

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



Н.К. Криони

2017 г.

Основная профессиональная образовательная программа

Уровень подготовки: высшее образование – специалитет

Специальность

10.05.05 «Безопасность информационных технологий
в правоохранительной сфере»
(код и наименование специальности)

Специализация

Технологии защиты информации в правоохранительной сфере
(наименование специализации)

Квалификация (степень) выпускника

Специалист

Форма обучения

очная

Год начала подготовки – 2013

Разработана в соответствии с
ФГОС ВПО Приказ № 132
Дата утверждения 01.02.2011 г.

Актуализирована в соответствии с
ФГОС ВО. Приказ №1612
Дата утверждения 19.12.2016 г.

Уфа 2017

Разработчики:

Доцент кафедры вычислительной
техники и защиты информации

В.А. Дуленко

Основная профессиональная образовательная программа обсуждена на кафедре
вычислительной техники и защиты информации
19 января 2017., протокол № 8.

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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере
19 января 2017., протокол № 5.

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
26 января 2017., протокол № 15.

Начальник ООПБС

Г.Т. Гарипова

СОДЕРЖАНИЕ

1. Общие положения	4
1.1. Основная профессиональная образовательная программа (определение)	4
1.2. Нормативные документы для разработки ОПОП ВО	4
1.3.1. Цели ОПОП ВО	5
1.3.2. Срок освоения	5
1.3.3. Трудоемкость	5
1.3.4. Образовательные технологии	5
1.3.5. Тип программы	5
1.4. Язык реализации ОПОП ВО	5
1.5. Требования к уровню подготовки, необходимому для освоения ОПОП ВО	6
2. Характеристика профессиональной деятельности	6
2.1. Область профессиональной деятельности выпускника	6
2.2. Объекты профессиональной деятельности выпускника	6
2.3. Виды профессиональной деятельности выпускника	6
2.4. Задачи профессиональной деятельности выпускника	7
3. Требования к результатам освоения ОПОП ВО	7
3.1. Компетенции выпускника, формируемые в результате освоения программы	8
3.2. Матрица соответствия дисциплин и компетенций, формируемых в результате освоения ОПОП ВО	12
3.3. Матрица соответствия компетенций, предусмотренных ОПОП, разработанной в соответствии с ФГОС ВПО, компетенциям ФГОС ВО	12
4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ОПОП ВО	12
4.1. Календарный учебный график	19
4.2. Учебный план	19
4.3. Рабочие программы дисциплин (модулей)	19
4.4. Программы практик и научно-исследовательской работы	19
4.4.1. Программа практик	19
4.4.2. Программа научно-исследовательской работы	21
5. Фактическое ресурсное обеспечение	21
5.1. Кадровое обеспечение	21
5.2. Учебно-методическое и информационное обеспечение	21
5.3. Материально-техническое обеспечение	24
6. Характеристики среды вуза, обеспечивающие развитие общекультурных и социально-личностных компетенций выпускников	25
7. Нормативно-методическое обеспечение системы оценки качества освоения обучающимися ОПОП ВО	29
7.1. Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации	29
7.2. Программа государственной итоговой аттестации	29
8. Условия реализации образовательной программы лицами с ограниченными возможностями здоровья	29
9. Другие нормативно-методические документы и материалы, обеспечивающие качество подготовки обучающихся	29
Пояснительная записка к программе по учету требований профессиональных стандартов (ПС)	30
ПРИЛОЖЕНИЯ	45

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 специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» и специализации «Технологии защиты информации в правоохранительной сфере» представляет собой систему документов, разработанную на основе Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по соответствующей специальности, 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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, утвержденный приказом Министерства образования и науки Российской Федерации 19 декабря 2016 г. № 1612;
4. Приказ Минобороны РФ и Министерства образования и науки РФ от 10 июля 2009 г. № 666/249 «Об организации деятельности учебных военных центров, факультетов военного обучения и военных кафедр при федеральных государственных образовательных учреждениях высшего профессионального образования»;
5. 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»;
6. 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);
7. Нормативно-методические документы Министерства образования и науки Российской Федерации;
8. Примерная основная образовательная программа, утвержденная УМО по специальности «Безопасность информационных технологий в правоохранительной сфере» (носит рекомендательный характер);
9. Устав УГАТУ и другие локальные нормативные акты университета.

1.3. Общая характеристика ОПОП ВО

1.3.1. Цели ОПОП ВО

ОПОП ВО по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализация «Технологии защиты информации в правоохранительной сфере» 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 данной специальности.

В области обучения целью ООП ВО специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализация «Технологии защиты информации в правоохранительной сфере» 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 специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализация «Технологии защиты информации в правоохранительной сфере» 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 специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» (очная форма обучения) – 5 лет.

1.3.3. Трудоемкость

Трудоемкость освоения обучающимся данной ОПОП ВО за весь период обучения в соответствии с ФГОС ВО по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» составляет 300 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 специалитета.

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 специалиста 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 ВПО по данной специальности область профессиональной деятельности специалиста со специализацией «Технологии защиты информации в правоохранительной сфере» включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с информационно-аналитическим обеспечением правоохранительной деятельности, обеспечением безопасности информационных технологий в правоохранительной сфере в условиях существования угроз в информационной сфере.

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

- академические, государственные органы, ведомственные и частные научно-исследовательские и производственные организации, связанные с решением проблем, связанных с обеспечением безопасности информационных технологий;
- 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 данной специальности являются: информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления.

Конкретный объект профессиональной деятельности может уточняться высшим учебным заведением совместно с заинтересованными участниками образовательного процесса с учетом реализуемой специализации.

2.3. Виды профессиональной деятельности выпускника

В соответствии с ФГОС ВО по данной специальности выпускник со специализацией «Технологии защиты информации в правоохранительной сфере» подготовлен к следующим видам профессиональной деятельности: эксплуатационной; правоохранительной; организационно-управленческой; информационно-аналитической; научно-исследовательской; проектно-технологической; экспертной, педагогической.

Конкретные виды профессиональной деятельности, к которым готовится специалист, определяются высшим учебным заведением совместно с обучающимися, научно-педагогическими работниками высшего учебного заведения и объединениями работодателей.

В соответствии с запросами рынка труда выпускник со специализацией «Технологии защиты информации в правоохранительной сфере» 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 специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» (по специализации «Технологии защиты информации в правоохранительной сфере») должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности и профилем ОПОП ВО:

1) эксплуатационная деятельность:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации;
- участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации;
- администрирование подсистем обеспечения информационной безопасности на объекте;

2) правоохранительная деятельность:

- обеспечение законности и правопорядка;
- предупреждение, выявление, пресечение, участие в раскрытии преступлений и иных правонарушений;
- информационно-аналитическое и информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий;

3) организационно-управленческая деятельность:

- организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
- разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;
- организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач;

4) информационно-аналитическая деятельность:

- получение и обработка поступающей информации;
- анализ и отбор данных и сведений для формирования информационных ресурсов;
- обработка акустических и видеозаписей, фотоматериалов с целью получения информации, необходимой для формирования ресурсов и оперативного реагирования;
- формирование автоматизированных, в том числе справочных, оперативно-розыскных, криминалистических учетов;
- осуществление информационного и оперативно-аналитического поиска;
- осуществление оперативно-розыскного анализа, идентификации, диагностики и прогнозирования, криминалистической диагностики;
- информационно-аналитическое обеспечение оперативно-розыскных мероприятий и следственных действий;
- информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий;

– противодействие деструктивным и негативным информационно-психологическим воздействиям;

5) научно-исследовательская деятельность:

– сбор, изучение, систематизация и обобщение научно-технической информации, отечественного и зарубежного опыта по проблемам информационно -аналитической работы и обеспечения защиты информации;

– анализ прикладных проблем информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, защиты информации и обеспечения безопасности информационных технологий;

– разработка заданий, планов, программ проведения прикладных научных исследований и технических разработок;

– проведение экспериментов по заданным методикам;

– выполнение прикладных научных исследований, подготовка отчетов, докладов;

6) проектно-технологическая деятельность:

– сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;

– участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации;

– адаптация к защищаемым объектам современных информационных технологий и методов обеспечения безопасности информации на основе отечественных и международных стандартов;

7) экспертная деятельность:

– производство судебных компьютерных экспертиз;

8) педагогическая деятельность:

– преподавание в организациях, осуществляющих образовательную деятельность, дисциплин (модулей) в области информационных технологий и информационной безопасности.

