**ПРОГРАММА СТРАТЕГИЧЕСКОГО РАЗВИТИЯ ИПСУБ**

**на 2021 – 2025 гг.**

**1. Резюме**

История юридического образования и юридической науки в Удмуртии начинается с 1972 года, институт права, социального управления и безопасности (далее – Институт) занимает ведущее место в подготовке юридических кадров в Удмуртской Республике.

Наряду со специальностью «Юриспруденция» была начата реализация новых образовательных программ. Открытие в 1998-1999 годах в Институте неюридических специальностей стало достойным ответом на вызовы времени и позволило удовлетворять все возрастающую потребность в квалифицированных кадрах, которые способны отвечать требованиям информационного общества. Сегодня Институт выступает конгломератом гуманитарного и технического образования, выпуская специалистов, соответствующих требованиям цифрового общества.

Все вышесказанное привело к созданию в 2001 году кафедры информационной безопасности в управлении. Деятельность кафедры связана с подготовкой студентов, обучающихся по направлениям подготовки, соответствующим приоритетным направлениям модернизации и технологического развития российской экономики - направление подготовки «Информационная безопасность». Учитывая сочетание юридического и технического направления, реализующихся в Институте, в 2015 году была начата подготовка специалистов по защите информации для правоохранительной сферы по специальности «Безопасность информационных технологий в правоохранительной сфере».

В настоящее время Институт входит в число ведущих вузов России, прошедших общественно-профессиональную аккредитацию Ассоциации юристов Российской Федерации. В 2015 году Институт принят в Ассоциацию юридического образования России (в числе 73 участников), что дает определенные преимущества при открытии новых специальностей и направлений подготовки специалистов, бакалавров и магистров, а также при прохождении общественно-профессиональной аккредитации в 2018 году.

На семи профильных кафедрах Института подготовку студентов обеспечивают 112 преподавателей (83,21 ставки), из них штатными являются 73 человека (65,17% общей численности ППС, занимающие 64,85 ставки, что составляет 77,94%). Штатных преподавателей с учеными степенями и званиями – 59 или 52,67% (занято 54,36 ставок, что составляет 65,32%), докторов наук – 12 или 10,71% (7,65 ставок или 9,19%). Реализацию ОП подготовки специалистов обеспечивают научно-педагогические кадры, имеющие базовое высшее профессионально образование, соответствующее профилю преподаваемых дисциплин.

В возрасте до 35 лет с ученой степенью (званием) осуществляют педагогическую деятельность 8 штатных преподавателей, что составляет 7,14% от общей численности ППС.

В настоящее время в Институте осуществляется подготовка студентов по 5 направлениям бакалавриата, 3 специальностям ВО, 3 магистерским программам, 5 специальностям аспирантской подготовки.

Вестник Удмуртского университета (серия «Экономика и право») на протяжении последних 6 лет является изданием, рекомендованным ВАК. Индекс цитирования нашей серии довольно высок, журнал пользуется популярностью среди юридических вузов Уральского и Приволжского федеральных округов.

**Наиболее острые проблемы Института:**

1. Конкуренция со стороны центральных вузов и внутри региона (прежде всего со стороны Ижевского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) и ИжГТУ).

2. «Старение» педагогического состава (количество штатных ППС с ученой степенью/званием в возрасте до 35 лет – 8 чел.).

3. Низкая публикационная активность в научных изданиях, индексируемых в международных системах Web of Science и Scopus.

4. Низкий темп роста «остепененности» по показателю защит докторских диссертаций.

5. Устаревание материально-технической базы, недостаточное финансирование в области информационной безопасности.

6. Отсутствие образовательных направлений, касающихся формирования новой модели юриста-выпускника в части реализации компетенций цифровой экономики.

**2. Потенциал института**

**2.1. Образовательные и научные компетенции**

Основной потенциал Института реализуется посредством ведения образовательной деятельности – подготовки широкого круга бакалавров, магистров и специалистов в сфере юриспруденции и информационной безопасности, реализации программ дополнительного профессионального образования, послевузовского образования.

В процессе обучения активное участие принимают работодатели по направлениям юриспруденции, ИТ отрасли, промышленных предприятий города Ижевска, органов аттестации. Взаимодействие с работодателями осуществляется в различных формах, одной из форм является участие студентов в ИТ-лагере, проводимом в республике под эгидой Министерства информатизации и связи Удмуртской Республики, компаний ИТ отрасли республики, крупных вендоров в области ИТ и информационной безопасности. Кроме этого, участие студентов в киберспорте позволяет сформировать компетенции, связанные с виртуальной и дополненной реальностью. Киберспорт представляет собой многогранную сферу, имеющую большой образовательный потенциал для развития личности в условиях информационного общества, представляет вид соревновательной деятельности и специальной практики подготовки к соревнованиям на основе компьютерных и/или видеоигр, где игра предоставляет среду взаимодействия объектов управления, обеспечивая равные условия состязаний человека с человеком или команды с командой.

