне ее.

Библиотечный фонд укомплектован печатными изданиями из расчета не менее 50 экземпляров каждого из изданий основной литературы, перечисленной в рабочих программах дисциплин (модулей), практик и не менее 25 экземпляров дополнительной литературы на 100 обучающихся. Общий фонд библиотеки УГАТУ 1336379 изданий (из них печатные документы 902494 (из них периодические издания 68756)), электронные издания 430448, аудиовизуальные материалы 3437.

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

№	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 Гос. 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»	6139223 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор 15\0208-16 от 15.03.2016

5.	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
6.	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 Гос. контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор № Questel/15146/0208-16 от 02.06.2016
7.	Научные полнотекстовые журналы издательства Taylor& Francis Group* http://www.tandfonline.com/	1700 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Гос. 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
8.	Научные полнотекстовые журналы издательства Sage Publications* http://online.sagepub.com/	790 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Гос. контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/151 47/0208-16 от 02.06.2016
9.	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 Гос. 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
10.	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 Гос. 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
11.	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 Гос. 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
12.	Научные полнотекстовые журналы Американского института физики http://scitation.aip.org/	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Гос. контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №AIP/151 48/0208-16 от 02.06.2016

13.	Научные полнотекстовые ресурсы Optical Society of America* http://www.opticsinfobase.org/	19 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Гос. контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OSA/151 49/0208-16 от 02.06.2016
14.	База данных GreenFile компании EBSCO* http://www.greeninfoonline.com	5800 библиографич записей, частично с полными текстами	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен компанией EBSCO российским организациям-участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)
15.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиографич. записей		В рамках Гос. контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор №INSPEC/151 51/0208-16 от 02.06.2016
16.	Архив научных полнотекстовых журналов зарубежных издательств*- http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849–1995) SAGE Publications (1800-1998) цифровой архив журнала Science (1880 -1996) Taylor & Francis (1798-1997) Институт физики Великобритании The Institute of Physics (1874-2000)	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)

*Обучающимся инвалидам и лицам с ограниченными возможностями здоровья предоставляются печатные и электронные образовательные ресурсы в формах, адаптированных к ограничениям их здоровья.

При инклюзивном обучении лиц с ОВЗ предоставляется возможность использовать следующие материально-технические средства:

- для студентов с ОВЗ по зрению предусматривается применение средств преобразования визуальной информации в аудио и тактильные сигналы, таких как, брайлевская компьютерная техника, электронные лупы, видеоувеличители, программы невизуального доступа к информации, программы-синтезаторы речи;

- для студентов с ОВЗ по слуху предусматривается применение сурдотехнических средств, таких как, системы беспроводной передачи звука, техники для усиления звука, видеотехника, мультимедийная техника и другие средства передачи информации в доступных формах;

- для студентов с нарушениями опорно-двигательной функции предусматривается применение специальной компьютерной техники с соответствующим программным обеспечением, в том числе, специальные возможности операционных систем, таких, как экранная клавиатура и альтернативные устройства ввода информации.

При реализации программ с использованием дистанционных образовательных техно-

логий используется действующая в университете электронно-образовательная среда. Разработка учебных материалов осуществляется с учетом возможностей предоставления контента в различных формах – визуально, аудиально. Разрабатываемый нетекстовый контент преобразуется в альтернативные формы, удобные для различных категорий пользователей без потери данных и структуры. Предусматривается возможность масштабирования текста, применения экранной клавиатуры. В образовательном процессе активно используются различные формы организации on-line и off-line занятий, в том числе, вебинары, виртуальные лекции, обсуждение вопросов освоения дисциплины в рамках форумов, выполнение совместных работ с применением технологий проектной деятельности с возможностью включения всех участников образовательного процесса в активную работу.

5.3. Материально-техническое обеспечение

Материально-техническая база включает в себя:

1) Спортивный комплекс, включающий спортивные залы, тренажерные залы, спортивные площадки под открытым небом;

2) Кабинеты-аудитории, оснащенные обычной доской, интерактивной доской, партами, мультимедийным оборудованием;

3) Блок поточных аудиторий, оснащенных проекционным оборудованием;

4) Учебные специализированные кабинеты:

– компьютерные классы с компьютерами, включенными в локальную сеть УГАТУ с возможностью выхода в Internet;

– телестудия с теле- и аудиоаппаратурой;

– лаборатории для проведения лабораторных работ с соответствующим оборудованием (физики, электротехники и т.д.);

– лаборатория микропроцессорных средств и систем;

– лаборатория систем и сетей передачи данных;

– лаборатория интегрированных информационно-управляющих систем;

– лаборатория оптоэлектронных устройств ввода информации;

– лаборатория электроники и систем связи;

– лаборатория схемотехники ЭВМ;

– лаборатория защиты информации;

– лаборатория программно-аппаратных средств защиты информации;

– лаборатория технических средств защиты информации.

5) Библиотеку с книжным и электронным фондом, читальными залами.

6) Общеуниверситетский сайт и сайты факультетов и кафедр.

7) Вычислительное и телекоммуникационное оборудование и программные средства, необходимые для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности: серверы: CPU IntelXenon 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 SeagataConstellation CS 3,5” 7200rpm 64 MbCrucia<CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11; компьютерная техника: IntelCore i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb.

8) Лицензионное 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);
- Программный комплекс –Microsoft Projec tProfessional (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования);
- Программный комплекс – операционная система Microsoft VisioPro (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования);
- Программный комплекс – серверная операционная система Windows Server Datacenter (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования);

− Kaspersky Endpoint Security для бизнеса (№ лицензии 13C8-140128-132040, 500 users);

− Dr.Web® Desktop Security Suite (КЗ) +ЦУ (AH99-VCUN-TPPJ-6k3L, 415 рабочих станций);

− ESET Smart Security Business (EAV-8424791, 500 пользователей);

− Пакет прикладных программ для выполнения инженерных и научных расчетов, ориентированных на работу с массивами данных - MATLAB, Simulink (Гос.контракт на основании протокола единой комиссии по размещению заказов УГАТУ №ЭА 01-271/11 от 08.12.2011 и др., до 50 мест); MATLAB DistributedComputingServer (Гос.контракт на основании протокола единой комиссии по размещению заказов УГАТУ №ЭА 01-271/11 от 08.12.2011 и др., 256 мест.

При использовании электронных изданий университет обеспечивает каждого обучающегося во время самостоятельной подготовки рабочим местом в компьютерном классе с выходом в Интернет.

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 предоставляется возможность доступа к зданию с собакой-поводырем.

6. Характеристики среды вуза, обеспечивающие развитие общекультурных и социально-личностных компетенций выпускников

В УГАТУ создано социокультурное пространство, призванное способствовать удовлетворению интересов и потребностей студентов, формировать у них социально-ценностные качества и убеждения, обеспечивающие гармоничное, разностороннее развитие личности будущего конкурентоспособного специалиста.

Цель воспитательного процесса – создание условий для дальнейшего всестороннего развития гармоничной личности, способной к саморазвитию и реализации полученных профессиональных и социальных качеств, для достижения успеха в жизни.

Намеченная цель требует решения следующих задач:

- повышение воспитательного потенциала учебных дисциплин;
- развитие проектной деятельности в области воспитательной работы и вовлечение в нее обучающихся;
- развитие корпоративной культуры в университете;
- развитие и поддержка органов студенческого самоуправления и студенческих инициатив.

Документационное обеспечение воспитательной работы со студентами УГАТУ:

1. Законодательные акты об образовании.
2. Устав УГАТУ.
3. Правила внутреннего распорядка.
4. Положение о стипендиальном обеспечении и других формах материальной поддержки студентов, аспирантов и докторантов УГАТУ. Положение о воспитательной работе в УГАТУ.
5. Положение об отделе по воспитательной работе в УГАТУ.
6. Положение о совете по воспитательной работе.
   - Положение о кураторе студенческой академической группы.
   - Этический кодекс студента УГАТУ.

Основные направления воспитательной работы в университете:

1. Гражданско-патриотическое и интернациональное воспитание студентов.
2. Нравственно-эстетическое воспитание, воспитание экологической культуры.
3. Профессиональное воспитание.
4. Организация научно-исследовательской работы студентов.
5. Формирование культуры здорового образа жизни.

Организация целостного учебно-воспитательного процесса, взаимодействие субъек-

тов социокультурной среды УГАТУ.

Воспитательная деятельность в УГАТУ осуществляется через учебный процесс, практики, научно-исследовательскую деятельность студентов и систему внеучебной работы по различным направлениям.

В вузе выстроена многоуровневая система воспитательной работы.

Курирует воспитательную деятельность в вузе проректор по учебной работе, на уровне факультетов – заместители деканов по воспитательной работе.

Координацию всех задействованных в воспитательном процессе структурных подразделений осуществляет отдел по воспитательной работе.

Важная роль в воспитательном процессе отводится кураторам студенческих академических групп в задачи которых входит оказание помощи студентам младших курсов в период адаптации в университете, в решении жилищно-бытовых проблем, а также контроль текущей успеваемости, посещения занятий. В университете регулярно осуществляется проверка эффективности деятельности кураторов студенческих академических групп 1 курса, проводятся семинары для кураторов. В помощь им разработана «Рабочая тетрадь куратора».

УГАТУ – единственный вуз в РБ, имеющий военную кафедру и учебный военный центр. Университет располагает летно-испытательным комплексом «Аэропорт» УГАТУ, в котором находятся лучшие образцы современной авиационной техники. УВЦ и ВК совместно с Советом ветеранов и ДОСААФ УГАТУ играют важную роль в патриотическом воспитании студентов.

Социальная инфраструктура УГАТУ и социальная поддержка студентов. Социальная структура университета включает в себя необходимые для жизнедеятельности студентов объекты.

Студгородок УГАТУ состоит из 9 общежитий. Общее количество мест – 3324. Студенты проживают в 2-3 местных комнатах. Обеспеченность местами в общежитии студентов, обучающихся за счет бюджета – 100 %. В каждом общежитии есть спортивные комнаты, кухни самообслуживания, помещения для занятий и для организации мероприятий, душевые. Оснащение общежитий отвечает всем санитарно-гигиеническим нормам.

В комплексе студгородка имеются

- санаторий-профилакторий – один из лучших вузовских лечебно-оздоровительных центров республики. Общее количество мест – 150; ежегодно принимает 1500 студентов и 150 преподавателей и сотрудников;
- здравпункт и столовая;
- продовольственных магазина, ателье проката, отделение Сберегательного банка России, 2 мастерских по ремонту обуви, прачечная, 2 парикмахерских салона, фотосалон. На территории студгородка работает филиал кафедры физического воспитания. В распоряжении студентов – зал тяжелой атлетики, зал акробатики, стрелковый тир, лыжная база.

В каждом общежитии работает локальная вычислительная сеть с открытым доступом локальной сети УГАТУ и услугам сети Интернет. В настоящее время подключено более 1800 личных компьютеров студентов и аспирантов.

В вузгородке имеется:

- библиотека, в которой имеется более миллиона экземпляров отечественной и зарубежной литературы (ежегодное пополнение фондов – около 20 тысяч экземпляров);
- столовая (общее количество мест – 600), буфеты во 2, 5, 6, 7, 8 корпусах;
- здравпункт (медицинское обслуживание студентов осуществляет также межвузовская студенческая поликлиника № 49);
- спортивные сооружения;
- конференц-залы, актовые залы, музеи, кинозал.

Внеучебные мероприятия проводятся в Доме студента площадью 7302 кв.м. со зрительным залом на 800 мест и с помещениями для занятий кружков и творческих коллективов.