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 понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы (ОК-1);

2. Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма (ОК-2);

3. Способность ориентироваться в политических, социальных и экономических процессах (ОК-3);

4. Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета (ОК-4);

5. Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-5);

6. Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния (ОК-6);

7. Способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии (ОК-7);
8. Способность принимать организационно-управленческие решения (ОК-8);
9. Способность организовывать свою жизнь в соответствии с социально значимыми представлениями о здоровом образе жизни (ОК-9);
10. Способность осуществлять письменную и устную коммуникацию на русском языке (ОК-10);
11. Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков (ОК-11);
12. Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12).

Общепрофессиональные компетенции:

1. Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1);
2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации (ОПК-2).

Профессиональные компетенции:

Эксплуатационная деятельность:

1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1);
2. Способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2);
3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации (ПК-3);
4. Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации (ПК-4);
5. Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5);
6. Способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации (ПК-6).

Правоохранительная деятельность:

7. Способность выполнять служебные обязанности по охране общественного порядка (ПК-7);
8. Способность участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений (ПК-8);
9. Способность применять при выполнении профессиональных задач криминалистическую технику и специальные технические средства, используемые, в деятельности правоохранительного органа, в интересах которого осуществляется подготовка специалистов (ПК-9);
10. Способность правильно и полно отражать результаты профессиональной деятельности в служебной документации (ПК-10);

11. Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в военное время (ПК-11);

12. Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач (ПК-12).

Организационно-управленческая деятельность:

13. Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13);

14. Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов (ПК-14);

15. Способность принимать управленческие решения (ПК-15);

16. Способность осуществлять документационное обеспечение управленческой деятельности (ПК-16);

17. Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов (ПК-17);

18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации (ПК-18);

19. Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности (ПК-19).

Информационно-аналитическая деятельность:

20. Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач (ПК-20);

21. Способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы (ПК-21);

22. Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22);

23. Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику (ПК-23);

24. Способность осуществлять противодействие деструктивным и негативным информационно-психологическим воздействиям (ПК-24).

Научно-исследовательская деятельность:

25. Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования (ПК-25);

26. Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты (ПК-26);

27. Способность готовить научные отчеты по результатам выполненных исследований (ПК-27).

Проектно-технологическая деятельность:

28. Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны (ПК-28);

29. Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации (ПК-29);

30. Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации (ПК-30);

31. Способность принимать участие в создании системы защиты информации на объекте информатизации (ПК-31).

Экспертная деятельность:

32. Способность осуществлять производство судебных компьютерных экспертиз (ПК-32).

Педагогическая деятельность:

33. Способность проектировать, осуществлять, контролировать и оценивать результаты образовательного процесса по дисциплинам (модулям) в области информационных технологий и информационной безопасности в организациях, осуществляющих образовательную деятельность (ПК-33).

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).

Военные профессиональные компетенции по военно-учетной специальности 461300 «Эксплуатация и ремонт радиоэлектронного оборудования самолетов, вертолетов и авиационных ракет»

1. Способность и готовность на основе знаний героического военного прошлого народов нашей страны и истории их борьбы за свободу и независимость воспитывать у личного состава ВС РФ патриотизм, высокий моральный дух, героизм, мужество, инициативу и стойкость в бою, веру в свое оружие и отечественное военное искусство, Родину и непреклонную волю к победе (ВПК.ОК-1);

2. Способность действовать в соответствии с основными нормативными правовыми актами, регламентирующими полномочия органов военного управления, воинскую обязанность, комплектование ВС РФ военнослужащими, порядок прохождения военной службы (ВПК.ОК-2);

3. Способность понимать основы применения ВС РФ и других войск (ВПК.ОК-3);

4. Способность применять положения общевоинских уставов ВС РФ при обеспечении твердой воинской дисциплины и поддержании внутреннего порядка в подразделении (ВПК.ОПК-1);

5. Способность применять штатное стрелковое оружие (ВПК.ОПК-2);

6. Способность организовывать среди личного состава подразделения работы по сохранению здоровья, профилактике травматизма и отравлений, уметь оказывать первую медицинскую помощь при ранениях, ожогах, обморожениях, отравлениях в очагах массового поражения и других травмах (ВПК.ОПК-3);

7. Способность организовывать и проводить учебные занятия с подчиненными (ВПК.ОПК-4);

8. Способность соблюдать требования безопасности при эксплуатации штатных типов вооружения и военной техники (ВПК.ОПК-5);

9. Способность организовать боевую и специальную подготовку подчиненного личного состава, а также проводить мероприятия по поддержанию боевой и мобилизационной готовности войск (ВПК.ОПК-6);

10. Способность оценивать обстановку, самостоятельно принимать обоснованное решение, ставить задачи частям и подразделениям по реализации принятого решения и контролировать их выполнение (ВПК.ОПК-7);

11. Способность применять знания тактики и топографии при оформлении рабочей карты командира и ведении других боевых документов (ВПК.ОПК-8);

12. Способность выполнять работы по техническому обслуживанию систем и устройств боевых воздушных судов (ВПК.ПК-1);

13. Способность проводить анализ работы систем и устройств авиационной техники (ВПК.ПК-2);

Способность осуществлять подготовку к полетам (предварительную, предполетную, к повторному полету, послеполетную), день работ на авиационной технике (ВПК.ПК-3).

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

В процессе актуализации ОПОП установлено соответствие компетенций, предусмотренных ОПОП, разработанной в соответствии с ФГОС ВПО, компетенциям ФГОС ВО.

Компетенции ФГОС ВПО		Компетенции ФГОС ВО	
Код	Наименование	Код	Наименование
ОК-1	Способность понимать и анализировать мировоззренческие, социально и лично значимые философские проблемы, вопросы ценностномотивационной ориентации; значение гуманистических ценностей, свободы и демократии	ОК-1	Способность понимать и анализировать мировоззренческие, социально и лично значимые философские проблемы
ОК-8	Способность владеть культурой научного мышления, анализировать логику рассуждений и высказываний		
ОК-2	Способность понимать движущие силы и закономерности исторического процесса, уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социально-культурные различия	ОК-2	Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма
ОК-3	Способность ориентироваться в политических и социальных процессах, использовать знания и методы гуманитарных и социальных наук при решении профессиональных задач	ОК-3	Способность ориентироваться в политических, социальных и экономических процессах
ОК-4	Способность понимать социальную значимость своей профессии, цель и смысл государственной службы, выполнять гражданский и служебный долг, профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	ОК-4	Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета
ОК-11	Способность соблюдать требования законов и иных нормативных правовых актов, нетерпимо относиться к коррупционному поведению		

ОК-5	Способность к толерантному поведению, к социальному и профессиональному взаимодействию с учетом этнокультурных и конфессиональных различий, к работе в коллективе, кооперации с коллегами, к предупреждению и конструктивному разрешению конфликтных ситуаций в процессе профессиональной деятельности	ОК-5	Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности
ОК-6	Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психического состояния	ОК-6	Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психического состояния
ОК-9	Способность осуществлять устную и письменную коммуникации на русском языке, логически верно, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии	ОК-7	Способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии
ОК-8	Способность владеть культурой научного мышления, анализировать логику рассуждений и высказываний		
ОК-7	Способность проявлять инициативу, в том числе в ситуациях риска, принимать ответственность за свои решения в рамках профессиональной компетенции, креативно мыслить, творчески решать профессиональные задачи	ОК-8	Способность принимать организационно-управленческие решения
ОК-13	Способность анализировать свои возможности, самосовершенствоваться и повышать свой интеллектуальный и общекультурный уровень, профессиональную квалификацию, развивать социальные и профессиональные компетенции, изменять вид и характер своей профессиональной деятельности, адаптироваться к изменяющимся социокультурным условиям и меняющимся условиям профессиональной деятельности		
ОК-12	Способность организовать свою жизнь в соответствии с социально значимыми представлениями о здоровом образе жизни, достигать и поддерживать должный уровень физической подготовленности, необходимой для обеспечения социальной активности и полноценной профессиональной деятельности	ОК-9	Способность организовывать свою жизнь в соответствии с социально значимыми представлениями о здоровом образе жизни
ОК-9	Способность осуществлять устную и письменную коммуникации на русском языке, логически верно, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии	ОК-10	Способность осуществлять письменную и устную коммуникацию на русском языке
ОК-10	Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков	ОК-11	Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков

ПК-25	Способность работать с различными источниками информации, информационными ресурсами и технологиями; использовать в профессиональной деятельности прикладные программные средства, современные средства телекоммуникации, автоматизированные информационно-справочные, информационно-поисковые системы, базы данных, автоматизированные рабочие места; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	ОК-12	Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
ОК-14	Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	ОПК-1	Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач
ПК-8	Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2	Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации
ПК-1	Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ПК-1	Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз
ПК-38	Способность принимать участие в создании системы защиты информации на объекте информатизации		
ПК-2	Способность осваивать новые образцы программных комплексов, технических средств и информационных технологий, выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств обработки и защиты информации, эксплуатировать и администрировать подсистемы обеспечения информационной безопасности на объекте	ПК-2	Способность применять технические и программно-аппаратные средства обработки и защиты информации
ПК-3	Способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности, применять программные и технические средства системного, прикладного и специального назначения, в том числе средства защиты информации, составляющей государственную тайну		
ПК-4	Способность выбирать и применять программно-аппаратные и криптографические средства защиты информации		

ПК-5	Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну	ПК-3	Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации
ПК-7	Способность проводить анализ эффективности системы защиты информации		
ПК-6	Способность участвовать в исследовании и проверке объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации	ПК-4	Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации
ПК-30	Способность проводить анализ состояния безопасности информации на объектах и в отдельных системах с использованием отечественных и зарубежных стандартов		
ПК-2	Способность осваивать новые образцы программных комплексов, технических средств и информационных технологий, выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств обработки и защиты информации, эксплуатировать и администрировать подсистемы обеспечения информационной безопасности на объекте	ПК-5	Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния
		ПК-6	Способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации
ПК-9	Способность выполнять служебные обязанности по обеспечению законности и правопорядка	ПК-7	Способность выполнять служебные обязанности по охране общественного порядка
ПК-10	Способность участвовать в пресечении и раскрытии правонарушений и преступлений в качестве специалиста	ПК-8	Способность участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений
ПК-11	Способность осуществлять информационно-аналитическое обеспечение оперативно-розыскных мероприятий, следственных действий, управленческой деятельности		
ПК-13	Способность реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений		
ПК-14	Способность применять при выполнении профессиональных задач криминалистическую и специальную технику, используемую в деятельности правоохранительных органов	ПК-9	Способность применять при выполнении профессиональных задач криминалистическую технику и специальные технические средства, используемые, в деятельности правоохранительного органа, в интересах которого осуществляется подготовка специалистов
ПК-15	Способность правильно и полно отражать результаты профессиональной деятельности в служебной документации	ПК-10	Способность правильно и полно отражать результаты профессиональной деятельности в служебной документации
ПК-17	Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в	ПК-11	Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в

	военное время, оказывать первую медицинскую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач	ПК-12	в военное время Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач
ПК-1	Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ПК-13	Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов
ПК-5	Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну		
ПК-24	Способность соблюдать в профессиональной деятельности требования нормативных правовых актов и иных нормативных документов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности		
ПК-37	Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации		
ПК-38	Способность принимать участие в создании системы защиты информации на объекте информатизации		
ПК-18	Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов	ПК-14	Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов
ПК-16	Способность выявлять и содействовать пресечению коррупционных проявлений в служебном коллективе		
ПК-20	Способность выявлять и устранять причины и условия, способствующие коррупционным проявлениям в коллективе		
ПК-19	Способность принимать оптимальные управленческие решения	ПК-15	Способность принимать управленческие решения
ПК-21	Способность осуществлять документационное обеспечение управленческой деятельности	ПК-16	Способность осуществлять документационное обеспечение управленческой деятельности
ПК-22	Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на предмет соответствия требованиям государственных и ведомственных нормативных документов	ПК-17	Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов
ПК-23	Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации	ПК-18	Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации
ПК-24	Способность соблюдать в профессиональной деятельности требования нормативных правовых актов и иных нормативных документов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности	ПК-19	Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности

ПК-25	Способность работать с различными источниками информации, информационными ресурсами и технологиями; использовать в профессиональной деятельности прикладные программные средства, современные средства телекоммуникации, автоматизированные информационно-справочные, информационно-поисковые системы, базы данных, автоматизированные рабочие места; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	ПК-20	Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач
ПК-26	Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности		
ПК-25	Способность работать с различными источниками информации, информационными ресурсами и технологиями; использовать в профессиональной деятельности прикладные программные средства, современные средства телекоммуникации, автоматизированные информационно-справочные, информационно-поисковые системы, базы данных, автоматизированные рабочие места; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	ПК-21	Способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы
ПК-27	Способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы		
ПК-28	Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности	ПК-22	Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности
ПК-29	Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику	ПК-23	Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику
ПК-12	Способность осуществлять мероприятия по информационно-психологическому обеспечению правоохранительной деятельности; применять при решении профессиональных задач психологические методы, средства и приемы	ПК-24	Способность осуществлять противодействие деструктивным и негативным информационно-психологическим воздействиям
ПК-31	Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования	ПК-25	Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования

ПК-32	Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты	ПК-26	Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты
ПК-34	Способность составлять обзоры по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности	ПК-27	Способность готовить научные отчеты по результатам выполненных исследований
ПК-33	Способность готовить научные отчеты по результатам выполненных исследований		
ПК-35	Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	ПК-28	Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны
ПК-7	Способность проводить анализ эффективности системы защиты информации		
ПК-36	Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации	ПК-29	Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации
ПК-37	Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	ПК-30	Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации
ПК-30	Способность проводить анализ состояния безопасности информации на объектах и в отдельных системах с использованием отечественных и зарубежных стандартов	ПК-31	Способность принимать участие в создании системы защиты информации на объекте информатизации
ПК-38	Способность принимать участие в создании системы защиты информации на объекте информатизации		
ПК-6	Способность участвовать в исследовании и проверке объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации	ПК-32	Способность осуществлять производство судебных компьютерных экспертиз
ПК-10	Способность участвовать в пресечении и раскрытии правонарушений и преступлений в качестве специалиста		
ПК-11	Способность осуществлять информационно-аналитическое обеспечение оперативно-розыскных мероприятий, следственных действий, управленческой деятельности		
ПК-13	Способность реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений		
ПК-29	Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику		

ПК-39	Способность к проектированию, реализации, контролю и оценке результатов учебно-воспитательного процесса по дисциплинам в области информационных технологий и информационной безопасности в общеобразовательных учреждениях, образовательных учреждениях начального профессионального, среднего профессионального и дополнительного образования	ПК-33	Способность проектировать, осуществлять, контролировать и оценивать результаты образовательного процесса по дисциплинам (модулям) в области информационных технологий и информационной безопасности в организациях, осуществляющих образовательную деятельность
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 специализации, 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, в том числе первичных умений и навыков научно-исследовательской деятельности. Способ проведения – стационарная и выездная.

2. Производственная.

2.1. Тип – практика по получению профессиональных умений и опыта профессиональной деятельности. Способ проведения – стационарная и выездная.

2.2. Тип – преддипломная практика по получению профессиональных умений и опыта профессиональной деятельности, для выполнения выпускной квалификационной работы. Способ проведения – стационарная и выездная.

2.3. Тип – научно-исследовательская работа. Способ проведения – стационарная и 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 специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

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 60%).

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 70%).

Доля работников из числа руководителей и работников организаций, деятельность которых связана с направленностью реализуемой программы бакалавриата в общем числе работников, реализующих программу специалитета составляет 8% (критериальное значение, предусмотренное ФГОС ВО – не менее 1%).