**2.1.1. Специальности и направления ИПСУБ:**

**Бакалавриат. 40.03.01 «Юриспруденция»**

Подготовка осуществляется по следующим профилям:

* уголовное право;
* гражданское право;
* государственное право;
* природоресурсное, экологическое и аграрное право.

**Бакалавриат. 10.03.01 «Информационная безопасность»**

Область профессиональной деятельности выпускников, освоивших программу бакалавриата, включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере. Объектами профессиональной деятельности выпускников, освоивших программу бакалавриата, являются:

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

Сбалансированное сочетание технического и гуманитарного образования делают бакалавра по этому направлению высококвалифицированным специалистом современного уровня. Потребности в таких специалистах чрезвычайно велики во всех областях деятельности.

**Специальность. 10.05.05 Безопасность информационных технологий в правоохранительной сфере**

Область профессиональной деятельности выпускников, освоивших программу специалитета, 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.

Объектами профессиональной деятельности выпускников, освоивших программу специалитета, 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.

**Специальность. 40.05.03 «Судебная экспертиза»**

Область профессиональной деятельности выпускников, освоивших программу специалитета, включает судебно-экспертную деятельность по обеспечению судопроизводства, предупреждения, раскрытия и расследования правонарушений путем использования специальных знаний для обнаружения, фиксации, изъятия и исследования материальных носителей информации, необходимой для установления фактических данных.

Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются свойства и признаки материальных носителей розыскной и доказательственной информации.

**Специальность. 40.05.01 «Правовое обеспечение национальной безопасности»**

Область профессиональной деятельности выпускников, освоивших программу специалитета, включает разработку и реализацию правовых норм, правовое обеспечение национальной безопасности, обеспечение законности и правопорядка, юридическое образование и правовое воспитание. Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются события и действия, имеющие юридическое значение, общественные отношения в сфере реализации правовых норм, правового обеспечения национальной безопасности, обеспечения законности и правопорядка.

**Специальность. 40.05.02 «Правоохранительная деятельность»**

Область профессиональной деятельности выпускников, освоивших программу специалитета, включает разработку и реализацию правовых норм, обеспечение законности и правопорядка, безопасности личности, общества и государства, борьбу с преступлениями и иными правонарушениями, исполнение наказания, юридическое образование и правовое воспитание.

Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются события и действия, имеющие юридическое значение, общественные отношения в сфере реализации правовых норм, осуществления правоохранительной деятельности.

**2.1.2. Магистратура:**

Магистратура Института – четвертая юридическая магистратура в Российской Федерации и первая из магистратур, ориентированная на уголовно-правовую специализацию. Данная образовательная программа позволяет получить высшую юридическую квалификацию в России. Она рассчитана на 2 года. В соответствии с государственным стандартом магистр может заниматься преподавательской, научно-исследовательской деятельностью, а также работать в правоохранительных органах, юрисконсультом, экспертом.

Подготовка осуществляется по следующим магистерским программам:

* Магистратура. 40.04.01.01 «Правовая политика государства: история и современность»
* Магистратура. 40.04.01.02 «Уголовный процесс, криминалистика и теория оперативно-розыскной деятельности»
* Магистратура. 40.04.01.03 «Судопроизводство в Российской Федерации».

**2.1.3. Аспирантура:**

**40.06.01 «Юриспруденция» Уголовное право и криминология; уголовно-исполнительное право (12.00.08).**

Содержанием специальности 12.00.08 – «Уголовное право и криминология; уголовно-исполнительное право» является исследование уголовного законодательства, его источников и отдельных институтов; уголовного права и уголовно-правовых отношений; уголовного законотворчества и практики его применения; исследование преступности как социального негативного явления, структуры и динамики преступности; особенностей причин отдельных видов преступности и их предупреждения; исследование содержания уголовного наказания, его целей задач и порядка исполнения; эффективности наказания и уголовно-исполнительного законотворчества.

Важными направлениями в рамках указанных областей исследования по данной специальности являются предмет и методы правового регулирования, формы и методы достижения целей и задач современной уголовной политики, борьба с преступностью и повышение эффективности исполнения наказания в отношении осужденных, сравнительный анализ уголовного и уголовно-исполнительного законодательства в зарубежных странах, взаимодействие с другими странами по вопросам предупреждения преступности.

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу аспирантуры:

- научно-исследовательская деятельность в области юриспруденции;

- преподавательская деятельность по образовательным программам высшего образования.

Выпускники аспирантуры являются научными кадрами высшей квалификации, способными самостоятельно ставить и решать производственные проблемы в сфере уголовного права и криминологии, уголовно-исполнительного права.

**Руководители программы: Понятовская Татьяна Григорьевна, д.ю.н, профессор.**

**40.06.01 «Юриспруденция» Уголовный процесс (12.00.09)**

Содержанием специальности 12.00.09 – «Уголовный процесс» является разработка проблем и положений уголовного процесса: сущность и основные понятия; источники уголовно-процессуального права; принципы и субъекты уголовного процесса; теория доказательств; возможностей криминалистической науки и их реализация в практике раскрытия и расследования преступлений; изучение закономерностей формирования и развития судебных экспертиз, а также их использования в уголовном судопроизводстве; исследование проблем теории и практики оперативно-розыскной деятельности по обнаружению, предупреждению и раскрытию преступлений, оперативно-розыскному обеспечению расследования и судебного разбирательства уголовных дел, пресечению и нейтрализации криминального противодействия уголовному судопроизводству.