Университет имеет спортивные оздоровительные лагеря «Агидель» (на берегу реки Белой) и «Авиатор» (на берегу Павловского водохранилища), рассчитанные на отдых 1000 студентов и 250 преподавателей и сотрудников за сезон.

В течение учебного года студенты отдыхают в санатории-профилактории, а в период летних каникул им предоставляется возможность побывать в спортивно-оздоровительных лагерях УГАТУ, а также на побережье Чёрного моря.

Социальная поддержка студентов включает также:

- оказание материальной помощи обучающимся;
- назначение социальной стипендии;
- контроль за соблюдением социальных гарантий;
- содействие социальной адаптации первокурсников к условиям учебы в университете и студентов, проживающих в общежитии.

Одна из форм социальной поддержки студентов университета – присуждение именных стипендий:

- Президента РФ;
- Правительства РФ;
- Главы Республики Башкортостан;
- Правительства РБ;
- Ученого совета;
- ОАО «Башкирэнерго»;
- им. В.П. Лесунова;
- им. Р.Р. Мавлютова и др.

Научно-исследовательская работа студентов Основной источник формирования компетенций – научные исследования студентов. В целях активизации научно-исследовательской деятельности и повышения эффективности студенческих научных разработок в университете практикуются различные формы работы.

Фестиваль науки, в котором приняли участие 4000 школьников и студентов. В программу мероприятия входят научно-популярные лекции, проведение научных опытов, посещение научных лабораторий вуза, знакомство с новыми научными достижениями, представленными в популярной форме.

В рамках фестиваля проходит Неделя науки, включающая в себя:

– внутривузовские туры олимпиад по общенаучным (общеинженерным) дисциплинам;

– внутривузовские туры конкурсов на лучший реферат, лучшую научную работу студентов, лучший курсовой проект; – студенческая научно-теоретическая конференция, где ежегодно работает более 80 секций.

Всероссийская молодёжная научная конференция «Мавлютовские чтения», в которой принимают участие более 700 студентов и аспирантов УГАТУ, представляющих свои исследования по 40 научным направлениям. По результатам работы конференции издаются сборники тезисов докладов.

УГАТУ – базовый вуз по проведению туров Всероссийской студенческой олимпиады. Университет регулярно проводит туры пяти региональных и трёх Всероссийских туров олимпиад и конкурсов выпускных квалификационных работ по различным направлениям и специальностям.

В вузе издается электронный и печатный журнал «Молодёжный вестник УГАТУ», который также даёт возможность публиковать результаты своих научных исследований всем студентам и аспирантам, занимающимся научно-исследовательской работой.

В УГАТУ создано Студенческое научное общество (СНО), в рамках которого в настоящее время действуют 7 студенческих научных кружков, дискуссионный клуб, студенческое конструкторское бюро.

С 2012 года в университете проходит конкурс научно-исследовательских работ студентов, участники которого представили результаты более ста научных исследований в двенадцати научных направлениях. По итогам конкурса победители и призёры получили материальное вознаграждение.

С 2009 года студенты и аспиранты университета регулярно принимают участие в конкурсе УМНИК и выигрывают гранты для реализации своих научных проектов.

Внеучебная деятельность студентов. Внеучебная работа, организуемая администрацией, профессорско-преподавательским составом, различными подразделениями и обществен-

ными организациями УГАТУ направлена на вовлечение студентов в деятельность, способствующую формированию прогрессивного стиля мышления и служащую школой для дальнейшей карьеры.

Студенческое самоуправление в университете представлено профкомом студентов, советом обучающихся, студенческими советами общежитий и другими молодежными объединениями, осуществляющими социально-воспитательную работу. Так, в вузе успешно работают волонтеры, студенты проводят благотворительные акции.

В УГАТУ проводится множество гражданско-патриотических, культурно-массовых, спортивных, развлекательных мероприятий. При активной поддержке ректората многие из них организует профком студентов и аспирантов, который по праву считается в нашем вузе центром студенческой жизни. Организаторами выступают также совет обучающихся, студенческий и спортивный клубы, деканаты. В университете стали традиционными конкурсы художественного творчества «Взлёт» и «Студенческая весна», посвящение первокурсников в студенты и бенефис выпускников, шоу «Мистер УГАТУ» и «Мисс УГАТУ», КВН, а также особенно любимые студентами конкурсы «А ну-ка, парни!» и «А ну-ка, девушки!». Среди последних воплощенных задумок активистов можно отметить День этикета, танцевальный баттл, большой флешмоб на площади УГАТУ, фотоконкурсы и Фестиваль Безбашенного Рока.

Традиционные мероприятия формируют корпоративную культуру университета, единое социокультурное пространство. УГАТУ имеет свою эмблему, знамя, гимн, а также флаги и эмблемы факультетов.

В рамках студклуба УГАТУ работают студия эстрадного танца «Л'Этуаль», театр танца «Вираж», танцевальный коллектив «Флэшка», вокальная студия SOUL, Мастерская театральных миниатюр имени МенЯ и другие студенческие коллективы.

Наш университет – это надежная площадка для реализации смелых проектов, развития студентов как будущих грамотных руководителей. Этому способствует активная работа студенческого научного общества, самые успешные члены которого ежегодно выезжают на молодёжный форум «Селигер». На базе СОЛ «Авиатор» организована ежегодная летняя школа студенческого актива. Экологический отряд вовлекает студентов в работу по благоустройству города. Профкомом регулярно проводятся конкурсы «Лучшая группа УГАТУ» и «Студенческий лидер».

Ежегодно в стенах вуза проводятся День борьбы с курением и День борьбы со СПИДом. Спорт вне занятий по физической культуре для студента УГАТУ – это осенние и весенние старты на факультетах, военно-спортивная эстафета, посвящённая 9 мая, День лыжника. В университете существует спортклуб, на базе которого работает 25 секций по 28 видам спорта, среди которых кикбоксинг, бокс-сават, пауэрлифтинг, полиатлон, аэробика.

Все желающие могут посещать спортивные секции, кружки по военно-прикладным видам спорта. При УГАТУ существуют турклуб, объединения по техническим и военно-техническим видам спорта, дельтаклуб.

Воспитательная работа и студенческое самоуправление в УГАТУ направлены на создание социокультурной среды, формирующей, ценности, которые станут определяющими в жизни студентов.

Информационное обеспечение воспитательного процесса

Информационное обеспечение учебно-воспитательного процесса в УГАТУ осуществляется через газету «Авиатор», студенческие периодические издания «Взлет» и «Советник», а также через медиацентр, на базе которого создано студенческое телевидение «Студент TV».

7. Нормативно-методическое обеспечение системы оценки качества освоения обучающимися ОПОП ВО

Оценка качества освоения обучающимися основных образовательных программ включает текущий контроль успеваемости, промежуточную и государственную итоговую аттестацию обучающихся.

7.1. Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации

В соответствии с требованиями ФГОС ВО для проведения текущего контроля успеваемости и промежуточной аттестации созданы фонды оценочных средств.

Фонды оценочных средств входят в состав соответственно рабочих программ учебных дисциплин, программ практик и НИР.

7.2. Программа государственной итоговой аттестации

Государственная итоговая аттестация выпускника высшего учебного заведения является обязательной и осуществляется после освоения основной профессиональной образовательной программы в полном объеме.

Государственная итоговая аттестация включает защиту выпускной квалификационной работы.

Программа государственной итоговой аттестации прилагается.

8. Условия реализации образовательной программы лицами с ограниченными возможностями здоровья

Содержание образования и условия организации обучения студентов с ограниченными возможностями здоровья определяются базовой образовательной программой. Программа при необходимости может быть адаптирована. 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.

Адаптированная образовательная программа разрабатывается на основе ОПОП ВО по соответствующему направлению подготовки (специальности) с учетом особых условий, касающихся учебно-методического, организационного, материально-технического и информационного сопровождения.

9. Другие нормативно-методические документы и материалы, обеспечивающие качество подготовки обучающихся

Другие нормативно-методические документы и материалы, обеспечивающие качество подготовки обучающихся не предусмотрены.

Пояснительная записка к программе по учету требований профессиональных стандартов (ПС)

1. Определение объема учета ПС в образовательной программе

Направление подготовки	Направленность подготовки	Номер уровня квалификации	Наименование выбранного профессионального стандарта
10.03.01 «Информационная безопасность»	Безопасность автоматизированных систем	6	06.033 Специалист по защите информации в автоматизированных системах (Утвержден Приказом Минтруда России №522н от 15.09.2016)

2. Анализ обобщенных трудовых функций

№ п./п.	Код ОТФ	Наименование ОТФ	Изменение	Обоснование
1	B	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	без изменений	
2	C	Внедрение систем защиты информации автоматизированных систем	без изменений	
3	D	Разработка систем защиты информации автоматизированных систем	Добавить ТФ 7-го уровня: D/01.7, D/02.7, D/03.7	Решение профессиональных задач ФГОС требует включения дополнительных ТФ из ПС
4	E	Формирование требований к защите информации в автоматизированных системах	Добавить ТФ 8-го уровня: E/01.8	Решение профессиональных задач ФГОС требует включения дополнительных ТФ из ПС

3. Анализ трудовых функций

Сопоставление профессиональных задач ФГОС и трудовых функций ПС

Требования ФГОС ВО	Требования ПС		Выводы
Профессиональные задачи	**Обобщенные трудовые функции (ОТФ)**	**Трудовые функции (ТФ)**	
Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (B)	Диагностика систем защиты информации автоматизированных систем (B/01.6)	Профессиональная задача является частью трех ОТФ, ТФ представлены в явном виде.
		Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций (B/04.6)	
	Внедрение систем защиты информации автоматизированных систем (C)	Установка и настройка средств защиты информации в автоматизированных системах (C/01.6)	
	Разработка систем защиты информации	Тестирование систем защиты инфор-	

	автоматизированных систем (D)	мации автоматизированных систем (D/01.7)	
Администрирование подсистем информационной безопасности объекта	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (B)	Администрирование систем защиты информации автоматизированных систем (B/02.6)	Полное соответствие
Участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (B)	Аудит защищенности информации в автоматизированных системах (B/06.6)	Полное соответствие
Сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (B)	Мониторинг защищенности информации в автоматизированных системах (B/05.6)	Профессиональная задача является частью двух ОТФ, ТФ представлены не явно. Частичное соответствие
		Аудит защищенности информации в автоматизированных системах (B/06.6)	
	Внедрение систем защиты информации автоматизированных систем (C)	Анализ уязвимостей внедряемой системы защиты информации (C/03.6)	
Проведение проектных расчетов элементов систем обеспечения информационной безопасности	Разработка систем защиты информации автоматизированных систем (D)	Разработка проектных решений по защите информации в автоматизированных системах (D/02.7)	Полное соответствие
Участие в разработке технологической и эксплуатационной документации	Разработка систем защиты информации автоматизированных систем (D)	Разработка эксплуатационной документации на системы защиты информации автоматизированных систем (D/03.7)	Полное соответствие
Проведение предварительного технико-экономического обоснования проектных расчетов	Формирование требований к защите информации в автоматизированных системах (E)	Обоснование необходимости защиты информации в автоматизированной системе (E/01.8)	Частичное соответствие
Проведение экспериментов по заданной методике, обработка и анализ их результатов	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (B)	Диагностика систем защиты информации автоматизированных систем (B/01.6)	Частичное соответствие
Проведение вычислительных экспериментов с использованием стандартных программных средств	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (B)	Диагностика систем защиты информации автоматизированных систем (B/01.6)	Частичное соответствие
Осуществление организационно-правового обеспечения информационной безопасности объекта защиты	Внедрение систем защиты информации автоматизированных систем (C)	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах (C/02.6)	Полное соответствие
		Внедрение организационных мер по защите информации в автоматизирован-	

		ных системах (С/04.6)	
Участие в совершенствовании системы управления информационной безопасностью	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (В)	Управление защитой информации в автоматизированных системах (В/03.6)	Частичное соответствие
Контроль эффективности реализации политики информационной безопасности объекта защиты	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (В)	Управление защитой информации в автоматизированных системах (В/03.6)	Частичное соответствие

Согласно проведенному анализу, для выбранного вида деятельности не выявлено отсутствующих профессиональных задач ФГОС ВО, согласно требованиям функций из соответствующих профессиональных стандартов.