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.xml+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 про-

граммах 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 №Т&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	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)

(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)			
--	--	--	--

*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, видеувеличители, программы не визуального 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 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.

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 IntelXeon 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/Seagate 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 Project Professional (№ 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 (K3) +ЦУ (АН99-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 про-

фессиональных 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 субъектов 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 сту-

дентов, 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 общественными 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 «Виразж», 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 СПИ-

Дом. 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 медиациентр, 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, включая подготовку к процедуре защиты и процедуру защиты.

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

№ п./п.	Направление подготовки	Направленность подготовки	Номер уровня квалификации	Наименование выбранного профессионального стандарта
1	10.05.05 «Безопасность информационных технологий в правоохранительной сфере»	Технологии защиты информации в правоохранительной сфере	7, 8	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	В	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	Дополнительно требуется включение ТФ 6-го уровня квалификации	Решение профессиональных задач ФГОС требует включения дополнительных ТФ из ПС
2	С	Внедрение систем защиты информации автоматизированных систем	Дополнительно требуется включение ТФ 6-го уровня квалификации	Решение профессиональных задач ФГОС требует включения дополнительных ТФ из ПС
3	Д	Разработка систем защиты информации автоматизированных систем	без изменений	Решение профессиональных задач ФГОС требует включения дополнительных ТФ из ПС
4	Е	Формирование требований к защите информации в автоматизированных системах	Добавить ТФ 8-го уровня: Е/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 технических систем обеспечения безопасности информации		Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (В)	Диагностика систем защиты информации автоматизированных систем (В/01.6) Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций (В/04.6)	Профессиональная задача является частью трех ОТФ, ТФ представлены в явном виде.
		Внедрение систем защиты информации автоматизированных систем (С)	Установка и настройка средств защиты информации в автоматизированных системах (С/01.6)	
		Разработка систем защиты информации автоматизированных систем (D)	Тестирование систем защиты информации автоматизированных систем (D/01.7)	

Участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (В)	Аудит защищенности информации в автоматизированных системах (В/06.6)	Полное соответствие
Администрирование подсистем обеспечения информационной безопасности на объекте	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (В)	Администрирование систем защиты информации автоматизированных систем (В/02.6)	Полное соответствие
Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (В)	Мониторинг защищенности информации в автоматизированных системах (В/05.6)	Профессиональная задача является частью трех ОТФ, ТФ представлены не явно. Частичное соответствие
	Внедрение систем защиты информации автоматизированных систем (С)	Аудит защищенности информации в автоматизированных системах (В/06.6)	
	Формирование требований к защите информации в автоматизированных системах (Е)	Анализ уязвимостей внедряемой системы защиты информации (С/03.6)	
Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации	Разработка систем защиты информации автоматизированных систем (D)	Обоснование необходимости защиты информации в автоматизированной системе (Е/01.8)	ТФ представлены не явно. Частичное соответствие
		Разработка проектных решений по защите информации в автоматизированных системах (D/02.7)	
		Разработка эксплуатационной документации на системы защиты информации автоматизированных систем (D/03.7)	

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 формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК -1).	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 ре-	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО

	шений по защите информации в автоматизированных системах. Уровень квалификации – 7.	
Способность применять технические и программно-аппаратные средства обработки и защиты информации (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 организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации (ПК-3).	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 участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации (ПК-4).	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 осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5).	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 осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации (ПК-6).	Администрирование систем защиты информации автоматизированных систем. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13).	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 организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов (ПК-17).	Диагностика систем защиты информации автоматизированных систем. Аудит защищенности информации в автоматизированных системах. Уровень квалификации – 6	Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО
Способность разрабатывать предложе-	Разработка предложений по	Выбранные трудовые функ-

<p>ния по совершенствованию системы управления безопасностью информации (ПК-18).</p>	<p>совершенствованию системы управления безопасностью информации в автоматизированных системах. Уровень квалификации – 7.</p>	<p>ции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности (ПК-19).</p>	<p>Мониторинг защищенности информации в автоматизированных системах. Аудит защищенности информации в автоматизированных системах. Уровень квалификации – 6</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач (ПК-20).</p>	<p>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.</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22).</p>	<p>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.</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования (ПК-25).</p>	<p>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.</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты (ПК-26).</p>	<p>Диагностика систем защиты информации автоматизированных систем. Уровень квалификации – 6</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны (ПК-28).</p>	<p>Анализ уязвимостей внедряемой системы защиты информации. Уровень квалификации – 6. Разработка проектных решений по защите информации в автоматизированных</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>

	<p>системах. Обоснование необходимости защиты информации в автоматизированной системе. Уровень квалификации – 7.</p>	
<p>Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации (ПК-29).</p>	<p>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.</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации (ПК-30).</p>	<p>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</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность принимать участие в создании системы защиты информации на объекте информатизации (ПК-31).</p>	<p>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.</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-1).</p>	<p>Установка и настройка средств защиты информации в автоматизированных системах. Уровень квалификации – 6. Обоснование необходимости защиты информации в автоматизированной системе. Уровень квалификации – 7.</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-2).</p>	<p>Администрирование систем защиты информации автоматизированных систем. Уровень квалификации – 6</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность планировать и организовывать комплекс мероприятий по защи-</p>	<p>Управление защитой информации в автоматизиро-</p>	<p>Выбранные трудовые функции профессиональных стан-</p>

<p>те информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации (ПСК-3).</p>	<p>ванных 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.</p>	<p>дартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>
<p>Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности (ПСК-4).</p>	<p>Установка и настройка средств защиты информации в автоматизированных системах. Уровень квалификации – 6 Разработка технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем. Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации. Уровень квалификации – 7.</p>	<p>Выбранные трудовые функции профессиональных стандартов хорошо согласуются с профессиональными компетенциями ФГОС ВО</p>

5. Формирование результатов освоения программы с учетом ПС

Результаты освоения ОПОП ВО

Виды профессиональной деятельности	Профессиональные задачи	Профессиональные компетенции и/или профессионально-специализированные компетенции
<p>Эксплуатационная</p>	<p>Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации</p>	<p>Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК -1); Способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2); Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5).</p>

	<p>Участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации</p>	<p>Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации (ПК-3);</p> <p>Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации (ПК -4).</p>
	<p>Администрирование подсистем обеспечения информационной безопасности на объекте</p>	<p>Способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации (ПК-6).</p> <p>Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-2).</p>
<p>Организационно-управленческая</p>	<p>Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов</p>	<p>Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13);</p> <p>Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов (ПК-14);</p> <p>Способность принимать управленческие решения (ПК-15);</p> <p>Способность осуществлять документационное обеспечение управленческой деятельности (ПК-16).</p>
	<p>Разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности</p>	<p>Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов (ПК-17);</p> <p>Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации (ПК-18);</p> <p>Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности (ПК-19).</p>
<p>Информационно-аналитическая</p>	<p>Получение и обработка поступающей информации</p>	<p>Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ре-</p>

		<p>сурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач (ПК-20);</p> <p>Способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы (ПК-21).</p>
	Анализ и отбор данных и сведений для формирования информационных ресурсов	<p>Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22);</p> <p>Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику (ПК-23);</p> <p>Способность осуществлять противодействие деструктивным и негативным информационно-психологическим воздействиям (ПК-24).</p>
Научно-исследовательская	Сбор, изучение, систематизация и обобщение научно-технической информации, отечественного и зарубежного опыта по проблемам информационно-аналитической работы и обеспечения защиты информации	Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования (ПК-25).
	Разработка заданий, планов, программ проведения прикладных научных исследований и технических разработок	Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты (ПК-26).
	Проведение экспериментов по заданным методикам	
	Выполнение прикладных научных исследований, подготовка отчетов, докладов	Способность готовить научные отчеты по результатам выполненных исследований (ПК-27).
Проектно-технологическая	Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации	Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны (ПК-28).
	Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации	<p>Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации (ПК-29);</p> <p>Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации (ПК-30);</p> <p>Способность принимать участие в создании системы защиты информации на объекте информатизации (ПК-31).</p>

Общепрофессиональные компетенции:

- Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1);
- Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации (ОПК-2).