Важными направлениями в рамках указанных областей исследования по данной специальности являются предмет и методы правового регулирования, вопросы совершенствования уголовно-процессуального законодательства, изучение возможностей криминалистической науки и их реализация на практике, рассмотрение закономерностей формирования и развития судебных экспертиз различных классов, современные формы оперативно-розыскной деятельности.

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу аспирантуры:

- научно-исследовательская деятельность в области юриспруденции;

- преподавательская деятельность по образовательным программам высшего образования.

Выпускники аспирантуры являются научными кадрами высшей квалификации, способными самостоятельно ставить и решать производственные проблемы в сфере уголовного процесса, криминалистики и оперативно-розыскной деятельности.

**Руководитель программы: Татьянина Лариса Геннадьевна, д.ю.н, профессор.**

**40.06.01 «Юриспруденция» Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность (12.00.12)**

Содержанием специальности 12.00.12 – «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность» является исследование проблем использования современных возможностей криминалистической науки и их реализации в практике раскрытия и расследования преступлений, а также разрешения дел в суде; закономерностей формирования и развития судебных экспертиз различных классов, родов и видов, типизации их объектов, задач, методов исследования, а также ситуаций и форм использования этих возможностей в судопроизводстве; проблем теории и практики оперативно-розыскной деятельности по обнаружению, предупреждению и раскрытию преступлений, оперативно-розыскному обеспечению расследования и судебного разбирательства уголовных дел, пресечению и нейтрализации криминального противодействия уголовному судопроизводству.

Важными направлениями в рамках указанных областей исследования по данной специальности является изучение возможностей криминалистической науки и их реализация на практике, рассмотрение закономерностей формирования и развития судебных экспертиз различных классов, современные формы оперативно-розыскной деятельности.

Предмет научных исследований, проводимых в рамках данной специальности, составляют закономерности собирания, исследования, оценки и использования доказательств при расследовании преступлений, специальные средства и методы судебного исследования доказательств и предотвращения преступлений; научные, правовые, организационно-управленческие, морально-этические, методологические основы судебно-экспертной и оперативно-розыскной деятельности.

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу аспирантуры:

- научно-исследовательская деятельность в области юриспруденции;

- преподавательская деятельность по образовательным программам высшего образования.

**Руководители программы: Каминский Александр Маратович, д.ю.н, профессор.**

**40.06.01 «Юриспруденция» 12.00.06 – «Природоресурсное право; аграрное право; экологическое право»**

Содержание специальности 12.00.06 – «Природоресурсное право; аграрное право; экологическое право» являются исследованиями законодательства и регулируемых им отношений в сфере определения правового режима природных ресурсов, правового статуса субъектов, их использующих. Изучению в рамках данной специальности подлежат федеральное законодательство Российской Федерации и законодательство субъектов Российской Федерации и разработка предложений по их совершенствованию, нормы международного права и практика международных организаций и судебных органов по урегулированию экологических правоотношений, законодательство зарубежных стран; правовое регулирование земельных отношений, правоотношения в сфере использования, распоряжения и охраны земли, правового статуса субъектов этих правоотношений, видов прав на землю, оснований возникновения и прекращения данных правоотношений, защиты земельных прав.

Важными направлениями в рамках указанных областей исследования по данной специальности являются предмет и методы правового регулирования, формы и методы государственного управления, экспертизы, контроля и надзора, система и структура экологического права, во взаимосвязи с другими отраслями права; понятия, основные правовые институты и содержание права охраны окружающей среды, природопользования и экологической безопасности; правовой режим охраны и защиты прав и законных интересов государства, общества, юридических лиц.

**Руководитель программы: к.ю.н., доцент Белокрылова Е.А.**

**40.06.01 «Юриспруденция» 12.00.03 – «Гражданское право; предпринимательское право; семейное право; международное частное право»**

Содержанием специальности является исследование и разработка предложений по совершенствованию гражданского и предпринимательского права, норм семейного права и международного частного права, исследование их источников, законности в этой сфере. Изучению в рамках данной специальности подлежат федеральное законодательство Российской Федерации и законодательство зарубежных стран, системы договорных, обязательственных, брачно-семейных и наследственных отношений, имущественных и личных неимущественных отношений в сфере интеллектуальной собственности, а также отношений в сфере контрактного права и международного частного права.

Важными направлениями в рамках указанных областей исследования по данной специальности являются предмет и методы правового регулирования, формы и методы государственного управления, контроля и надзора, правовой режим охраны и защиты прав и законных интересов правообладателей, охрана семейно-брачных отношений, исследование коллизионных норм права, анализ разрешения гражданско-правовых и семенных споров в делах с участием иностранцев.