4. Формирование перечня компетенций, вносимых в ОПОП дополнительно к компетенциям ФГОС ВО

Сопоставление профессиональных компетенций ФГОС и трудовых функций ПС

Требования ФГОС ВО	Требования ПС	Выводы
Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1).	Установка и настройка средств защиты информации в автоматизированных системах. Уровень квалификации – 6. Тестирование систем защиты информации автоматизированных систем. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2).	Установка и настройка средств защиты информации в автоматизированных системах. Уровень квалификации – 6. Тестирование систем защиты информации автоматизированных систем. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3).	Администрирование систем защиты информации автоматизированных систем. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4).	Управление защитой информации в автоматизированных системах. Мониторинг защищенности информации в автоматизированных системах. Анализ уязвимостей внедряемой системы защиты информации. Внедрение организационных мер по защите информации в автоматизированных системах. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5).	Диагностика систем защиты информации автоматизированных систем. Аудит защищенности информации в автоматизиро-	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО

	ванных системах. Уровень квалификации – 6	
Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6).	Диагностика систем защиты информации автоматизированных систем. Аудит защищенности информации в автоматизированных системах. Уровень квалификации – 6. Тестирование систем защиты информации автоматизированных систем. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).	Анализ уязвимостей внедряемой системы защиты информации. Уровень квалификации – 6. Разработка проектных решений по защите информации в автоматизированных системах. Обоснование необходимости защиты информации в автоматизированной системе. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8).	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах. Уровень квалификации – 6. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9).	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах. Уровень квалификации – 6. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10).	Мониторинг защищенности информации в автоматизированных системах. Аудит защищенности информации в автоматизированных системах. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11).	Диагностика систем защиты информации автоматизированных систем. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-	Аудит защищенности информации в автоматизированных системах. Уровень	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с

12).	квалификации – 6. Разработка проектных решений по защите информации в автоматизированных системах. Уровень квалификации – 7.	профессиональными компетенциями ФГОС ВО
Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13).	Управление защитой информации в автоматизированных системах. Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций. Анализ уязвимостей внедряемой системы защиты информации. Внедрение организационных мер по защите информации в автоматизированных системах. Уровень квалификации – 6. Разработка проектных решений по защите информации в автоматизированных системах. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-1).	Установка и настройка средств защиты информации в автоматизированных системах. Уровень квалификации – 6. Обоснование необходимости защиты информации в автоматизированной системе. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-2).	Администрирование систем защиты информации автоматизированных систем. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации (ПСК-3).	Управление защитой информации в автоматизированных системах. Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций. Анализ уязвимостей внедряемой системы защиты информации. Внедрение организационных мер по защите информации в автоматизированных системах. Уровень квалификации – 6. Тестирование систем защиты информации автоматизированных систем. Уровень квалификации – 7.	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности (ПСК-4).	Установка и настройка средств защиты информации в автоматизированных системах. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО

5. Формирование результатов освоения программы с учетом ПС

Результаты освоения ОПОП ВО

Виды профессиональной деятельности	Профессиональные задачи	Профессиональные компетенции и/или профессионально-специализированные компетенции
Эксплуатационная	Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований	− Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1). − Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2). − Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)
	Администрирование подсистем информационной безопасности объекта	− Способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3). − Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-2).
	Участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем	− Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5). − Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6).
Проектно-технологическая	Сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	− Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7). − Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-1). − Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности
	Проведение проектных расчетов элементов систем обеспечения информационной безопасности	

	Участие в разработке технологической и эксплуатационной документации	− Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8).
	Проведение предварительного технико-экономического обоснования проектных расчетов	− Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).
Экспериментально-исследовательская	Сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования	− Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9). − Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10).
	Проведение экспериментов по заданной методике, обработка и анализ их результатов	− Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11).
	Проведение вычислительных экспериментов с использованием стандартных программных средств	− Способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).
Организационно-управленческая	Осуществление организационно-правового обеспечения информационной безопасности объекта защиты	− Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15). − Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации (ПСК-3).
	Организация работы малых коллективов исполнителей	− Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14).
	Участие в совершенствовании системы управления информационной безопасностью	− Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13).
	Изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа	
	Контроль эффективности реализации политики информационной безопасности объекта защиты	

Общепрофессиональные компетенции: − Способность анализировать физические явления и процессы для решения профессиональных задач (ОПК-1). − Способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2). − Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3). − Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4). − Способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5). − Способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6). − Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).
Общекультурные компетенции: − Способность использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1). − Способность использовать основы экономических знаний в различных сферах деятельности (ОК-2). − Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3). − Способность использовать основы правовых знаний в различных сферах деятельности (ОК-4). − Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5). − Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6). − Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7). − Способность к самоорганизации и самообразованию (ОК-8). − Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

6. Учет ПС при разработке фонда оценочных средств и формировании структуры и содержании программы

Формирование содержания практики

Трудовые функции	Освоенные результаты компетенции	Виды работ на практике
− Обоснование необходимости защиты информации в автоматизированной системе; − Внедрение организационных мер по защите информации в автоматизированных системах.	Вид профессиональной деятельности: проектно-технологическая, экспериментально-исследовательская Учебная практика Объем практики (в зачетных единицах) – 3 ЗЕ	
	ОПК-1 Способность анализировать физические явления и процессы для решения профессиональных задач; ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений; ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методиче-	− Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите; − Выявление степени участия персонала в обработке защищаемой информации; − Планирование мероприятий по обеспечению защиты информации в автоматизированной системе; − Определение требуемого класса (уровня) защищенности автоматизированной системы; − Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня

	ских документов; ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	защищенности информации, содержащейся в информационной системе; − Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации.
− Диагностика систем защиты информации автоматизированных систем; − Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций; − Установка и настройка средств защиты информации в автоматизированных системах; − Тестирование систем защиты информации автоматизированных систем; − Администрирование систем защиты информации автоматизированных систем; − Аудит защищенности информации в автоматизированных системах; − Мониторинг защищенности информации в автоматизированных системах; − Анализ уязвимостей внедряемой системы защиты информации; − Разработка проектных решений по защите информации в автоматизированных системах; − Разработка эксплуатационной документации на системы защиты информации автоматизированных систем; − Обоснование необходимости защиты информации в автоматизированной системе; − Разработка организационно-распорядительных документов по защите информации в автоматизированных системах; − Внедрение организационных мер по защите информации в автоматизированных системах; − Управление защитой информации в автоматизированных системах.	Вид профессиональной деятельности: проектно-технологическая, эксплуатационная, экспериментально-исследовательская Производственная практика Объем практики (в зачетных единицах) – 6 ЗЕ	
	ОПК-1 Способность анализировать физические явления и процессы для решения профессиональных задач; ОПК-2 Способность применять соответствующий математический аппарат для решения профессиональных задач; ОПК-3 Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач; ОПК-4 Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации; ОПК-5 Способность использовать нормативные правовые акты в профессиональной деятельности; ОПК-7 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; ПК-3 Способность администрировать подсистемы ин-	− Обнаружение, идентификация и устранение инцидентов в процессе эксплуатации автоматизированной системы; − Оценка защищенности автоматизированных систем с помощью типовых программных средств; − Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы; − Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; − Оценка последствий от реализации угроз безопасности информации в автоматизированной системе; − Обнаружение и устранение неисправностей в работе системы защиты информации автоматизированной системы; − Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций; − Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы; − Выявление угроз безопасности информации в автоматизированных системах; − Анализ и устранение недостатков в функционировании системы защиты информации автоматизированной системы; − Оценка информационных рисков; − Экспертиза состояния защищенности информации автома-

	формационной безопасности объекта защиты; ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений; ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; ПК-9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; ПК-15 Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	тизированных систем; − Определение правил и процедур выявления инцидентов и реагирования на них; − Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы; − Проведение анализа уязвимостей автоматизированных и информационных систем; − Подбор инструментальных средств тестирования систем защиты информации автоматизированных систем; − Разработка проектов нормативных документов, регламентирующих работу по защите информации; − Разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах; − Анализ технической документации информационной инфраструктуры автоматизированной системы; − Анализ защищенности информационной инфраструктуры автоматизированной системы; − Формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач; − Анализ структурных и функциональных схем защищенных автоматизированных информационных систем; − Обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем; − Использование программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах; − Определение требуемого класса (уровня) защищенности автоматизированной системы.
− Диагностика систем защиты информации автоматизированных систем; − Тестирование систем защиты информации автоматизированных систем; − Аудит защищенности информации в автоматизированных системах; − Анализ уязвимостей внедряемой системы защиты информации; − Разработка проектных реше-	Вид профессиональной деятельности: проектно-технологическая, экспериментально-исследовательская Преддипломная практика Объем практики (в зачетных единицах) – 6 ЗЕ	
	ОПК-1 Способность анализировать физические явления и процессы для решения профессиональных задач; ОПК-2 Способность применять соответствующий математический аппарат для решения профессиональных задач; ОПК-3 Способность применять	− Обнаружение, идентификация и устранение инцидентов в процессе эксплуатации автоматизированной системы; − Оценка защищенности автоматизированных систем с помощью типовых программных средств; − Расчет показателей эффективности защиты информации, об-

ний по защите информации в автоматизированных системах; − Обоснование необходимости защиты информации в автоматизированной системе; − Управление защитой информации в автоматизированных системах.	положения электротехники, электроники и схемотехники для решения профессиональных задач; ОПК-4 Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации; ОПК-5 Способность использовать нормативные правовые акты в профессиональной деятельности; ОПК-7 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений; ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; ПК-9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; ПК-10 Способность проводить анализ информационной без-	рабатываемой в автоматизированных системах; − Оценка информационных рисков; − Экспертиза состояния защищенности информации автоматизированных систем; − Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных системс целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; − Выявление уязвимости информационно-технологических ресурсов автоматизированных систем; − Выявление основных угроз безопасности информации в автоматизированных системах; − Составление методик тестирования систем защиты информации автоматизированных систем; − Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах; − Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем; − Разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах; − Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем; − Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы; − Проведение экспертизы состояния защищенности информации автоматизированных систем; − Проведение анализа уязвимостей автоматизированных и информационных систем; − Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; − Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите; − Планирование мероприятий по обеспечению защиты информа-

	опасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; ПК-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации; ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; ПСК-1 Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации; ПСК-2 Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей; ПСК-3 Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации; ПСК-4 Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности.	ции в автоматизированной системе; − Определение требуемого класса (уровня) защищенности автоматизированной системы.
− Диагностика систем защиты информации автоматизированных систем; − Аудит защищенности информации в автоматизированных системах; − Анализ уязвимостей внедряемой системы защиты информации; − Разработка проектных решений по защите информации в автоматизированных системах; − Обоснование необходимости защиты информации в автоматизированной системе; − Управление защитой информации в автоматизированных системах.	Вид профессиональной деятельности: экспериментально-исследовательская Научно-исследовательская работа Объем практики (в зачетных единицах) – 3 ЗЕ	
	ОПК-1 Способность анализировать физические явления и процессы для решения профессиональных задач; ОПК-2 Способность применять соответствующий математический аппарат для решения профессиональных задач; ОПК-5 Способность использовать нормативные правовые акты в профессиональной деятельности; ОПК-7 Способность определять информационные ресурсы, подлежащие защите, угрозы без-	−Оценка защищенности автоматизированных систем с помощью типовых программных средств; −Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; −Оценка информационных рисков; −Экспертиза состояния защищенности информации автоматизированных систем; −Обоснование критериев эффективности функционирования

	опасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений; ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; ПК-9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; ПК-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; ПК-11 Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов; ПК-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации; ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по	защищенных автоматизированных систем; −Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем; −Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы; −Уточнение модели угроз безопасности информации автоматизированной системы; −Проведение анализа уязвимостей автоматизированных и информационных систем; −Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах; −Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем; −Разработка проектов нормативных документов, регламентирующих работу по защите информации; −Разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах; −Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите; −Планирование мероприятий по обеспечению защиты информации в автоматизированной системе; −Определение требуемого класса (уровня) защищенности автоматизированной системы; −Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность; −Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; −Оценка последствий от реализации угроз безопасности информации в автоматизированной системе.