Общекультурные компетенции:

- Способность понимать и анализировать мировоззренческие, социально и лично значимые философские проблемы (ОК-1);
- Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма (ОК-2);
- Способность ориентироваться в политических, социальных и экономических процессах (ОК-3);
- Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета (ОК-4);
- Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-5);
- Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния (ОК-6);
- Способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии (ОК-7);
- Способность принимать организационно-управленческие решения (ОК-8);
- Способность организовывать свою жизнь в соответствии с социально значимыми представлениями о здоровом образе жизни (ОК-9);
- Способность осуществлять письменную и устную коммуникацию на русском языке (ОК-10);
- Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков (ОК-11);
- Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12).

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
<ul style="list-style-type: none"> – Обоснование необходимости защиты информации в автоматизированной системе; – Внедрение организационных мер по защите информации в автоматизированных системах. 	<p>Вид профессиональной деятельности: проектно-технологическая, экспериментально-исследовательская</p> <p>Учебная практика</p> <p>Объем практики (в зачетных единицах) – 3 ЗЕ</p> <p>ОПК-1 Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач;</p> <p>ПК-2 Способность применять технические и программно-аппаратные средства обработки и защиты информации;</p> <p>ПК-10 Способность правильно и полно отражать результаты профессиональной деятельности в служебной документации;</p> <p>ПК-11 Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в военное время;</p>	<ul style="list-style-type: none"> – 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 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;

	<p>ПК-13 Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;</p> <p>ПК-20 Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач;</p> <p>ПК-21 Способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы.</p>	<p>– Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.</p>
<ul style="list-style-type: none"> – 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; – Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем; – Обоснование необходимости защиты информации в автоматизированной системе; – Разработка организационно-распорядительных документов по защите информации в автоматизированных системах; – Внедрение организационных 	<p>Вид профессиональной деятельности: проектно-технологическая, эксплуатационная, информационно-аналитическая, экспериментально-исследовательская</p> <p>Производственная практика</p> <p>Объем практики (в зачетных единицах) – 15 ЗЕ</p> <p>ОПК-1 Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач;</p> <p>ПК-1 Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;</p> <p>ПК-2 Способность применять технические и программно-аппаратные средства обработки и защиты информации;</p> <p>ПК-3 Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации;</p> <p>ПК-4 Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации;</p> <p>ПК-5 Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния;</p> <p>ПК-6 Способность осуществлять</p>	<ul style="list-style-type: none"> – 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 автоматизированных систем; – Определение правил и процедур выявления инцидентов и реагирования на них;

<p>мер по защите информации в автоматизированных системах;</p> <ul style="list-style-type: none"> - Управление защитой информации в автоматизированных системах. 	<p>администрирование подсистем обеспечения информационной безопасности объекта информатизации;</p> <p>ПК-13 Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;</p> <p>ПК-17 Способность организовать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов;</p> <p>ПК-18 Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации;</p> <p>ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности;</p> <p>ПК-20 Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач;</p> <p>ПК-21 Способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы;</p> <p>ПК-22 Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности;</p> <p>ПК-28 Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны;</p> <p>ПК-29 Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации;</p> <p>ПК-30 Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации;</p> <p>ПК-31 Способность принимать участие в создании системы защиты информации на объекте информатизации;</p> <p>ПСК-1 Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных си-</p>	<ul style="list-style-type: none"> - 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; - Разработка технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем; - Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.
---	---	---

	<p>стемах, при организации защиты обрабатываемой в них информации;</p> <p>ПСК-2 Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей;</p> <p>ПСК-3 Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации;</p> <p>ПСК-4 Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности.</p>	
<ul style="list-style-type: none"> - 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 решений по защите информации в автоматизированных системах; - Обоснование необходимости защиты информации в автоматизированной системе; - Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем; - Управление защитой информации в автоматизированных системах. 	<p>Вид профессиональной деятельности: проектно-технологическая, информационно-аналитическая, экспериментально-исследовательская</p> <p>Преддипломная практика</p> <p>Объем практики (в зачетных единицах) – 6 ЗЕ</p> <p>ОПК-1 Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования процессов и явлений при решении профессиональных задач;</p> <p>ПК-1 Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;</p> <p>ПК-2 Способность применять технические и программно-аппаратные средства обработки и защиты информации;</p> <p>ПК-3 Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации;</p> <p>ПК-5 Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния;</p> <p>ПК-6 Способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации;</p> <p>ПК-13 Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;</p> <p>ПК-17 Способность организовыв-</p>	<ul style="list-style-type: none"> - Обнаружение, идентификация и устранение инцидентов в процессе эксплуатации автоматизированной системы; - 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; - Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с 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

	<p>вать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов;</p> <p>ПК-18 Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации;</p> <p>ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности;</p> <p>ПК-20 Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач;</p> <p>ПК-21 Способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы;</p> <p>ПК-22 Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности;</p> <p>ПК-25 Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования;</p> <p>ПК-26 Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты</p> <p>ПК-27 Способность готовить научные отчеты по результатам выполненных исследований;</p> <p>ПК-28 Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны;</p> <p>ПК-29 Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации;</p> <p>ПК-30 Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации;</p> <p>ПК-31 Способность принимать участие в создании системы защиты информации на объекте информатизации;</p> <p>ПСК-1 Способность учитывать и использовать особенности информационных технологий, применя-</p>	<p>защищенности информации автоматизированных систем;</p> <ul style="list-style-type: none"> - 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 информации в автоматизированной системе; - Определение требуемого класса (уровня) защищенности автоматизированной системы; - Разработка технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем; - Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.
--	---	--

	<p>емых в автоматизированных системах, при организации защиты обрабатываемой в них информации;</p> <p>ПСК-2 Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей;</p> <p>ПСК-3 Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации;</p> <p>ПСК-4 Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности.</p>	
<ul style="list-style-type: none"> – 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. 	<p>Вид профессиональной деятельности: экспериментально-исследовательская, информационно-аналитическая</p> <p>Научно-исследовательская работа</p> <p>Объем практики (в зачетных единицах) – 3 ЗЕ</p> <p>ОПК-1 Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач;</p> <p>ПК-18 Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации;</p> <p>ПК-20 Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач;</p> <p>ПК-25 Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования;</p> <p>ПК-26 Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты</p> <p>ПК-27 Способность готовить научные отчеты по результатам выполненных исследований;</p> <p>ПК-28 Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны;</p> <p>ПСК-1 Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных систе-</p>	<ul style="list-style-type: none"> – 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 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

	<p>мах, при организации защиты обрабатываемой в них информации;</p> <p>ПСК-2 Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей;</p> <p>ПСК-3 Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации;</p> <p>ПСК-4 Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем связанных с обеспечением информационной безопасности.</p>	<p>(уровня) защищенности автоматизированной системы;</p> <ul style="list-style-type: none"> - 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; - Разработка технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем; - Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты 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)											
История	ОК-2										
Философия	ОК-1										
Иностранный язык 1	ОК11										
Иностранный язык 2	ОК-11										
Экономика	ОК-3	ПК-28									
Психология и педагогика	ОК-5	ОК-6	ОК-8	ПК-24	ПК-33						
Логика	ОК-7										
Политология	ОК-3										
Профессиональная этика и служебный этикет	ОК-4	ОК-5									
Математика	ОПК-1										
Физика 1	ОПК-1										
Физика 2	ОПК-1										
Физические основы защиты информации	ОПК-1										
Информатика и информационные технологии в правоохранительной деятельности. Часть 1	ОК-12	ПК-20	ПК-21								
Информатика и информационные технологии в правоохранительной деятельности. Часть 2	ОК-12	ПК-20	ПК-21								
Математические основы обработки информации	ОПК-1	ПК-20	ПК-26								
Прикладная математика:											
Методы оптимизации	ОПК-1										
Элементы математической логики	ОПК-1	ПК-20	ПК-21								
Базы данных	ПК-20	ПК-21									
Средства вычислительной техники	ОК-12	ПК-2	ПК-5	ПК-20							
Безопасность жизнедеятельности	ОПК-2										
Управление информационной безопасностью	ОК-8	ПК-1	ПК-3	ПК-18	ПК-28						