**Руководитель: к.ю.н., профессор Кузнецова Н.В.**

**2.3. Связи с органами власти, предприятиями, ведущими вузами и институтами РАН**

**2.3.1. Академические партнеры Института.** Институт занимает достойные позиции в Приволжском федеральном округе, поддерживает связи с ведущими вузами России. В числе академических партнеров ИПСУБ:

- Институт законодательства и сравнительного правоведения при Правительстве РФ;

- Институт государства и права РАН;

- Саратовская государственная юридическая академия;

- Уральский государственный юридический университет;

- Южно-Уральский государственный университет и др.

Взаимодействие с названными партнерами осуществляется в рамках защит кандидатских и докторских диссертаций, оппонирования, участия в научных мероприятиях, учебно-методической деятельности и т.п.

**2.3.2. Работодатели.** Институт оказывает существенное влияние на подготовку кадров в Удмуртской Республике. Ежегодное распределение выпускников показывает большой интерес со стороны федеральных ведомств работодателей на территории Удмуртской Республики – органов государственной власти, местного самоуправления, организаций с государственным участием и организаций оборонно-промышленного комплекса, организаций лицензиатов ФСТЭК и ФСБ России, операторов, осуществляющих обработку персональных данных.

В качестве потенциальных работодателей, экспертов образовательных программ, платформ производственной практики выступают:

- Аппарат Главного Федерального инспектора Аппарата полномочного представителя Президента РФ по Приволжскому Федеральному округу;

- Управление Министерства юстиции РФ по Удмуртской Республике;

- Следственное управление следственного комитета РФ по УР;

- МВД УР;

- Управление ФНС РФ по Удмуртской Республике;

- Федеральная инспекция труда по Удмуртской Республике;

- Минприроды УР;

- Министерство информатизации и связи Удмуртской Республики;

- Федеральная служба по надзору в сфере природопользования УР;

- Судебный Департамент;

- Управление мировых судей;

- Управление судебных приставов по УР;

- Нотариальная Палата УР;

- Прокуратура Удмуртской Республики;

- иные Федеральные, региональные и местные органы власти.

А также иные организации:

- Пенсионный фонд РФ;

- Главное бюро медико-социальной экспертизы по УР;

- Федерация профсоюзов Удмуртской Республики;

- Удмуртская республиканская коллегия адвокатов;

- Удмуртская республиканская общественная организация «Союз научных и инженерных общественных отделений»;

- ООО «КОМОС ГРУПП» и др.

**2.3.3. Информационные партнеры:**

- Региональное представительство D-Link в Удмуртской Республике;

- Официальный представитель сети КонсультантПлюс в Удмуртской Республике – ООО НТВП «Кедр-Консультант»;

- ООО «Канкор-ИНФОРМ» (справочно-правовая система «ГАРАНТ») и др.

**2.3.4. Иное партнерское взаимодействие:**

- Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Удмуртской Республике. Студенты Института (направления «Информационная безопасность») входят в состав Молодежной палаты Роскомнадзора от Удмуртской Республики.

- Управление ФСТЭК России по ПФО. Институт входит в состав Совета учебно-методического центра по защите информации Приволжского федерального округа.

- СО АНО «Школа-кроха». Университет выступает партнером Всероссийского командного турнира по компьютерной и информационной безопасности для школьников 1-5 кл. «Киберсфера».

- Филиал ПАО «Ростелеком» в Удмуртской Республике. Филиал выступает соорганизатором конкурса проектов по информационной безопасности для школьников Удмуртской Республики.

- Министерство информатизации и связи Удмуртской Республики. Университет участвует в профориентационных мероприятиях проекта «ИТ вектор образования» Министерства.

В настоящее время в ИПСУБ поддерживает договоры с отечественными организациями (вендорами): «Positive Technologies», «Код безопасности», «КриптоПро». СерчИнформ, Директум, ООО «Новые облачные технологии», АО «НПО РусБИТТех», АО «ИнфоВотч». Ведется работа в рамках Сетевой академии CISCO.

**3. Стратегические цели и показатели развития института**

**3.1. Образовательная деятельность**

**Стратегические цели:**

- поддержка единства учебной, научно-инновационной и воспитательной, творческой деятельности;

- дальнейшее усиление позиций и повышение статуса Института в сфере образовательной деятельности на региональном, федеральном и международном уровнях;

- просветительская работа по направлению кибербезопасности;

- использование в образовательном процессе подготовки специалистов в области информации образовательных платформ, симулирующих бизнес-среду, в которой возникает серия неожиданных киберугроз;

- создание виртуальной среды/центра обработки данных (ЦОД) для обеспечения возможности проведения практических и лабораторных работ с использованием технологии виртуальных машин, применение геймификации;

- создание лаборатории для развития компетенции WorldSkills «Корпоративная защита от внутренних угроз информационной безопасности»;

- продолжение организации профориентационной деятельности со школьниками г. Ижевска и Удмуртской Республики в рамках участия в мероприятиях проекта ИТ-вектора Министерства информатизации и связи Удмуртской Республики;

- разработка траектории обучения студентов, позволяющая получить новые цифровые компетенции в процессе обучения по образовательным программам Института;

- увеличение контингента по ускоренным срокам обучения направлений подготовки и специальностей, реализуемых в Институте.