	обеспечению информационной безопасности, управлять процессом их реализации; ПСК-1 Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации; ПСК-2 Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей; ПСК-3 Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации.	

ПРИЛОЖЕНИЯ

Приложение 1

Матрица соответствия дисциплин и компетенций, формируемых в результате освоения ОПОП ВО

Содержание дисциплин и иных форм учебной деятельности	Формируемые компетенции											
Дисциплины (модули)	**ОК-1**	**ОК-2**	**ОК-3**	**ОК-4**	**ОК-5**	**ОК-6**	**ОК-7**	**ОК-8**	**ОК-9**	**ОПК-1**	**ОПК-2**	**ОПК-3**
	ОПК-4	**ОПК-5**	**ОПК-6**	**ОПК-7**	**ПК-1**	**ПК-2**	**ПК-3**	**ПК-4**	**ПК-5**	**ПК-6**	**ПК-7**	**ПК-8**
	ПК-9	**ПК-10**	**ПК-11**	**ПК-12**	**ПК-13**	**ПК-14**	**ПК-15**	**ПСК-1**	**ПСК-2**	**ПСК-3**	**ПСК-4**	
Философия	ОК-1											
История	ОК-3											
Иностранный язык	ОК-7											
Иностранный язык в профессиональной деятельности	ОК-7											
Экономика	ОК-2	ПК-7										
Правоведение	ОК-4											
Основы управленческой деятельности	ОК-6	ОК-8	ПК-13	ПК-14								
Психология и педагогика	ОК-6	ОК-8	ПК-14									
Модуль Математика												
Линейная алгебра и аналитическая геометрия	ОПК-2	ПК-7	ПК-11									
Математический анализ	ОПК-2	ПК-7	ПК-11									
Теория вероятностей и математическая статистика	ОПК-2	ПК-7	ПК-11									
Дискретная математика	ОПК-2	ПК-7	ПК-11									
Информатика	ОПК-4	ПК-2										
Физика	ОПК-1											
Физические основы защиты информации	ОПК-1	ПК-12										
Теория информации	ОПК-2	ПК-1										
Основы информационной безопасности	ОПК-4	ОПК-7	ПК-7	ПК-9								
Аппаратные средства вычислительной техники	ПК-1	ПСК-4										

Программно-аппаратные средства защиты информации	ОПК-7	ПК-1	ПК-2	ПК-3	ПСК-2							
Защита информационных процессов в компьютерных системах	ОПК-7	ПК-1	ПК-2	ПСК-1	ПСК-2							
Криптографические методы защиты информации	ОПК-2	ПК-2	ПК-6									
Организационное и правовое обеспечение информационной безопасности	ОПК-5	ПК-9	ПК-13	ПК-15								
Техническая защита информации	ОПК-3	ПК-1	ПК-6	ПК-12	ПК-13							
Сети и системы передачи информации	ОПК-4	ПК-1	ПСК-1	ПСК-2	ПСК-4							
Безопасность жизнедеятельности	ОПК-6											
Математическая логика и теория алгоритмов	ОПК-2	ПК-2										
Программирование												
Языки программирования	ПК-2	ПСК-4										
Технологии и методы программирования	ПК-2	ПСК-4										
Управление информационной безопасностью	ОПК-7	ПК-4	ПК-13									
Документоведение	ПК-8	ПК-9										
Защита и обработка документов ограниченного доступа	ПК-8	ПК-15	ПСК-1									
Электротехника	ОПК-1	ОПК-3	ПК-1									
Электроника и схемотехника	ОПК-1	ОПК-3	ПК-1									
Информационные технологии	ОПК-4	ПК-2	ПСК-1									
Проектирование защищенных компьютерных систем	ОПК-7	ПК-7	ПК-8									
Стандарты информационной безопасности и аудит	ПК-5	ПК-10										
Технические средства охраны	ОПК-3	ПК-1	ПК-13									
Физическая культура	ОК-9											
Русский язык	ОК-7	ПК-8	ПК-9									
Теория принятия решений	ОПК-2	ПК-7										
Теория нечетких систем	ОПК-2	ПК-7										
Математические основы теории надежности	ОПК-2	ПК-12	ПСК-3									

Прикладная математика												
Методы оптимизации	ОПК-2	ПК-7										
Теория автоматов	ОПК-3	ПСК-4										
Телекоммуникационные технологии	ОПК-4	ПК-2	ПСК-1	ПСК-4								
Компьютерно-техническая экспертиза	ОПК-4	ОПК-5	ПК-2									
Комплексная система защиты информации на предприятии	ОПК-7	ПК-4	ПК-13									
Организация ЭВМ и систем	ОПК-3	ПК-1	ПК-2	ПСК-4								
Экономика защиты информации	ОК-2	ПК-7										
Введение в профессиональную деятельность	ОК-5											
Элективные курсы по физической культуре	ОК-9											
Социология	ОК-5	ОК-6	ПК-14									
Социология управления	ОК-5	ОК-6	ПК-14									
Политология	ОК-3	ОК-5	ПК-14									
Прикладная политология	ОК-3	ОК-5	ПК-14									
Компьютерная графика	ПК-2											
Web-дизайн	ПК-2											
Информационное право	ОК-4	ОПК-5	ПК-13									
Право интеллектуальной собственности	ОК-4	ОПК-5	ПК-13									
Моделирование технических систем	ОПК-2	ПК-7										
Имитационное моделирование	ОПК-2	ПК-7	ПСК-4									
Методы искусственного интеллекта	ОПК-2	ПК-2	ПСК-1									
Информационные технологии моделирования интеллектуальных систем	ОПК-2	ПК-2	ПСК-1									
Психология воздействия	ОК-6	ПК-14										
Специальные информационные технологии	ОК-6	ПК-14										
Теория принятия решений в системах защиты информации	ОПК-2	ПК-7										
Модели и методы принятия решений в системах защиты информации	ОПК-2	ПК-7										
Катастрофоустойчивость информационных систем	ОПК-7	ПК-12	ПСК-3									

Безопасность критически важных информационных систем	ОПК-7	ПК-12	ПСК-3									
Современные банковские технологии	ПК-2	ПК-4	ПСК-1									
Безопасность систем электронной торговли	ПК-2	ПК-4	ПСК-1									
Электрорадиоизмерения	ОПК-3	ПК-1	ПК-6	ПК-12								
Основы метрологии	ОПК-3	ПК-1	ПК-6	ПК-12								
Практики	**ОК-5**	**ОК-6**	**ОК-7**	**ОК-8**	**ОПК-1**	**ОПК-2**	**ОПК-3**	**ОПК-4**	**ОПК-5**	**ОПК-6**	**ОПК-7**	**ПК-1**
	ПК-2	**ПК-3**	**ПК-4**	**ПК-7**	**ПК-8**	**ПК-9**	**ПК-10**	**ПК-11**	**ПК-12**	**ПК-13**	**ПК-15**	**ПСК-1**
	ПСК-2	**ПСК-3**	**ПСК-4**									
Учебная	ОК-5	ОК-6	ОК-7	ОК-8	ОПК-1	ОПК-2	ОПК-3	ОПК-4	ОПК-5	ОПК-6	ОПК-7	ПК-1
	ПК-2	ПК-7	ПК-8	ПК-9	ПК-13							
Производственная	ОК-5	ОК-6	ОК-7	ОК-8	ОПК-1	ОПК-2	ОПК-3	ОПК-4	ОПК-5	ОПК-6	ОПК-7	ПК-1
	ПК-2	ПК-3	ПК-4	ПК-7	ПК-8	ПК-9	ПК-13	ПК-15				
Преддипломная	ОК-5	ОК-7	ОК-8	ОПК-1	ОПК-2	ОПК-3	ОПК-4	ОПК-5	ОПК-6	ОПК-7	ПК-1	ПК-2
	ПК-3	ПК-4	ПК-7	ПК-8	ПК-9	ПК-10	ПК-12	ПК-13	ПСК-1	ПСК-2	ПСК-3	ПСК-4
Научно-исследовательская работа	ОК-7	ОК-8	ОПК-1	ОПК-2	ОПК-3	ОПК-5	ОПК-7	ПК-2	ПК-4	ПК-7	ПК-8	ПК-9
	ПК-10	ПК-11	ПК-12	ПК-13	ПСК-1	ПСК-2	ПСК-3					
Государственная итоговая аттестация	**ОК-1**	**ОК-2**	**ОК-3**	**ОК-4**	**ОК-5**	**ОК-6**	**ОК-7**	**ОК-8**	**ОК-9**	**ОПК-1**	**ОПК-2**	**ОПК-3**
	ОПК-4	**ОПК-5**	**ОПК-6**	**ОПК-7**	**ПК-1**	**ПК-2**	**ПК-3**	**ПК-4**	**ПК-5**	**ПК-6**	**ПК-7**	**ПК-8**
	ПК-9	**ПК-10**	**ПК-11**	**ПК-12**	**ПК-13**	**ПК-14**	**ПК-15**	**ПСК-1**	**ПСК-2**	**ПСК-3**	**ПСК-4**	
Факультативы	**ОК-6**	**ОК-7**	**ОК-8**									
Культура делового человека	ОК-6	ОК-7	ОК-8									

Рецензия

на основную профессиональную образовательную программу подготовки бакалавра по направлению 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Представленная к рецензированию ОПОП ориентирована на следующие объекты, области и виды профессиональной деятельности выпускника.

Объектами профессиональной деятельности по профилю «Безопасность автоматизированных систем» в соответствие с ФГОС ВО по данному направлению подготовки являются:

- объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;
- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;
- процессы управления информационной безопасностью защищаемых объектов.

В соответствии с ФГОС ВО по данному направлению подготовки выпускник с профилем подготовки «Безопасность автоматизированных систем» подготовлен к следующим видам профессиональной деятельности:

- эксплуатационная;
- проектно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая.

В соответствии с запросами рынка труда выпускник с профилем подготовки «Безопасность автоматизированных систем» подготовлен к:

- применению современных информационных технологий в профессиональной деятельности;
- обоснованному применению технологических решений при проектировании систем защиты информации;
- осуществлению контроля и диагностики состояния компонентов системы обеспечения информационной безопасности;
- использованию основных законов естественнонаучных дисциплин в профессиональной деятельности, применению методов математического анализа и моделирования, теоретического и экспериментального исследования;
- выполнению профессиональной деятельности.