Программирование: языки, методы и технологии:												
Языки программирования и основы алгоритмизации	ОК-12	ОПК-1	ПК-2	ПСК-4								
Технологии и методы программирования	ОК-12	ОПК-1	ПК-2	ПСК-4								
Системы и сети передачи данных	ОК-12	ПК-2	ПК-20	ПСК-1	ПСК-2							
Основы электротехники и радиоэлектроники:												
Теоретические основы электротехники	ПК-2	ПК-4	ПК-5	ПК-26	ПК-31							
Основы радиоэлектроники	ПК-2	ПК-4	ПК-5	ПК-26	ПК-31							
Основы электро-, радиоизмерений	ПК-2	ПК-4	ПК-5	ПК-26	ПК-31							
Теория информационной безопасности и методология защиты информации	ОПК-1	ПК-1	ПК-31									
Информационное право	ПК-13	ПК-19										
Правовая защита информации	ПК-1	ПК-3	ПК-13	ПК-19	ПК-30							
Организационная защита информации	ПК-1	ПК-13	ПК-30	ПК-31								
Документоведение	ПК-10	ПК-16	ПК-27									
Защита и обработка документов ограниченного доступа	ПК-19	ПК-29	ПК-31									
Инженерно-техническая защита информации	ПК-1	ПК-2	ПК-31									
Программно-аппаратная защита информации	ПК-1	ПК-2	ПК-4	ПК-6	ПК-31							
Криптографическая защита информации	ОПК-1	ПК-1	ПК-2									
Модуль: специальная или военная подготовка												
Специальная подготовка												
Оказание медицинской помощи при авариях и ЧС	ПК-12											
Тактико-специальная подготовка	ПК-7	ПК-8	ПК-9	ПК-11								
Противодействие информационной разведке	ОПК-1	ПК-7	ПК-8	ПК-9								
Специальные информационные правовые системы	ОК-12	ПК-20	ПК-21									
Основы криминалистики	ОПК-1	ПК-8	ПК-9	ПК-32								

Военная подготовка													
Общая тактика	ВПК.ОПК-6	ВПК.ОПК-7	ВПК.ОПК-8										
Общевоинские уставы ВС РФ	ВПК.ОК-2	ВПК.ОПК-1											
Управление подразделениями в мирное время	ВПК.ОК-2												
Стрелковая подготовка	ВПК.ОПК-4												
Огневая подготовка из стрелкового оружия	ВПК.ОПК-2	ВПК.ОПК-3											
Компьютерно-техническая экспертиза	ПК-32												
Психология воздействия	ОК-5	ОК-6	ПК-24										
Специальные информационные технологии в правоохранительной деятельности	ОК-12	ПК-8	ПК-23	ПСК-1									
Правоохранительные органы	ПК-7	ПК-8											
Криминология	ОПК-1	ПК-8											
Информационно-аналитическое обеспечение правоохранительной деятельности	ОК-12	ПК-8	ПК-20	ПК-21	ПК-22	ПК-23							
Физическая культура	ОК-9												
Русский язык и культура речи	ОК-10	ПК-16	ПК-27										
Искусственный интеллект в системах защиты информации	ОК-12	ПК-20	ПСК-1										
Нейросетевые технологии обработки информации	ОК-12	ПК-20	ПСК-1										
Проектирование защищенных компьютерных систем	ПК-31	ПСК-1	ПСК-4										
Экономика защиты информации	ОК-3	ПК-28											
Администрирование компьютерных систем	ПК-2	ПК-6	ПСК-2										
Комплексная система защиты информации на предприятии	ПК-1	ПК-3	ПК-30	ПК-31									
Технические средства охраны	ПК-1	ПК-2	ПК-5	ПК-31									
Защита информационных процессов в компьютерных системах	ПК-1	ПК-2	ПК-31	ПСК-1									
Стандарты информационной безопасности и аудит	ПК-4	ПК-13	ПК-17	ПК-29	ПК-31								

Элективные курсы по физической культуре	ОК-9											
Факультативные дисциплины												
Основы авиационной техники	ВПК.ПК-2											
Тактика ВВС	ВПК.ОК-3											
Практики												
Учебная	ОК-1 ПК-11	ОК-3 ПК-12	ОК-4 ПК-13	ОК-5 ПК-20	ОК-6 ПК-21	ОК-9	ОК-10	ОК-11	ОК-12	ОПК-1	ПК-2	ПК-10
Производственная	ОК-1 ОПК-2 ПК-13 ПК-29	ОК-3 ПК-1 ПК-15 ПК-30	ОК-4 ПК-2 ПК-16 ПК-31	ОК-5 ПК-3 ПК-17 ПК-32	ОК-6 ПК-4 ПК-18 ПК-33	ОК-7 ПК-5 ПК-19 ПСК-1	ОК-8 ПК-6 ПК-20 ПСК-2	ОК-9 ПК-8 ПК-21 ПСК-3	ОК-10 ПК-9 ПК-22 ПСК-4	ОК-11 ПК-10 ПК-23	ОК-12 ПК-11 ПК-24	ОПК-1 ПК-12 ПК-28
Преддипломная	ОК-1 ПК-6 ПК-23 ПСК-3	ОК-3 ПК-9 ПК-25 ПСК-4	ОК-4 ПК-10 ПК-26	ОК-7 ПК-13 ПК-27	ОК-10 ПК-14 ПК-28	ОК-11 ПК-15 ПК-29	ОК-12 ПК-16 ПК-30	ОПК-1 ПК-18 ПК-31	ПК-1 ПК-19 ПК-32	ПК-2 ПК-20 ПК-33	ПК-3 ПК-21 ПСК-1	ПК-5 ПК-22 ПСК-2
Научно-исследовательская работа	ОК-1 ПСК-2	ОК-7 ПСК-3	ОК-12 ПСК-4	ОПК-1	ПК-18	ПК-20	ПК-25	ПК-26	ПК-27	ПК-28	ПК-33	ПСК-1
Государственная итоговая аттестация	ОК-1 ОПК-1 ПК-11 ПК-23 ПСК-2 ВПК.ОПК-7	ОК-2 ОПК-2 ПК-12 ПК-24 ПСК-3 ВПК.ОПК-8	ОК-3 ПК-1 ПК-13 ПК-25 ПСК-4 ВПК.ПК-1	ОК-4 ПК-2 ПК-14 ПК-26 ВПК.ОК-1 ВПК.ПК-2	ОК-5 ПК-3 ПК-15 ПК-27 ВПК.ОК-2 ВПК.ПК-3	ОК-6 ПК-4 ПК-16 ПК-28 ВПК.ОК-3	ОК-7 ПК-5 ПК-17 ПК-29 ВПК.ОПК-1	ОК-8 ПК-6 ПК-18 ПК-30 ВПК.ОПК-2	ОК-9 ПК-7 ПК-19 ПК-31 ВПК.ОПК-3	ОК-10 ПК-8 ПК-20 ПК-32 ВПК.ОПК-4	ОК-11 ПК-9 ПК-21 ПК-33 ВПК.ОПК-5	ОК-12 ПК-10 ПК-22 ПСК-1 ВПК.ОПК-6

Рецензия

на основную профессиональную образовательную программу по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере»

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

Объектами профессиональной деятельности по специализации «Технологии защиты информации в правоохранительной сфере» в соответствии с ФГОС ВО по данной специальности являются:

- информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности;
- технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта);
- объекты информатизации правоохранительных органов;
- организационно-правовые механизмы, регламентирующие информационно-аналитическую деятельность в правоохранительной сфере;
- процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления.

В соответствии с ФГОС ВО данной специальности выпускник со специализацией «Технологии защиты информации в правоохранительной сфере» подготовлен к следующим видам профессиональной деятельности:

- эксплуатационная;
- правоохранительная;
- организационно-управленческая;
- информационно-аналитическая;
- научно-исследовательская;
- проектно-технологическая;
- экспертная;
- педагогическая.