**3.2. Научная и инновационная деятельность**

**Стратегические цели:**

- обеспечение конкурентоспособного уровня и востребованности выпускников Института на региональном и федеральном уровнях;

- фундаментализация научных исследований, проводимых в Институте;

- расширение спектра научных исследований и работ по приоритетным направлениям развития науки;

- максимальное использование научного потенциала Института в повышении качества образования и развития научной деятельности Института.

**3.3. Воспитательная деятельность и развитие корпоративной культуры**

**Стратегические цели:**

- совершенствование форм и методов воспитательной работы с учетом особенностей современного общества и специфических условий многонациональной Удмуртской Республики;

- формирование адекватного отношения коллектива к изменившимся правилам жизни вуза в конкурентной среде;

- осознание, усвоение и разделение большинством коллектива основных элементов корпоративной культуры, формирование корпоративной социальной ответственности на всех уровнях управления;

- повышение общего уровня культуры информационной безопасности обучающихся;

- минимизация рисков современной системы обеспечения информационной безопасности обучающихся.

**3.4. Деятельность по укреплению и развитию социальной сферы**

**Стратегические цели:**

- дальнейшее развитие системы социальной защиты и поддержки работников и обучающихся в Институте;

- создание условий для охраны здоровья работников и обучающихся в Институте;

- создание системы защиты прав и интересов работников и обучающихся в Институте.

**3.5. Деятельность в области цифровизации**

Сложившаяся регламентация учебного процесса осложняет реализацию задачи персонализации обучения, внедрения в образовательный процесс инновационных траекторий образования, позволяющих студентам получать необходимые знания, умения и навыки в области цифровых технологий. В соответствии с тенденциями, сложившимися в современной экономической сфере, а также задачами в области цифровизации общества, требуется от образовательных учреждений изменения образовательной парадигмы в подготовке обучающихся и построения новой модели-выпускника, который будет соответствовать современным реалиям и удовлетворять запросом работодателей. В связи с этим возникает необходимость:

- разработки новых программ обучения обучающихся, направленных на развитие общей цифровой грамотности, формирующих цифровые компетенции, позволяющие выпускникам юридических вузов свободно интегрироваться в цифровую экономику;

- предоставления возможности Институту и внедрять в учебный процесс основные образовательные программы обучения студентов, учитывающие специфику потребностей цифровой экономики;

- подготовки нового поколения преподавателей Института, способных разрабатывать и решать задачи правового обеспечения цифровой экономики, создавать образовательный контент, в том числе в мобильном варианте, актуальный для рынка цифровых услуг, с использованием цифрового инструментария в оболочках электронных учебников и учебных пособий с визуализацией и аудио сопровождением;

- создания программы переподготовки педагогических работников Института, адаптированных к решению задач инновационного внедрения современных цифровых технологий в образовательный процесс;

- актуализации образовательных технологий с учетом внедрения в образовательный процесс персональных траекторий обучения, позволяющих студентам выбирать формальные, неформальные, информальные способы формирования базовых цифровых компетенций, вводить новые формы аттестации выпускников с привлечением работодателей, имеющих опыт работы на торговых цифровых площадках, с цифровыми продуктами и стартапами;

- приведения в соответствие с требованиями цифровизации общества материально-технической базы и информационно–образовательной среды Института.

**Стратегические цели:**

- выведение Института на уровень информатизации и использования новых цифровых технологий обучения, достигнутый наиболее развитыми вузами России;

- реализация концепции «опережающего образования» и создания условий для открытого образования с использованием новых цифровых технологий;

- подготовка выпускников Института к профессиональной деятельности в условиях цифрового общества.

**3.6. Организационно-управленческая деятельность**

**Стратегические цели:**

- совершенствование системы управленческих мероприятий по улучшению условий для профессиональной деятельности работающих и образовательной деятельности обучающихся;

- переход на внутренний безбумажный документооборот.

**3.7. Финансово-экономическая деятельность**

**Стратегические цели:**

- обеспечение финансовой устойчивости Института;

- развитие и использование механизма многоканального финансирования Института;

- совершенствование механизма определения приоритетности в распределении и использовании финансовых средств;

- поиск возможностей увеличения объема финансовых средств для улучшения материального положения работающих в Институте;

- обеспечение разумного и экономного расходования средств для финансирования основных видов деятельности Института.

**Показатели развития Института:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Показатели | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 |
| Приведенный контингент чел.\* | 1292,3 | 1196,5 | 1163,2 | 1143,4 | 1143,4 | 1143,4 | 1143,4 |
| Доходы от образовательной деятельности млн.руб.\*\* | 145,449 | 144,468 | 143,124 | 143,543 | 145,620 | 147,068 | 148,686 |
| Объемы НИР, млн.руб. | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 |
| Публикации WoS Scopus | 3 | 3 | 4 | 4 | 4 | 4 | 5 |
| Доля НПР моложе 35 лет, % | 8 чел. (7,14%) | 8 | 9 | 9 | 9 | 10 | 10 |
| Количество штатных докторов наук, чел. | 12 чел. (10,71%) | 12 | 13 | 13 | 13 | 14 | 14 |
| Объем ДО, млн. руб. | 0,456 | 0,355 | 0,355 | 0,355 | 0,366 | 0,376 | 0,387 |

\*Снижение контингента и доходов с 2020 года обусловлено прекращением набора по направлению подготовки «Документоведение и архивоведение».