В число организаций и учреждений, в которых может осуществлять профессиональную деятельность выпускник по данному направлению подготовки и профилю входят:

– академические, ведомственные и частные научно-исследовательские и производственные организации, связанные с решением проблем, связанных с обеспечением безопасности компьютерных систем;

– учреждения системы высшего и среднего профессионального образования, среднего общего образования.

Выбранные объекты, области и виды профессиональной деятельности выпускника соответствуют кадровым потребностям работодателя, представляющего рецензию.

В ОПОП заявленные результаты обучения были сформированы с учетом требований профессиональных стандартов, согласованных с представителями работодателя, представляющего рецензию на этапе разработки ОПОП.

Для заявленных в ОПОП компетенций были разработаны фонды оценочных средств (ФОС), показатели и критерии оценивания которых однозначно позволяют проверить их сформированность на различных этапах их формирования.

В целом, ФОС (контрольно-измерительные оценочные материалы) позволяют оценить достижение запланированных результатов обучения и уровень сформированности всех компетенций, заявленных в ОПОП. Для каждого результата обучения по дисциплине (модулю) и/или практике имеются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

Исходя из вышеизложенного, можно сделать заключение, что ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», реализуемая в ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ) по профилю «Безопасность автоматизированных систем» соответствует требованиям образовательного стандарта, профессионального стандарта и современным требованиям рынка труда.

Директор ЗАО «Республиканский центр защиты информации» С.Н. Зарипов

РЕСПУБЛИКАНСКИЙ ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ
ИНН 0274079299

ВЫПИСКА из протокола заседания

Научно-методического совета

по укрупненной группе направлений подготовки
10.00.00 Информационная безопасность
(шифр и наименование)

На основании анализа состава и содержания документов основной образовательной программы по направлению подготовки
10.03.01 Информационная безопасность
(шифр и наименование образовательной программы)

по профилю (направленности) Безопасность автоматизированных систем,
реализуемой по форме обучения очной
(указать нужное: очной, очно-заочной (вечерней), заочной)

Научно-методический совет подтверждает, что:
- ОПОП не изменялась и является актуальной на 2017–2018 уч.год;
- комплект рабочих программ дисциплин не изменялся и является актуальным на 2017–2018 уч.год;
- программа практик не изменялась и является актуальной на 2017–2018 уч.год;
- программа НИР не изменялась и является актуальной на 2017–2018 уч.год;
- программа ГИА не изменялась и является актуальной на 2017–2018 уч.год.

Председатель НМС Васильев В.И.
подпись

«23» 06 2017 г.
дата

ВЫПИСКА
из протокола заседания
научно-методического совета по УГСН 10.00.00
Информационная безопасность
№ _10_ от _28___ июня 2018 г.

На основании анализа состава и содержания документов основной образовательной программы уровня ВО бакалавриата по направлению подготовки __10.03.01 Информационная безопасность, по профилю «Безопасность автоматизированных систем», очная форма обучения

Научно-методический совет подтверждает, что:

- внесены изменения (дополнения) в основную профессиональную образовательную программу (ОПОП):

1. Раздел 5(пункт5.2) Основной профессиональной образовательной программы, в связи с обновлением ЭБС и электронных ресурсов библиотеки УГАТУ, а также имеющегося и приобретенного нового лицензионного программного обеспечения учебного процесса.

ЭБС, доступные УГАТУ на 2018--2019 год.

Электронные ресурсы

Отечественные:

№	Наименование ресурса	Объем фонда электронных ресурсов (экз.)	Доступ	Реквизиты договоров
1	2	3	4	5
1.	Электронная коллекция образовательных ресурсов УГАТУ http://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus	682	С компьютера в сети УГАТУ	Свидетельство о регистрац. №2012620618 от 22.06.2012
2.	ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru	1784	С компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Учредительный договор Ассоциации образовательных организаций «Электронное образование Республики Башкортостан» от 29.11.2013
3.	ЭБС Консорциума аэрокосмических вузов России http://elsau.ru/	4704	С компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Договор о сетевом взаимодействии от 15.12.2014
4.	ЭБС «Лань» http://e.lanbook.com/	42 337	С компьютера, имеющего выход в Интернет, после регистрации в ЭБС в сети УГАТУ	Договор № ЕД-936/0305-17 от 18.07.2017

5.	ЭБС BOOK.ru - http://www.book.ru	7018	С компьютера, имеющего выход в Интернет, после регистрации в ЭБС в сети УГАТУ	Договор №1276/0305-17 от 13.11.2017
6.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	919 000	С компьютеров библиотеки, подключенных к ресурсу.	Договор ЕД 165/0305-18 от 19.03.2018
7.	База данных «Электронно-библиотечная система elibrary» http://elibrary.ru/	4 наим. полнотекстовых отечественных журналов	Доступ с компьютеров в сети УГАТУ.	Договор 1399/0305-17 от 08.12.2017
8.	СПС «КонсультантПлюс»	2 520086 док.	С компьютеров в сети УГАТУ.	Договор №1494/0302-17 от 19.12.2017
9.	СПС «Гарант»	8 768552 док.	С компьютеров библиотеки	Договор 2/1304-18 от 24.01.2018
10.	ИПС «Технорма»	41 025	С компьютеров библиотеки, подключенных к ресурсу	Договор № 45/0305-18 от 06.02.2018

Зарубежные:

Информационные ресурсы, доступные УГАТУ по результатам конкурсов Министерства науки и высшего образования РФ				
№	**Наименование ресурса**	**Объем фонда электронных ресурсов**	**Доступ**	**Реквизиты договоров**
1.	База данных Web of Science компании Clarivate Analytics (Scientific) LLC http://apps.webofknowledge.com/	Свыше 55 млн. библиографических записей, частично с полными текстами	С компьютеров сети УГАТУ, имеющих выход в Интернет	Сублиц. договор № WoS/ 1129 от 02.04.2018 151/0305-18 от 18.06.2018)
2.	База данных Scopus компании Elsevier https://www.scopus.com/	22800 изданий	С компьютеров сети УГАТУ, имеющих выход в Интернет	Сублиц. договор № Scopus /1129 от 09.01.2018 (118/0305-18 от 31.05.18)
3.	Патентная база данных компании Questel Orbit http://www.orbit.com	60 млн. документов	С компьютеров сети УГАТУ, имеющих выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018

4.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн.	С компьютеров сети УГАТУ, имеющих выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
5.	Научные журналы издательства **Taylor& Francis Group** http://www.tandfonline.com	1700 наимен. полнотекстовых журналов	С компьютеров сети УГАТУ, имеющих выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
6.	Научные журналы издательства Sage Publications http://online.sagepub.com/	790 наимен. полнотекстовых журналов	С компьютеров сети УГАТУ, имеющих выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
7.	Научные журналы издательства Oxford University Press http://www.oxfordjournals.org/	255 наимен полнотекстовых журналов	С компьютеров сети УГАТУ, имеющих выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
8.	Цифровая библиотека Association for Computing Machinery (ACM) http://dl.acm.org/	70 наимен. полнотекстовых журналов, 69 инф. бюллетеней,	С компьютера в сети УГАТУ, имеющего выход в Интернет	Сублиц. договор №ACM/25 от 01.11.2017

		1000 наимен. материалов конф		
9.	База данных Computers & Applied Sciences Complete компании EBSCO Publishing http://search.ebscohost.com	1000 наимен. полнотекстовых журналов	С компьютера в сети УГАТУ, имеющего выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
10.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиогр. записей	С компьютера в сети УГАТУ, имеющего выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
11.	Science **The American Association for the Advancement of Science** http://www.sciencemag.org	Полнотекстовый журнал	С компьютера в сети УГАТУ, имеющего выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
12.	Научные журналы Американского института физики http://scitation.aip.org/	18 наимен. полнотекстовых журналов	С компьютера в сети УГАТУ, имеющего выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
13.	Научные журналы Института физики (Великобритания)	105 наимен. полнотекстовых журналов	С компьютеров сети УГАТУ, имеющих выход в	УГАТУ в составе организаций, получивших поддержку РФФИ для

	компании IOP Publishing Limited http://iopscience.iop.org		Интернет	получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
14.	Научные ресурсы Optical Society of America http://www.opticsinfobase.org/	19 наимен. полнотекстовых журналов	С компьютеров сети УГАТУ, имеющих выход в Интернет	УГАТУ в составе организаций, получивших поддержку РФФИ для получения доступа к электронным научным информационным ресурсам зарубежных издательств во втором полугодии 2018 года. Договор на стадии подписания. Доступ открыт до 31.12.2018
Информационные ресурсы, доступные при финансовой поддержке РФФИ				
№	**Наименование ресурса**	**Объем фонда электронных ресурсов**	**Доступ**	**Реквизиты договоров**
1.	Электронные ресурсы издательства Elsevier https://www.sciencedirect.com/ • База данных Freedom Collection • Коллекция электронных книг Evidence Based Selection	2500 наимен. журналов, 15000 книг	С компьютеров сети УГАТУ, имеющих выход в Интернет	(Приложение к письму РФФИ № 206/0305-12 08.02.2018)
2.	Электронные ресурсы издательства Springer http://www.springerlink.com ▪ полнотекстовые журналы по различным отраслям знаний Springer Journals http://link.springer.com ▪ полнотекстовые книги по различным отраслям знаний Springer Journals http://link.springer.com ▪ научные протоколы по различным отраслям зна-	2281 наимен. журналов, 46 322 наим. книг, 44 847 протоколов, 680 справочных материалов, более 3,5 млн. библиографических записей и рефератов.	С компьютеров сети УГАТУ, имеющих выход в Интернет	Сублиц. договор №Springer/25 от 25.12.2017 (108/0305-18 от 26.03.2018)

	ний SpringerProtocols http://www.springerprotocols.com/ ▪ научные материалы в области физических наук SpringerMaterials http://materials.springer.com ▪ справочные материалы Springer ReferencesWork http://link.springer.com реферативная база данных по математике Zentralblatt MATH http://www.zentralblatt-math.org/zbmath/en			
3	Научные журналы Nature Publishing Group http://www.nature.com	120 наимен. полнотекстовых журналов	С компьютеров сети УГАТУ, имеющих выход в Интернет	При финансовой поддержке РФФИ в соответствии с «Условиями использования содержания баз данных издательств SPRINGERNATURE» (Приложение №2 к письму РФФИ № 779 от 16.09.2016)

Информационные ресурсы, доступные УГАТУ, как участнику НЭИКОН

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров
1.	База данных GreenFile компании EBSCO http://www.greeninfoonline.com	500 000 тыс библиогр. записей. в т.ч 5800, с полными текстами	С компьютеров сети УГАТУ, имеющих выход в Интернет	Доступ предоставлен компанией EBSCO
2.	Архив научных журналов зарубежных издательств http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849–1995) SAGE Publications (1800-1998) цифровой архив журнала Science (1880 -1996) Taylor & Francis (1798-1997) Институт физики Великобритании (The Institute of Physics) (1874-2000)	2361 наимен. полнотекстовых журналов	С компьютеров сети УГАТУ, имеющих выход в Интернет	Гос. контракт Минобрнауки России № 07.551.11.4002

Кафедра, реализующая образовательную программу подготовки, обеспечена необходимым комплектом программного обеспечения:

№ п/п	Наименование лицензии	Договор/лицензия
3.	Xspider Education	Лицензионный договор 090-18/E от 27.06.2018
4.	MaxPatrol Education	Лицензионный договор 090-18/E от 27.06.2018
5.	PT Application Firewall Education	Лицензионный договор 090-18/E от 27.06.2018
6.	MaxPatrol SIEM	Лицензионный договор 090-18/E от 27.06.2018
7.	СЗИ «Блокхост-МДЗ», 4 модуля: ШДЗ, ОП, КЦ, ГУ	Договор о сотрудничестве 21 от 04.06.2018
8.	СЗИ «Блокхост-сеть 2.0», автономный вариант	Договор о сотрудничестве 21 от 04.06.2018
9.	СЗИ «Блокхост-сеть 2.0», сервер управления	Договор о сотрудничестве 21 от 04.06.2018
10.	СЗИ «Блокхост-сеть 2.0», сетевой вариант	Договор о сотрудничестве 21 от 04.06.2018
11.	ПК «Litoria Desktop 2»	Договор о сотрудничестве 21 от 04.06.2018
12.	ПК «Efros Config Inspector 3.0» Premium, сервер	Договор о сотрудничестве 21 от 04.06.2018
13.	ПК «Efros Config Inspector 3.0» Premium, клиент Active Network Device	Договор о сотрудничестве 21 от 04.06.2018
14.	ПК «Efros Config Inspector 3.0» Premium, клиент сервера управления среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018
15.	ПК «Efros Config Inspector 3.0» Premium, клиент гипервизора среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018
16.	ПК «Efros Config Inspector 3.0» Premium, клиент Server Operating System	Договор о сотрудничестве 21 от 04.06.2018
17.	ПК «Efros Config Inspector 3.0» Premium, агент контроля целостности Windows OS	Договор о сотрудничестве 21 от 04.06.2018
18.	Kaspersky Endpoint Security для бизнеса - Стандартный	Договор №391/0304-18 от 26.06.2018 г.
19.	Infowatch Traffic Monitor Enterprise Edition 4.0	Соглашение 067-Е-ИВ/2013 о создании экспериментальной площадки (учебного класса) от 18.11.2013. Лицензия ES_Total_10_1Y до 01.01.2020
20.	Infowatch Endpoind Security	Соглашение 067-Е-ИВ/2013 о создании экспериментальной площадки (учебного класса) от 18.11.2013. Лицензия ES_Total_10_27-06-2017
21.	Infowatch Traffic Monitor Enterprise Edition 6.5	Лицензионное соглашение 932-N-ИВ/2016. Лицензия до 19.06.2019
22.	SearchInform Event Manager	Лицензионный договор 1726811 от 28.12.2016 на 3 года
23.	Astra Linux SE (Special Edition) РУСБ.10015-01 (программный продукт в формате BOX)	Лицензионный договор РБТ-14/1318-01-ВУЗ
24.	Специальная версия DLP системы Secure Tower	Лицензионный договор 05/17/2016-1 на 3 года
25.	Сервер безопасности Dallas Lock 8.0-С	лицензионный сертификат 181**-****-*57 от 01.2017
26.	Dallas Lock Linux	лицензионный сертификат 181**-****-**99 от 01.2017
27.	Сервер безопасности Dallas Lock 8.0-К	лицензионный сертификат 181**-****-*13 от 01.2017
28.	Dallas Lock 8.0-К(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**-****-*33 от 01.2017
29.	Dallas Lock 8.0-С(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**-****-*14 от 01.2017
30.	СЗВИ Dallas Lock 8.0	Лицензия 1909***-****-*87 от 06.2017 бессрочно
31.	СЗИ Secret Net 7 Клиент (автономный режим работы)	Лицензия WWIB-****-****-****-****-****-*00S от 16.01.2017
32.	СЗИ Secret Net 7.8 Клиент (автономный режим работы)	Лицензия WWIB-****-****-****-****-****-*001 от 05.03.2018
33.	СЗИ Secret Net 7.8 Сервер безопасности класса С	WWIL-****-****-****-****-****-*003 от 05.03.2018
34.	СЗИ Secret Net 7.8 (Клиент сетевой Режим работы)	WWIC-****-****-****-****-****-*00Q от 05.03.2018
35.	СЗИ Secret Net 7.8 (Терминальное подключение)	WWIA-****-****-****-****-****-*006 от 05.03.2018
36.	СЗИ «Secret Net LSP»	Лицензия 1****A от 16.01.2017
37.	СЗИ «Secret Net LSP»	Лицензия 1****5 от 05.03.2018
38.	Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net LSP	Ключ U*****W от 05.03.2018
39.	Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net	Ключ 3*****T от 05.03.2018

40.	Security Studio Endpoint Protection 7.6	Лицензия WWIS-****-****-****-****-****-*000 от 16.01.2017
41.	Secret Net Studio 8 Поставка Максимальная защита	Лицензия 1*****C, от 16.01.2017
42.	Secret Net Studio 8(модули защиты от НСД, контроля устройств)	Лицензия 1*****C, от 05.03.2018
43.	Secret Net Studio 8(модули персонального межсетевого экрана)	Лицензия 1*****B от 05.03.2018
44.	Secret Net Studio 8 (модуль «Дополнительная защита»)	Лицензия 1****D от 05.03.2018
45.	Secret Net Studio 8 (модуль «Защиты дисков и шифрования контейнеров»)	Лицензия 1*****C, от 05.03.2018
46.	Trust Access для защиты рабочих станций	Лицензия WWIM-****-****-****-****-****-*00Q от 16.01.2017
47.	Trust Access для защиты сервера	Лицензия WWIM-****-****-****-****-****-*00K от 16.01.2017
48.	СЗИ Security Code vGate R2 (Standart)	Лицензия 1****F от 16.01.2017
49.	СЗИ Security Code vGate R2 4.0(Enterprize Plus)	Лицензия 1****7 от 05.03.2018
50.	сервис прямой технической поддержки уровня «Стандартный» для СЗИ VGate	Ключ I****7 от 05.03.2018
51.	Secret MDM Secure Pack на 1 подключенное устройство при локальном размещении	Лицензия 1****A от 05.03.2018
52.	Сервис прямой технической поддержки уровня «Стандартный» для Secret MDM	Ключ B****V от 05.03.2018
53.	СКЗИ «Континент АП»	Лицензия WWIA-****-****-****-** от 05.03.2018
54.	Сервис прямой технической поддержки уровня «Стандартный» для СКЗИ Континент АП	Ключ 8****F от 05.03.2018
55.	Виртуальная машина «Континент»	Договор о сотрудничестве с ООО «Код безопасности» от 05.03.2018
56.	Dr.Web Desktop Security Suite	Договор №90/0304-18 от 22.02.2018 г.
57.	Statistica Basic Academic for Windows 10	Договор №ЭА-561/1701-17 от 14.12.2017 г.
58.	Семейство продуктов компании Microsoft • MS Windows, • MS Server, • MS Office, • MS Visio, • MS Project	Договор №ЭД-644/0304-17 от 21.12.2017 г.

2. Остальные документы ОПОП не изменялись и являются актуальными на 2018-2019 уч. год.

Председатель НМС  В.И. Васильев

ВЫПИСКА
из протокола заседания
научно-методического совета по УГСН 10.00.00
Информационная безопасность
№ 9 от 15 мая 2019 г.

СЛУШАЛИ: доцента кафедры ВТиЗИ Дуленко В.А. о внесении изменений и дополнений в основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», реализуемой в очной форме.

ПОСТАНОВИЛИ: утвердить следующие изменения и дополнения в основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», реализуемой в очной форме:

1. Пункт 5.2 ОПОП изложить в следующей редакции:

5.2 Учебно-методическое и информационное обеспечение

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к следующим электронно-библиотечным системам (ЭБС «Лань» http://e.lanbook.com/ , ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru, Консорциум аэрокосмических вузов России http://elsau.ru/, Электронная коллекция образовательных ресурсов УГАТУ http://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus), содержащим все издания основной литературы, перечисленные в рабочих программах дисциплин (модулей), практик, НИР сформированным на основании прямых договорных отношений с правообладателями.

Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивают возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет, как на территории университета, так и вне ее.

Обучающимся обеспечен доступ к электронным ресурсам и информационным справочным системам, информация о которых представлена на сайте: http://www.library.ugatu.ac.ru/.

УГАТУ обеспечен необходимым комплектом лицензионного программного обеспечения. Информация об используемом программном обеспечении приведена на сайте УГАТУ (http://it.ugatu.su/license.html – программное обеспечение, общее по вузу) и в рабочих программах дисциплин, программах практик, программе ГИА.

Программное обеспечение по выпускающей кафедре:

Наименование программного продукта	**Тип и номер лицензии**	**Примечания**
Xspider Education	Лицензионный договор 090-18/E от 27.06.2018	
MaxPatrol Education	Лицензионный договор 090-18/E от 27.06.2018	
PT Application Firewall Education	Лицензионный договор 090-18/E от 27.06.2018	
MaxPatrol SIEM	Лицензионный договор 090-18/E от 27.06.2018	
СЗИ «Блокхост-МДЗ», 4 модуля: ШДЗ, ОП, КЦ, ГУ	Договор о сотрудничестве 21 от 04.06.2018	
СЗИ «Блокхост-сеть 2.0», автономный вариант	Договор о сотрудничестве 21 от 04.06.2018	
СЗИ «Блокхост-сеть 2.0», сервер управления	Договор о сотрудничестве 21 от 04.06.2018	
СЗИ «Блокхост-сеть 2.0», сетевой вариант	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Litoria Desktop 2»	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, сервер	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, клиент Active Network Device	Договор о сотрудничестве 21 от 04.06.2018	

ПК «Efros Config Inspector 3.0» Premium, клиент сервера управления среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, клиент гипервизора среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, клиент Server Operating System	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, агент контроля целостности Windows OS	Договор о сотрудничестве 21 от 04.06.2018	
Kaspersky Endpoint Security для бизнеса - Стандартный	Договор №391/0304-18 от 26.06.2018 г.	
Infowatch Traffic Monitor Enterprise Edition 4.0	Соглашение 067-Е-ИВ/2013 о создании экспериментальной площадки (учебного класса) от 18.11.2013. Лицензия ES_Total_10_1Y до 01.01.2020	
Infowatch Endpoind Security	Соглашение 067-Е-ИВ/2013 о создании экспериментальной площадки (учебного класса) от 18.11.2013. Лицензия ES_Total_10_27-06-2017	
Infowatch Traffic Monitor Enterprise Edition 6.5	Лицензионное соглашение 932-N-ИВ/2016. Лицензия до 19.06.2019	
SearchInform Event Manager	Лицензионный договор 1726811 от 28.12.2016 на 3 года	
Astra Linux SE (Special Edition) РУСБ.10015-01 (программный продукт в формате BOX)	Лицензионный договор РБТ-14/1318-01-ВУЗ	
Специальная версия DLP системы Secure Tower	Лицензионный договор 05/17/2016-1 на 3 года	
Сервер безопасности Dallas Lock 8.0-С	лицензионный сертификат 181**-****-*57 от 01.2017	
Dallas Lock Linux	лицензионный сертификат 181**-****-**99 от 01.2017	
Сервер безопасности Dallas Lock 8.0-К	лицензионный сертификат 181**-****-*13 от 01.2017	
Dallas Lock 8.0-К(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**-****-*33 от 01.2017	
Dallas Lock 8.0-С(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**-****-*14 от 01.2017	
СЗВИ Dallas Lock 8.0	Лицензия 1909***-****-*87 от 06.2017 бессрочно	
СЗИ Secret Net 7 Клиент (автономный режим работы)	Лицензия WWIB-****-****-****-****-****-*00S от 16.01.2017	
СЗИ Secret Net 7.8 Клиент (автономный режим работы)	Лицензия WWIB-****-****-****-****-****-*001 от 05.03.2018	
СЗИ Secret Net 7.8 Сервер безопасности класса С	WWIL-****-****-****-****-****-*003 от 05.03.2018	
СЗИ Secret Net 7.8 (Клиент сетевой Режим работы)	WWIC-****-****-****-****-****-*00Q от 05.03.2018	
СЗИ Secret Net 7.8 (Терминальное подключение)	WWIA-****-****-****-****-****-*006 от 05.03.2018	
СЗИ «Secret Net LSP»	Лицензия 1****A от 16.01.2017	
СЗИ «Secret Net LSP»	Лицензия 1****5 от 05.03.2018	
Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net LSP	Ключ U*****W от 05.03.2018	
Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net	Ключ 3*****T от 05.03.2018	
Security Studio Endpoint Protection 7.6	Лицензия WWIS-****-****-****-****-****-*000 от	