В соответствии с запросами рынка труда выпускник со специализацией «Технологии защиты информации в правоохранительной сфере» 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 данной специальности и специализации входят:

– академические, государственные органы, ведомственные и частные научно-исследовательские и производственные организации, связанные с решением проблем, связанных с обеспечением безопасности информационных технологий;

– 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 специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», реализуемая в ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ) по специализации «Технологии защиты информации в правоохранительной сфере» соответствует требованиям образовательного стандарта, профессионального стандарта и современным требованиям рынка труда.

Директор ЗАО «Республиканский
центр защиты информации»



С.Н. Зарипов

ВЫПИСКА из протокола заседания

Научно-методического совета

по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

(шифр и наименование)

На основании анализа состава и содержания документов основной образовательной программы по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

(шифр и наименование образовательной программы)

специализации Технологии защиты информации в правоохранительной сфере,
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


подпись

Васильев В.И.

«20» 06 2017 г.
дата

ВЫПИСКА

из протокола заседания
научно-методического совета по специальности 10.05.05
Безопасность информационных технологий в правоохранительной сфере
№ 10 от 28 июня 2018 г.

На основании анализа состава и содержания документов основной образовательной программы уровня ВО специалитета по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере», очная форма обучения

Научно-методический совет подтверждает, что:

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

1. Раздел 5 (пункт 5.2) 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/	44 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 №АСМ/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 в сети УГАТУ, имеющих выход в	УГАТУ в составе организаций, получивших поддержку РФФИ для

	компания 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/ <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ▪ 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)

	<p>ний SpringerProtocols http://www.springerprotocols.com/</p> <ul style="list-style-type: none"> ▪ научные материалы в области физических наук SpringerMaterials http://materials.springer.com ▪ справочные материалы Springer ReferencesWork http://link.springer.com <p>реферативная база данных по математике Zentralblatt MATH http://www.zentralblatt-math.org/zblmath/en</p>			
3	<p>Научные журналы Nature Publishing Group http://www.nature.com</p>	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.	<p>База данных GreenFile компании EBSCO http://www.greeninfoonline.com</p>	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.	<p>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)</p>	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
1.	Xspider Education	Лицензионный договор 090-18/Е от 27.06.2018
2.	MaxPatrol Education	Лицензионный договор 090-18/Е от 27.06.2018
3.	PT Application Firewall Education	Лицензионный договор 090-18/Е от 27.06.2018
4.	MaxPatrol SIEM	Лицензионный договор 090-18/Е от 27.06.2018
5.	СЗИ «Блокхост-МДЗ», 4 модуля: ШДЗ, ОП, КЦ, ГУ	Договор о сотрудничестве 21 от 04.06.2018
6.	СЗИ «Блокхост-сеть 2.0», автономный вариант	Договор о сотрудничестве 21 от 04.06.2018
7.	СЗИ «Блокхост-сеть 2.0», сервер управления	Договор о сотрудничестве 21 от 04.06.2018
8.	СЗИ «Блокхост-сеть 2.0», сетевой вариант	Договор о сотрудничестве 21 от 04.06.2018
9.	ПК «Litoria Desktop 2»	Договор о сотрудничестве 21 от 04.06.2018
10.	ПК «Efros Config Inspector 3.0» Premium, сервер	Договор о сотрудничестве 21 от 04.06.2018
11.	ПК «Efros Config Inspector 3.0» Premium, клиент Active Network Device	Договор о сотрудничестве 21 от 04.06.2018
12.	ПК «Efros Config Inspector 3.0» Premium, клиент сервера управления среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018
13.	ПК «Efros Config Inspector 3.0» Premium, клиент гипервизора среды виртуализации	Договор о сотрудничестве 21 от 04.06.2018
14.	ПК «Efros Config Inspector 3.0» Premium, клиент Server Operating System	Договор о сотрудничестве 21 от 04.06.2018
15.	ПК «Efros Config Inspector 3.0» Premium, агент контроля целостности Windows OS	Договор о сотрудничестве 21 от 04.06.2018
16.	Kaspersky Endpoint Security для бизнеса - Стандартный	Договор №391/0304-18 от 26.06.2018 г.
17.	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
18.	Infowatch Endpoint Security	Соглашение 067-Е-ИВ/2013 о создании экспериментальной площадки (учебного класса) от 18.11.2013. Лицензия ES_Total_10_27-06-2017
19.	Infowatch Traffic Monitor Enterprise Edition 6.5	Лицензионное соглашение 932-Н-ИВ/2016. Лицензия до 19.06.2019
20.	SearchInform Event Manager	Лицензионный договор 1726811 от 28.12.2016 на 3 года
21.	Astra Linux SE (Special Edition) РУСБ.10015-01 (программный продукт в формате BOX)	Лицензионный договор РБТ-14/1318-01-ВУЗ
22.	Специальная версия DLP системы Secure Tower	Лицензионный договор 05/17/2016-1 на 3 года
23.	Сервер безопасности Dallas Lock 8.0-С	лицензионный сертификат 181**_****_*57 от 01.2017
24.	Dallas Lock Linux	лицензионный сертификат 181**_****_*99 от 01.2017
25.	Сервер безопасности Dallas Lock 8.0-К	лицензионный сертификат 181**_****_*13 от 01.2017
26.	Dallas Lock 8.0-К(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**_****_*33 от 01.2017
27.	Dallas Lock 8.0-С(СЗИ, НСД, СКН, МЭ, СОВ)	лицензионный сертификат 181**_****_*14 от 01.2017
28.	СЗВИ Dallas Lock 8.0	Лицензия 1909***_****_*87 от 06.2017 бессрочно
29.	СЗИ Secret Net 7 Клиент (автономный режим работы)	Лицензия WWIB_****_****_****_****_****_*00S от 16.01.2017
30.	СЗИ Secret Net 7.8 Клиент (автономный режим работы)	Лицензия WWIB_****_****_****_****_****_*001 от 05.03.2018
31.	СЗИ Secret Net 7.8 Сервер безопасности класса С	WWIL_****_****_****_****_****_*003 от 05.03.2018
32.	СЗИ Secret Net 7.8 (Клиент сетевой Режим работы)	WWIC_****_****_****_****_****_*00Q от 05.03.2018
33.	СЗИ Secret Net 7.8 (Терминальное подключение)	WWIA_****_****_****_****_****_*006 от 05.03.2018
34.	СЗИ «Secret Net LSP»	Лицензия 1****А от 16.01.2017
35.	СЗИ «Secret Net LSP»	Лицензия 1****5 от 05.03.2018
36.	Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net LSP	Ключ U*****W от 05.03.2018
37.	Сервис прямой технической поддержки уровня Стандартный» для СЗИ Secret Net	Ключ 3*****T от 05.03.2018

ВЫПИСКА

из протокола заседания
научно-методического совета по специальности 10.05.05
Безопасность информационных технологий в правоохранительной сфере
№ 10 от 15 мая 2019 г.

СЛУШАЛИ: доцента кафедры ВТиЗИ Дуленко В.А. о внесении изменений и дополнений в основную профессиональную образовательную программу по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере», реализуемой в очной форме.

ПОСТАНОВИЛИ: утвердить следующие изменения и дополнения в основной профессиональной образовательной программе по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере», 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.xml+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/Е от 27.06.2018	
MaxPatrol Education	Лицензионный договор 090-18/Е от 27.06.2018	
PT Application Firewall Education	Лицензионный договор 090-18/Е от 27.06.2018	
MaxPatrol SIEM	Лицензионный договор 090-18/Е 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	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 1У до 01.01.2020	
Infowatch Endpoint 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-Н-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****А 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*****Т 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*****С, от 16.01.2017	
Secret Net Studio 8(модули защиты от НСД, контроля устройств)	Лицензия 1*****С, от 05.03.2018	
Secret Net Studio 8(модули персонального межсетевоего экрана)	Лицензия 1*****В 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*****С, 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 1*****7 от 05.03.2018	
Secret MDM Secure Pack на 1 подключенное устройство при локальном размещении	Лицензия 1*****А от 05.03.2018	
Сервис прямой технической поддержки уровня «Стандартный» для Secret MDM	Ключ В*****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 <ul style="list-style-type: none"> • 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 незрительного 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						Всего часов
	1	2	3	4	5	6	
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. Исключить модуль «Военная подготовка», содержащий дисциплины: «Общая тактика», «Общевойсковые уставы ВС РФ», «Управление подразделениями в мирное время», «Строевая подготовка», «Огневая подготовка из стрелкового оружия».