\*\* Могут быть добавлены доходы от платного обучения аспирантов.

**4. Стратегические единицы Института**

**4.1. Научно-образовательные и научные центры (направления деятельности и решаемые задачи в науке, экономике, социальной сфере; партнеры; источники финансирования)**

**4.1.1. НОЦ «Экспертно-правовой центр»**

**Структура НОЦ:**

экспортный сектор;

сектор правовых экспертиз;

- консультационно-миграционный сектор;

- сектор правовой охраны использования результатов интеллектуальной деятельности;

- эколого-правовой сектор.

**Функции НОЦ:**

Консультационные услуги с привлечением внутренних и сторонних профильных экспертов по широкому кругу правовых вопросов.

Формирование реального и «онлайн» центра ведения переговоров.

Экспертиза и сопровождение экспортного контракта.

Содействие в обеспечении защиты интеллектуальной собственности за пределами территории Российской Федерации, в том числе получении патентов на результаты интеллектуальной деятельности.

Поиск партнеров для субъекта малого и среднего предпринимательства.

Обучение экспортно-импортной деятельности.

Участие в качестве правовых экспертов в эколого-инженерном сопровождении проектов промышленной деятельности высокого класса опасности.

Участие в общественных и государственных экологических экспертизах по проектам намечаемой промышленной, производственной и хозяйственной деятельности.

Участие в процедуре оценки воздействия на окружающую среду по проектам намечаемой промышленной, производственной и хозяйственной деятельности.

Разработка рекомендаций по совершенствованию действующего законодательства в области охраны окружающей среды и природопользования.

Подготовка сравнительно-правовых исследований в области охраны окружающей среды и природопользования.

Потенциальные партнёры: Council of Europe, Swiss Institute of Comparative Studies, Минприроды и экологии РФ, НИЦ «Курчатовский Институт», РосНано, РосРАО, Минприроды УР и т.д.

**4.1.2. Региональный учебно-научный центр по проблемам информационной безопасности в системе высшей школы «Информбезопасность»**.

Создан приказом Федерального агентства по образованию РФ № 126 от 9 марта 2005 года на базе Государственного образовательного учреждения высшего профессионального образования «Удмуртский государственный университет» в целях совершенствования подготовки специалистов по проблемам информационной безопасности.

Целью центра является оказание образовательных, учебно-методических, консультационных услуг в области информационной безопасности

Задачи центра:

повышение квалификации специалистов в области защиты информации;

проведение научно-исследовательских и опытно-конструкторских работ в области информационной безопасности с привлечением профессорско-преподавательского состава, аспирантов, студентов, а также ведущих специалистов организаций, учреждений и предприятий;

анализ предлагаемых на рынке средств защиты информации, а также их тестирование.

**Функции:**

- разработка программ дополнительного профессионального образования для подготовки квалифицированных кадров в области информационной безопасности и защиты государственной тайны в органах государственной власти и местного самоуправления, организациях оборонно-промышленного комплекса, учреждениях и организациях Удмуртской Республики;

- подготовка кадров для цифровой экономики (информационная безопасность);

- создание авторизованного центра подготовки с компанией «Код Безопасности» (г. Москва).

**Приоритетные направления деятельности Центра совместно с кафедрой «Информационная безопасность в управлении»:**

проведение работ по защите объектов информатизации;

организация и проведение работ по защите государственной тайны и конфиденциальной информации;

проведение прогнозных оценок развития и обеспечения безопасности региональных информационных систем;

участие в разработке концепции информационной безопасности региона;

организация и технология документирования управленческой деятельности предприятий;

разработка и реализация программ по повышению квалификации работников органов государственной власти и местного самоуправления, организаций и предприятий региона в области информационной безопасности;

проведение семинаров и конференций регионального уровня по проблемам защиты информации.

**4.2. Центры компетенций**

**4.2.1. Региональный Центр правовых компетенций на базе Удмуртского государственного университета.**

1. Стратегическое направление:

- мониторинг развития правового онлайн-обучения;

- формулировка перспективных онлайн-курсов;

- составление перспективных планов развития правового онлайн-образования в УР.

2. Технологическое направление:

- разработка правовых онлайн-курсов;

- актуализация и сопровождение онлайн-курсов;

- экспертиза правовых онлайн-курсов.

3. Направление развития кадрового потенциала

- разработка рабочих программ дополнительного обучения в сфере юриспруденции

- организация онлайн-курсов в сфере повышения правовой квалификации;

- документальное и методическое сопровождение онлайн-курсов в сфере повышения правовой квалификации.

Потенциальные партнёры: ФГБОУ ВО «Саратовская государственная юридическая академия», ФГБОУ ВО «Уральский государственный юридический университет».