	16.01.2017	
Secret Net Studio 8 Поставка Максимальная защита	Лицензия 1*****C, от 16.01.2017	
Secret Net Studio 8(модули защиты от НСД, контроля устройств)	Лицензия 1*****C, от 05.03.2018	
Secret Net Studio 8(модули персонального межсетевого экрана)	Лицензия 1*****B от 05.03.2018	
Secret Net Studio 8 (модуль «Дополнительная защита»)	Лицензия 1****D от 05.03.2018	
Secret Net Studio 8 (модуль «Защиты дисков и шифрования контейнеров»)	Лицензия 1*****C, от 05.03.2018	
Trust Access для защиты рабочих станций	Лицензия WWIM-****-****-****-****-****-*00Q от 16.01.2017	
Trust Access для защиты сервера	Лицензия WWIM-****-****-****-****-****-*00K от 16.01.2017	
СЗИ Security Code vGate R2 (Standart)	Лицензия 1****F от 16.01.2017	
СЗИ Security Code vGate R2 4.0(Enterprize Plus)	Лицензия 1****7 от 05.03.2018	
сервис прямой технической поддержки уровня «Стандартный» для СЗИ VGate	Ключ I****7 от 05.03.2018	
Secret MDM Secure Pack на 1 подключенное устройство при локальном размещении	Лицензия 1****A от 05.03.2018	
Сервис прямой технической поддержки уровня «Стандартный» для Secret MDM	Ключ B****V от 05.03.2018	
СКЗИ «Континент АП»	Лицензия WWIA-****-****-****-** от 05.03.2018	
Сервис прямой технической поддержки уровня «Стандартный» для СКЗИ Континент АП	Ключ 8****F от 05.03.2018	
Виртуальная машина «Континент»	Договор о сотрудничестве с ООО «Код безопасности» от 05.03.2018	
Dr.Web Desktop Security Suite	Договор №90/0304-18 от 22.02.2018 г.	
Statistica Basic Academic for Windows 10	Договор №ЭА-561/1701-17 от 14.12.2017 г.	
Семейство продуктов компании Microsoft • MS Windows, • MS Server, • MS Office, • MS Visio, • MS Project	Договор №ЭД-644/0304-17 от 21.12.2017 г.	

Обучающимся инвалидам и лицам с ограниченными возможностями здоровья предоставляются печатные и электронные образовательные ресурсы в формах, адаптированных к ограничениям их здоровья.

При инклюзивном обучении лиц с ОЗВ предоставляется возможность использовать следующие материально-технические средства:

для студентов с ОВЗ по зрению предусматривается применение средств преобразования визуальной информации в аудио и тактильные сигналы, таких как, брайлевская компьютерная техника, электронные лупы, видеоувеличители, программы невизуального доступа к информации, программы-синтезаторов речи;

для студентов с ОВЗ по слуху предусматривается применение сурдотехнических средств, таких как, системы беспроводной передачи звука, техники для усиления звука, видеотехника, мультимедийная техника и другие средства передачи информации в доступных формах;

для студентов с нарушениями опорно-двигательной функции предусматривается применение специальной компьютерной техники с соответствующим программным обеспечением, в том числе, специальные возможности операционных систем, таких, как экранная клавиатура и альтернативные устройства ввода информации.

При реализации программ с использованием дистанционных образовательных технологий используется действующая в университете электронно-образовательная среда. Разработка учебных материалов осуществляется с учетом возможностей предоставления контента в различных формах – визуально, аудиально. Разрабатываемый нетекстовый контент преобразуется в альтернативные формы, удобные для различных категорий пользователей без потери данных и структуры. Предусматривается возможность масштабирования текста, применения экранной клавиатуры. В образовательном процессе активно используются различные формы организации on-line и off-line занятий, в том числе, вебинары, виртуальные лекции, обсуждение вопросов освоения дисциплины в рамках форумов, выполнение совместных работ с применением технологий проектной деятельности с возможностью включения всех участников образовательного процесса в активную работу.

2. В рабочей программе дисциплин физическая культура и спорт, элективные дисциплины по физической культуре и спорту по очной форме обучения для набора 2019 года установить следующую трудоемкость дисциплины по видам работ (раздел 3):

Вид работы	Трудоемкость часов						
	1	2	3	4	5	6	Всего часов
Физическая культура и спорт							
Общая трудоемкость	72						72
Лекции (Л)	10						10
Практические занятия (ПЗ)	28						28
Самостоятельная работа студентов (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям, самостоятельное изучение разделов)	23						23
КСР	2						2
Подготовка и сдача зачета	9						9
Элективные дисциплины по физической культуре и спорту							
Общая трудоемкость	12	64	63	63	63	63	328
Лекции (Л)							
Практические занятия (ПЗ)	12	54	54	54	54	54	282
Самостоятельная работа студентов (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям, самостоятельное изучение разделов)		1					1
Подготовка и сдача зачета		9	9	9	9	9	45

3. В учебные планы начала года обучения 2017, 2018 внести следующие изменения:

3.1. Включить факультативную дисциплину «Нейрокомпьютеры», разработать рабочую программу дисциплины.

3.2. Установить изменение зачетных единиц, или распределения часов по видам занятий, или формы контроля по следующим дисциплинам:

№	Дисциплина	Семестр	Лекции	Лабораторные работы	Практические занятия	СРС	Контроль
1.	Проектирование защищенных компьютерных систем	7	12	20	4	27	За
2.	Техническая защита информации	6	30	28	14	36	Э
3.	Стандарты информационной безопасности и аудит	6	18	12	12	66	Э
4.	Информационные техно-	6	20	20		23	За

	логии						
5.	Теория принятия решений	6	18	12	6	63	За
6.	Теория нечетких систем	5	18	12	6	27	За
7.	Телекоммуникационные технологии	5	20	12	4	63	За
8.	Организационное и правовое обеспечение информационной безопасности	5	24	16	10	58	Э
9.	Культура делового человека	6	8		12	7	За
10.	Нейрокомпьютеры	6	8	12	2	5	За

4. В учебный план начала года обучения 2019 внести следующие изменения:

4.1. Включить факультативную дисциплину «Нейрокомпьютеры», разработать рабочую программу дисциплины.

4.2. Исключить дисциплины по выбору: Политология/Прикладная политология, Современные банковские технологии/Безопасность систем электронной торговли.

4.3. Установить изменение зачетных единиц, или распределения часов по видам занятий, или формы контроля по следующим дисциплинам:

№	Дисциплина	Семестр	Лекции	Лабораторные работы	Практические занятия	КСР	СРС	Контроль
1.	Теория информации	4	18		20		25	З
2.	Техническая защита информации	6	24	24	8		52	Э
3.	Управление информационной безопасностью	7	20	16	8		51	З
4.	Компьютерно-техническая экспертиза	7	16	12	8		27	З
5.	Информационное право	7	18	12	10		59	З
6.	Защита информационных процессов в компьютерных системах	7	30	28	8		78	Э
7.	Программно-аппаратные средства защиты информации	5	30	28	10		40	Э
8.	Сети и системы передачи информации	6	30	28	6		80	Э
9.	Комплексная система защиты информации на предприятии	7	24	20	8		56	Э
10.	Политология/Прикладная политология	3	Исключена					
11.	Электрорадиоизмерения/ Основы метрологии	3	10	12	2		111	ЗаО
12.	Методы оптимизации	3	18		20		61	За
13.	Теория автоматов	3	20		20		59	За
14.	Информатика	1	30	32	6	2	110	Э
15.	Языки программирования	1	20	20	6	2	51	За
16.	Русский язык	1	20		20	2	21	За
17.	Введение в профессиональную деятельность	1	10		8		45	За
18.	Основы информационной безопасности	4	26	24	8		122	Э, КР
19.	Криптографические методы защиты информа-	4	20	20	8		51	За

	ции							
20.	Электроника и схемотехника	4	30	24	6		84	Э
21.	Социология/ Социология управления	4	14		10		39	За
22.	Компьютерная графика/ Web-дизайн	4	20	20			95	ЗаО
23.	Моделирование технических систем/ Имитационное моделирование	8	20	20	6		62	Э
24.	Психология воздействия/ Специальные информационные технологии	6	20	8	16		91	ЗаО
25.	Современные банковские технологии/ Безопасность систем электронной торговли	8	Исключена					
26.	Теория принятия решений в системах защиты информации/ Модели и методы принятия решений в системах защиты информации	8	14	12	16		76	Э
27.	Катастрофоустойчивость информационных систем/ Безопасность критически важных информационных систем	8	12	12	6		69	За
28.	Математическая логика и теория алгоритмов	2	20		20		59	За
29.	Философия	2	36		20	4	48	Э
30.	История	1	36		20	4	48	Э
31.	Линейная алгебра и аналитическая геометрия	1	32		30	4	78	Э
32.	Математический анализ	1 2	28 28		30 30	4 4	73 46	За Э
33.	Дискретная математика	2	30		20	4	81	ЗаО
34.	Физика	3 4	26 26	24 24	22 24		72 70	РГР Э
35.	Физическая культура и спорт	1	10		28	2	23	За
36.	Элективные дисциплины по физической культуре и спорту	1 2 3 4 5 6			12 54 54 54 54 54		1	 За За За За За
37.	Культура делового человека	5	8		12		7	За
38.	Нейрокомпьютеры	7	8	12	2		5	За

Председатель научно-методического совета по УГСН 10.00.00 Информационная безопасность — В.И. Васильев

Начальник отдела образовательных программ и методического обеспечения программ бакалавриата и специалитета — Д.Ф. Муфаззалов

ВЫПИСКА
из протокола заседания
научно-методического совета по УГСН 10.00.00
Информационная безопасность
№ 9 от 15 мая 2020 г.

СЛУШАЛИ: доцента кафедры ВТиЗИ Дуленко В.А. о внесении изменений и дополнений в основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», реализуемой в очной форме на 2020-2021 учебный год.

ПОСТАНОВИЛИ: утвердить следующие изменения и дополнения в основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», реализуемой в очной форме на 2020-2021 учебный год:

1. Пункт 5.2 ОПОП изложить в следующей редакции:

5.2 Учебно-методическое и информационное обеспечение

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к следующим электронно-библиотечным системам (ЭБС «Лань» http://e.lanbook.com/ , ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru, Консорциум аэрокосмических вузов России http://elsau.ru/, Электронная коллекция образовательных ресурсов УГАТУ http://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus), содержащим все издания основной литературы, перечисленные в рабочих программах дисциплин (модулей), практик, НИР сформированным на основании прямых договорных отношений с правообладателями.

Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивают возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет, как на территории университета, так и вне ее.