3.2. Исключить дисциплины по выбору: «Эксплуатация и ремонт радиоэлектронного оборудования самолетов, вертолетов и авиационных ракет 1», «Эксплуатация и ремонт радиоэлектронного оборудования самолетов, вертолетов и авиационных ракет 2», «Эксплуатация и ремонт радиоэлектронного оборудования самолетов, вертолетов и авиационных ракет 3», «Эксплуатация и ремонт радиоэлектронного оборудования самолетов, вертолетов и авиационных ракет 4».

3.3. Исключить факультативные дисциплины: «Основы авиационной техники», «Тактика ВВС».

3.4. Включить дисциплины по выбору: «Web-дизайн», «Основы управления персоналом», «Катастрофоустойчивость информационных систем», «История развития вычислительной техники», «Модели безопасности баз данных». Разработать рабочие программы дисциплин.

3.5 Включить факультативные дисциплины: «Культура делового человека», «Нейрокомпьютеры». Разработать рабочие программы дисциплин.

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

№	Дисциплина	Семестр	Лекции	Лаб.	Практики	СРС	Контроль
1.	Проектирование защищенных компьютерных систем	9 10	10 10	12 8	2 2	12 52	Коллоков. Э, КР
2.	Инженерно-техническая защита информации	5 6 7	18 18 18	12 12 12	6 6 6	72 63 36	Коллоков. За Э, КР
3.	Телекоммуникационные технологии	5	20	12	4	27	З
4.	Правовая защита информации	8	28	16	28	36	Э
5.	Управление информационной безопасностью	7 8	30	24	18	36	Э КР
6.	Специальные информационные технологии в правоохранительной деятельности	7	24	20	8	56	Э
7.	Безопасность критически важных информационных систем/ Катастрофоустойчивость информационных систем	7	16	24	20	111	ЗаО
8.	Психология воздействия	8	28	24	20	63	ЗаО
9.	Безопасность систем баз данных/ Модели безопасности баз данных	8	10	24	20	54	Э
10.	Компьютерно-техническая экспертиза	8 9	12 12	16 16	8 8	36 72	Коллоков. Э
11.	Компьютерная графика/ Web-дизайн	5	20	28		87	ЗаО
12.	Основы управленческой деятельности/ Основы управления персоналом	6	16	20	20	88	Э
13.	Программно-аппаратная защита информации	5 6	30 36	24 28	4 8	77 72	За Э, КР
14.	Информационно-аналитическое обеспечение правоохранительной деятельности	9	30	24	18	135	ЗаО
15.	Культура делового человека	8	8		12	7	За

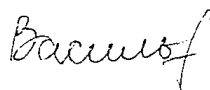
16.	Нейрокомпьютеры	8	8	12	2	5	За
17.	История развития вычислительной техники	3 4	6 6		10 10	11 11	За За

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

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

№	Дисциплина	Семестр	Лекции	Лаб.	Практики	КСР	СРС	Контроль
1.	Управление информационной безопасностью	7 8	20	20	8		96 36	Э КР
2.	Языки программирования и основы алгоритмизации	1 2	10 20	8 24	4 4		14 51	Коллоков. Э
3.	Информационно-аналитическое обеспечение правоохранительной деятельности	9	20	20	8		159	ЗаО
4.	Криминология	9	30	12	20		118	Э
5.	Программно-аппаратная защита информации	5 6	30 30	24 24	4 4		77 86	З Э,КР
6.	Тактико-специальная подготовка	4 5	24 24	20 20	4 4		51 51	ЗаО ЗаО
7.	Проектирование защищенных компьютерных систем	9 10	10 10	12 8	2 2		12 52	Коллоков. Э, РГР
8.	Физическая культура и спорт	1	10		28	2	23	За
9.	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
10.	Культура делового человека	6	8		12		7	За
11.	Нейрокомпьютеры	8	8	12	2		5	За

Председатель научно-методического совета по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере



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 специальности 10.05.05
Безопасность информационных технологий в правоохранительной сфере
№ 10 от 15 мая 2020 г.

СЛУШАЛИ: доцента кафедры ВТиЗИ Дуленко В.А. о внесении изменений и дополнений в основную профессиональную образовательную программу по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере», реализуемой в очной форме на 2020-2021 учебный год.

ПОСТАНОВИЛИ: утвердить следующие изменения и дополнения в основной профессиональной образовательной программе по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере», 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.xml+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/Е от 27.06.2018	
MaxPatrol Education	Лицензионный договор 090-18/Е от 27.06.2018	
PT Application Firewall Education	Лицензионный договор 090-18/Е от 27.06.2018	
MaxPatrol SIEM	Лицензионный договор 090-18/Е 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 Endpoint 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-Н-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****А 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	Ключ 3*****Т от 05.03.2018	

Net		
Security Studio Endpoint Protection 7.6	Лицензия WWIS-****-****-****-****-****-*000 от 16.01.2017	
Secret Net Studio 8 Поставка Максимальная защита	Лицензия 1*****С, от 16.01.2017	
Secret Net Studio 8(модули защиты от НСД, контроля устройств)	Лицензия 1*****С, от 05.03.2018	
Secret Net Studio 8(модули персонального межсетевоего экрана)	Лицензия 1*****В 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*****С, 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 1****7 от 05.03.2018	
Secret MDM Secure Pack на 1 подключенное устройство при локальном размещении	Лицензия 1****А от 05.03.2018	
Сервис прямой технической поддержки уровня «Стандартный» для Secret MDM	Ключ В****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 <ul style="list-style-type: none"> • 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 не визуального 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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере




В.И. Васильев

Начальник отдела образовательных программ и методического обеспечения программ бакалавриата и специалитета

Д.Ф. Муфаззалов

ВЫПИСКА

из протокола заседания № 10 научно-методического совета
по специальности 10.05.05 Безопасность информационных
технологий в правоохранительной сфере
от 27 мая 2021 г.

СЛУШАЛИ: доцента кафедры ВТиЗИ Дуленко В.А. о внесении изменений и дополнений в основную профессиональную образовательную программу по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере» для года начала подготовки с 2017 по 2020.

ПОСТАНОВИЛИ: утвердить следующие изменения и дополнения в основной профессиональной образовательной программе по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация «Технологии защиты информации в правоохранительной сфере» для года начала подготовки с 2017 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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере



В.И. Васильев

Выписка из протокола № 11 заседания кафедры от «08» 04. 2022 года
по специальности 10.05.05 «Безопасность информационных технологий в
правоохранительной сфере»,
направленность (профиль, специализация) «Организация и технологии защиты
информации (по отраслям)»,
форма обучения очная

СЛУШАЛИ: доц. каф. Даянова И.С. о внесении изменений и дополнений в основную профессиональную образовательную программу по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализация «Организация и технологии защиты информации (по отраслям)».

ПОСТАНОВИЛИ:

✓ утвердить отсутствие изменений и дополнений в основную профессиональную образовательную программу по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализация «Организация и технологии защиты информации (по отраслям)»;

состав комплекта лицензионного программного обеспечения не изменился; состав современных профессиональных баз данных и информационных справочных систем не изменился.

Заведующий кафедрой ВТиЗИ



Картак В.М.

ЛИСТ АКТУАЛИЗАЦИИ

Основная профессиональная образовательная программа актуализирована согласно Приказу № 1808-О от 28 декабря 2022 года Об актуализации основных профессиональных образовательных программ высшего образования (программ бакалавриата, программ магистратуры и программ специалитета), программ подготовки специалистов среднего звена (программ среднего профессионального образования), программ подготовки научных и научно-педагогических кадров в аспирантуре в соответствии с Приказом Министерства науки и высшего образования Российской Федерации от 08.07.2022 № 644 «О реорганизации ФГБОУ ВО «Башкирский государственный университет» и ФГБОУ ВО «Уфимский государственный авиационный технический университет» в форме слияния путем создания ФГБОУ ВО «Уфимский университет науки и технологии».