**5. Стратегические проекты института (до 2025 г.)**

**5.1. Проекты в сфере образования (крупные программы ВО и ДО)**

**5.1.1. Проект «IT-Юрист»**. За счет грантозаявительной деятельности (РФФИ, РНФ). Ответственные: к.ю.н., доцент Белокрылова Е.А, к.ю.н., доцент Люминарская С.В., ст. преподаватель Колчерина Ж.Н.

**Описание**. В настоящее время наиболее востребованными считаются юристы, специализирующиеся в сфере информационных технологий в различных областях права. Спрос на юристов в IT-отрасли последние годы устойчиво возрастает.

Традиционно работа юриста в области IT-технологий сводится к защите прав в сфере разработки, установки и обслуживания программного обеспечения, хранения и обмена данными на серверах и веб-сайтах, но границы правового поля постепенно расширяются и уже сегодня охватывают правоотношения граждан при электронном обмене информацией, общении в соцсетях, создании бизнес-моделей в интернете и иных технологически инновационных продуктах. Одновременное развитие цифровых технологий и происходящие в связи с этим изменения в законодательстве открывают для современных юристов большие перспективы.

Многие IT-юристы преимущественно практикуют в коммерческом праве в контексте использования цифровых технологий (электронный нотариат, судопроизводство и т.д.), а также предлагают свои услуги в решении конкретных правовых проблем в IT-инфрастркутуре, облачных сервисах, соглашениях по предоставлению SaaS, разработке и лицензировании программного обеспечения. Значительная часть IT-юристов специализируются еще более узко и предоставляют услуги конкретно по мониторингу, лицензированию и защите интеллектуальной собственности. Юристы, обладающие цифровыми компетенциями, впоследствии могут стать крайне востребованными специалистами.

Еще одна область IT-права, которая становится все более востребованной, но связана с более сложным правовым регулированием – кибер-право. Интернет превратился в крупную площадку для создания, ведения и развития крупных бизнес-проектов. Современное законодательство еще недостаточно подробно регулирует эту новую сферу, беря за основу международный опыт и действующее международное законодательство. В киберпространстве совершаются как специфические правонарушения, такие как нарушение прав интеллектуальной собственности (авторские, патентные права, права на секрет-производства), так и «обычные преступления» – мошенничество, вымогательство, незаконное предпринимательство и т.п. Одновременно крупные компании должны создать такую надежную защиту IT-систем, в которых хранятся конфиденциальные данные, чтобы такие системы могли противостоять кибер-атакам.

IT-юристам необходимо обладать компетенциями в сфере договорного законодательства, права интеллектуальной собственности, регулирования защиты персональных данных, хранения и передачи информации, в том числе и в электронном виде и т.д. В настоящее время рядом юридических лиц уже начинают создаваться IT-юридические отделы либо вводиться в штат отдельные должности IT-юристов. Среди адвокатских коллегий уже появляются такие, которые оказывают услуги исключительно по вопросам кибер-безопасности, следовательно, актуальность подготовки юристов в данной направлении крайне высока.

Уже сегодня презентованы широкой аудитории такие программные продукты как: *Autolawyer*(бот, который позволяет сформировать жалобу в страховую компанию на неправильно определенный коэффициент бонус-малус для ОСАГО); *Platforma*(подыскивает адвокатов, работающих по модели «no win no fee», когда адвокат получает вознаграждение только в случае выигрыша дела и взыскания денег истцом); *Flexbby*(автоматизирует документооборот);  Jeffit (решает стандартные задачи – ставит в календарь информацию о судебных заседаниях, выставляет счета клиентам и т.п.); *XSUD*(систематизирует информацию о судебных делах и контролирует работу сотрудников); *Patentbot*(позволяет автоматически подать заявку на регистрацию товарного знака, проверив предварительно его оригинальность);  *Freshdoc* (составляет договоры из модулей); *Simplawyer*(предлагает решения в области самоисполняемых договоров); *Правовед.ру* (сервис по консультациям массовых клиентов – бот, который отвечает на 85% вопросов по Закону о защите прав потребителей).

Отдельное место занимают технологические платформы по маркетплейсменту юристов, позволяющие подобрать специалиста под определенные задачи, с учетом специализации, стоимости услуг и других параметров. Подобные проекты созданы в США, Великобритании и России (*Lexoo,  Avvo и Legal Space* соответственно). По сути, речь идет об уберизации рынка юридических услуг.

Создание юридических программных продуктов позволит уже в ближайшем будущем существенно видоизменить как структуру юридического рынка услуг, так и саму профессию юриста. В самое ближайшее время legal research, простейший правовой анализ, составление типовых документов станут уделом искусственного интеллекта, что позволит вывести работу юристов на более высокий профессиональный уровень, а также обострить конкуренцию на старте юридической карьеры для выпускников высших учебных заведений.

Помимо этого, необходимо учитывать, что цифровые технологии уже сегодня нуждаются в серьезной правовой поддержке на уровне регулирования их функционирования и применения, следовательно, цифровизация юриспруденции предопределяет принципиально новый этап развития сопутствующих отраслей права. В первую очередь, это касается гражданского, уголовного, административного, финансового права, а также процессуальных правовых отраслей. Особая роль в этом процессе отведена развитию информационного права.