Обучающимся обеспечен доступ к электронным ресурсам и информационным справочным системам, информация о которых представлена на сайте: http://www.library.ugatu.ac.ru/.

УГАТУ обеспечен необходимым комплектом лицензионного программного обеспечения. Информация об используемом программном обеспечении приведена на сайте УГАТУ (http://it.ugatu.su/license.html – программное обеспечение, общее по вузу) и в рабочих программах дисциплин, программах практик, программе ГИА.

Программное обеспечение по выпускающей кафедре:

Наименование программного продукта	Тип и номер лицензии	Примечания
Xspider Education	Лицензионный договор 090-18/E от 27.06.2018	
MaxPatrol Education	Лицензионный договор 090-18/E от 27.06.2018	
PT Application Firewall Education	Лицензионный договор 090-18/E от 27.06.2018	
MaxPatrol SIEM	Лицензионный договор 090-18/E от 27.06.2018	
СЗИ «Блокхост-МДЗ», 4 модуля: ШДЗ, ОП, КЦ, ГУ	Договор о сотрудничестве 21 от 04.06.2018	
СЗИ «Блокхост-сеть 2.0», автономный вариант	Договор о сотрудничестве 21 от 04.06.2018	
СЗИ «Блокхост-сеть 2.0», сервер управления	Договор о сотрудничестве 21 от 04.06.2018	
СЗИ «Блокхост-сеть 2.0», сетевой вариант	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Litoria Desktop 2»	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, сервер	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premi-	Договор о сотрудничестве 21 от 04.06.2018	

um, клиент Active Network Device		
ПК «Efros Config Inspector 3.0» Premium, клиент сервера управления среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, клиент гипервизора среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, клиент Server Operating System	Договор о сотрудничестве 21 от 04.06.2018	
ПК «Efros Config Inspector 3.0» Premium, агент контроля целостности Windows OS	Договор о сотрудничестве 21 от 04.06.2018	
Kaspersky Endpoint Security для бизнеса - Стандартный	Договор №391/0304-18 от 26.06.2018 г.	
Infowatch Traffic Monitor Enterprise Edition 4.0	Соглашение 067-Е-ИВ/2013 о создании экспериментальной площадки (учебного класса) от 18.11.2013. Лицензия ES_Total_10_1Y до 01.01.2020	
Infowatch Endpoind Security	Соглашение 067-Е-ИВ/2013 о создании экспериментальной площадки (учебного класса) от 18.11.2013. Лицензия ES_Total_10_27-06-2017	
Infowatch Traffic Monitor Enterprise Edition 6.5	Лицензионное соглашение 932-N-ИВ/2016. Лицензия до 19.06.2019	
SearchInform Event Manager	Лицензионный договор 1726811 от 28.12.2016 на 3 года	
Astra Linux SE (Special Edition) РУСБ.10015-01 (программный продукт в формате BOX)	Лицензионный договор РБТ-14/1318-01-ВУЗ	
Специальная версия DLP системы Secure Tower	Лицензионный договор 05/17/2016-1 на 3 года	
Сервер безопасности Dallas Lock 8.0-С	лицензионный сертификат 181**-****-*57 от 01.2017	
Dallas Lock Linux	лицензионный сертификат 181**-****-**99 от 01.2017	
Сервер безопасности Dallas Lock 8.0-К	лицензионный сертификат 181**-****-*13 от 01.2017	
Dallas Lock 8.0-К(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**-****-*33 от 01.2017	
Dallas Lock 8.0-С(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**-****-*14 от 01.2017	
СЗВИ Dallas Lock 8.0	Лицензия 1909***-****-*87 от 06.2017 бессрочно	
СЗИ Secret Net 7 Клиент (автономный режим работы)	Лицензия WWIB-****-****-****-****-****-*00S от 16.01.2017	
СЗИ Secret Net 7.8 Клиент (автономный режим работы)	Лицензия WWIB-****-****-****-****-****-*001 от 05.03.2018	
СЗИ Secret Net 7.8 Сервер безопасности класса С	WWIL-****-****-****-****-****-*003 от 05.03.2018	
СЗИ Secret Net 7.8 (Клиент сетевой Режим работы)	WWIC-****-****-****-****-****-*00Q от 05.03.2018	
СЗИ Secret Net 7.8 (Терминальное подключение)	WWIA-****-****-****-****-****-*006 от 05.03.2018	
СЗИ «Secret Net LSP»	Лицензия 1****A от 16.01.2017	
СЗИ «Secret Net LSP»	Лицензия 1****5 от 05.03.2018	
Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net LSP	Ключ U*****W от 05.03.2018	
Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net	Ключ 3*****T от 05.03.2018	

Security Studio Endpoint Protection 7.6	Лицензия WWIS-****-****-****-****-****-*000 от 16.01.2017	
Secret Net Studio 8 Поставка Максимальная защита	Лицензия 1*****C, от 16.01.2017	
Secret Net Studio 8(модули защиты от НСД, контроля устройств)	Лицензия 1*****C, от 05.03.2018	
Secret Net Studio 8(модули персонального межсетевого экрана)	Лицензия 1*****B от 05.03.2018	
Secret Net Studio 8 (модуль «Дополнительная защита»)	Лицензия 1****D от 05.03.2018	
Secret Net Studio 8 (модуль «Защиты дисков и шифрования контейнеров»)	Лицензия 1*****C, от 05.03.2018	
Trust Access для защиты рабочих станций	Лицензия WWIM-****-****-****-****-****-*00Q от 16.01.2017	
Trust Access для защиты сервера	Лицензия WWIM-****-****-****-****-****-*00K от 16.01.2017	
СЗИ Security Code vGate R2 (Standart)	Лицензия 1****F от 16.01.2017	
СЗИ Security Code vGate R2 4.0(Enterprize Plus)	Лицензия 1****7 от 05.03.2018	
сервис прямой технической поддержки уровня «Стандартный» для СЗИ VGate	Ключ I****7 от 05.03.2018	
Secret MDM Secure Pack на 1 подключенное устройство при локальном размещении	Лицензия 1****A от 05.03.2018	
Сервис прямой технической поддержки уровня «Стандартный» для Secret MDM	Ключ B****V от 05.03.2018	
СКЗИ «Континент АП»	Лицензия WWIA-****-****-****-** от 05.03.2018	
Сервис прямой технической поддержки уровня «Стандартный» для СКЗИ Континент АП	Ключ 8****F от 05.03.2018	
Виртуальная машина «Континент»	Договор о сотрудничестве с ООО «Код безопасности» от 05.03.2018	
Dr.Web Desktop Security Suite	Договор №90/0304-18 от 22.02.2018 г.	
Statistica Basic Academic for Windows 10	Договор №ЭА-561/1701-17 от 14.12.2017 г.	
Семейство продуктов компании Microsoft • MS Windows, • MS Server, • MS Office, • MS Visio, • MS Project	Договор №ЭД-644/0304-17 от 21.12.2017 г.	

Обучающимся инвалидам и лицам с ограниченными возможностями здоровья предоставляются печатные и электронные образовательные ресурсы в формах, адаптированных к ограничениям их здоровья.

При инклюзивном обучении лиц с ОВЗ предоставляется возможность использовать следующие материально-технические средства:

для студентов с ОВЗ по зрению предусматривается применение средств преобразования визуальной информации в аудио и тактильные сигналы, таких как, брайлевская компьютерная техника, электронные лупы, видеоувеличители, программы невизуального доступа к информации, программы-синтезаторов речи;

для студентов с ОВЗ по слуху предусматривается применение сурдотехнических средств, таких как, системы беспроводной передачи звука, техники для усиления звука, видеотехника, мультимедийная техника и другие средства передачи информации в доступных формах;

для студентов с нарушениями опорно-двигательной функции предусматривается применение специальной компьютерной техники с соответствующим программным обеспечением, в том

числе, специальные возможности операционных систем, таких, как экранная клавиатура и альтернативные устройства ввода информации.

При реализации программ с использованием дистанционных образовательных технологий используется действующая в университете электронно-образовательная среда. Разработка учебных материалов осуществляется с учетом возможностей предоставления контента в различных формах – визуально, аудиально. Разрабатываемый нетекстовый контент преобразуется в альтернативные формы, удобные для различных категорий пользователей без потери данных и структуры. Предусматривается возможность масштабирования текста, применения экранной клавиатуры. В образовательном процессе активно используются различные формы организации on-line и off-line занятий, в том числе, вебинары, виртуальные лекции, обсуждение вопросов освоения дисциплины в рамках форумов, выполнение совместных работ с применением технологий проектной деятельности с возможностью включения всех участников образовательного процесса в активную работу.

Председатель научно-методического совета по УГСН 10.00.00 Информационная безопасность — В.И. Васильев

Начальник отдела образовательных программ и методического обеспечения программ бакалавриата и специалитета — Д.Ф. Муфаззалов

ВЫПИСКА

из протокола заседания № 9 научно-методического совета
по УГСН 10.00.00 Информационная безопасность
от 27 мая 2021 г.

СЛУШАЛИ: доцента кафедры ВТиЗИ Дуленко В.А. о внесении изменений и дополнений в основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем» для года начала подготовки с 2018 по 2020.

ПОСТАНОВИЛИ: утвердить следующие изменения и дополнения в основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем» для года начала подготовки с 2018 по 2020.

1. В основную профессиональную образовательную программу добавить пункты:

4.6 Практическая подготовка.

Образовательная деятельность в форме практической подготовки организована при реализации дисциплин и практик, предусмотренных учебным планом. Реализация компонентов образовательной программы в форме практической подготовки осуществляется путем чередования с реализацией иных компонентов образовательной программы в соответствии с календарным учебным графиком и учебным планом. Практическая подготовка при реализации дисциплин организуется путем проведения практических занятий, практикумов, лабораторных работ, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.7 Календарный план воспитательной работы

Перечень мероприятий воспитательной работы, планируемых к проведению в 2021 г. представлен на сайте УГАТУ.

4.8 Программа воспитания обучающихся.

При реализации данной образовательной программы предусматривается воспитательная работа с обучающимися с целью:

- формирования у обучающихся духовных, социальных и профессиональных ценностей;
- обогащения личностного и социального опыта обучающихся;
- повышения степени вовлеченности обучающихся в организацию и проведение мероприятий воспитательного характера;
- создания полноценной социально-педагогической воспитывающей среды и условий для самореализации студентов;
- развития традиций корпоративной культуры университета;
- повышения эффективности и качества реализуемых мероприятий;
- выпуска конкурентоспособных специалистов, обладающих высоким уровнем социально-личностных и профессиональных компетенций.

Рабочая программа воспитания обучающихся УГАТУ представлен на сайте УГАТУ.

Председатель научно-
методического совета по УГСН
10.00.00 Информационная безопасность

В.И. Васильев

Выписка из протокола № 11 заседания кафедры от « 08 » 04. 2022 года
по направлению 10.03.01 «Информационная безопасность»,
направленность (профиль, специализация) «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»,
форма обучения очная

СЛУШАЛИ: доц. каф. Даянова И.С. о внесении изменений и дополнений в основную профессиональную образовательную программу по направлению подготовки 10.03.01 «Информационная безопасность», профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)».

ПОСТАНОВИЛИ:

✓ утвердить отсутствие изменений и дополнений в основную профессиональную образовательную программу по направлению подготовки 10.03.01 «Информационная безопасность», профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»;
состав комплекта лицензионного программного обеспечения не изменился; состав современных профессиональных баз данных и информационных справочных систем не изменился.

Заведующий кафедрой ВТиЗИ _____ Картак В.М.