Нормативное регулирование цифровой экономики, институциональные преобразования, связанные с цифровизацией и автоматизацией, переориентирование государственного управления от воспроизводства процессов к управлению изменениями, определение правового статуса криптовалют – всё это вызовы, стоящие в первую очередь перед отечественной правовой системой, отвечать на которые будет призвано юридическое сообщество. Развитие технологических инструментов, усиление отраслей права, регулирующих вопросы защиты информации, а также указанные выше задачи позволят сформироваться самостоятельным юридическим практикам нового типа, новым профессиональным направлениям.

Учитывая объективность процесса цифровизации, а также огромный потенциал внедрения технологий в профессию юриста, стоит обратить внимание на возрастающее значение юридического образования, которое должно обеспечивать фундаментальную межотраслевую подготовку профессиональных кадров. Поэтому крайне важно проводить постоянную актуализацию знаний, предлагаемых обучающимся. Необходимы новые подходы в подготовке юристов, позволяющие будущим профи научиться правильно формировать правовую позицию, аргументировать и доносить ее публично, проводить переговоры, и наконец – эффективно использовать профессиональные технологические инструменты.

Программой «Цифровая экономика в Российской Федерации» (утверждена распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р) предусмотрено к концу первой половины 2019 года принятие программ обучения юристов в сфере цифровой экономики, поэтому очень важно, чтобы в данный процесс были вовлечены крупнейшие научные центры, университеты. В конечном счете, именно фундаментальное современное и динамично развивающееся юридическое образование должно стать драйвером развития профессии юриста в условиях глобальной цифровизации.

**Проект предполагается осуществлять по двум основным направлениям:**

1. Обучение профессорско-преподавательского состава Института новым цифровым технологиям, встраиваемым в образовательный процесс (Институт математики, информационных технологий и физики);

2. Подготовка и реализация учебных дисциплин, необходимых для подготовки IT-юриста (на каждой из кафедр Института следует выделить 2-3 преподавателей, адаптирующих существующие учебные дисциплины в соответствии с компетенциями цифровой экономики).

**Основные направления развития отдельных отраслей юриспруденции, возникающие в связи с развитием цифровой экономики:**

1) развитие отдельных отраслей законодательства в целях их адаптации к цифровой экономике:

– гражданского законодательства (развитие законодательства о сделках в условиях цифровизации; законодательная регламентация оборота виртуальных объектов в цифровом пространстве без использования законных платежных средств как единиц расчета и непосредственного взаимодействия контрагентов как сторон обязательства; цифровизация публичных реестров юридических лиц и индивидуальных предпринимателей);

– трудового и социального законодательства в части, касающейся правовой защиты граждан от безработицы в условиях информационных технологических новаций в сфере труда и социального обеспечения, выявления барьеров, затрудняющих формирование гибких трудовых отношений, перспектив принятия нормативных правовых актов, обеспечивающих регулирование трудовых отношений с гибкой и дистанционной занятостью в условиях цифровой экономики;

– финансового законодательства;

– законодательства о судопроизводстве (цифровизация правосудия);

– законодательства об исполнительном производстве, включая развитие электронного взаимодействия между участниками процесса, судами, службой судебных приставов, организациями, администрирующими проведение процедуры медиации, иными органами и организациями при исполнении судебных решений;

– законодательства об альтернативных способах разрешения споров в части создания электронной системы альтернативных механизмов разрешения споров (электронная медиация и онлайн-разрешение споров), включая определение спектра инструментов, используемых для урегулирования споров онлайн; применение алгоритмов автоматизированного разрешения простых однотипных споров он-лайн; проведение пилотных проектов по внедрению таких механизмов; создание условий для повышения уровня доверия участников экономического оборота к онлайн-механизмам урегулирования споров и т.п.;

– законодательства о нотариате, в том числе в части дистанционного совершения нотариальных действий;

– законодательства об информации, документообороте, отчетности;

– законодательства об интеллектуальных правах, включая поощрение использования результатов интеллектуальной деятельности для нужд цифровой экономики в части облегчения регистрационных процедур; применение технологии блокчейн в авторском праве; создание правового режима 3D-модели как объекта интеллектуально-правовой защиты и регулирования;

– комплексных отраслей законодательства в части оборота данных; искусственного интеллекта; технологий децентрализованного ведения реестров с учетом предложений, сформированных в рамках дорожных карт Национальной технологической инициативы, Стратегии научно-технологического развития и др. к следующим отношениям:

создания и использования специальных правовых режимов для организаций, ведущих деятельность в приоритетных видах деятельности цифровой экономики и (или) имеющих определенный уровень информатизации процессов с учетом положений концепции управления изменениями;

формирования инструментов стимулирования развития цифровой экономики;

определения принципов и подходов к международному регулированию отношений в цифровой среде;

использования цифровых технологий при осуществлении контрольно-надзорных функций, а также функций, связанных с обжалованием действий и решений органов контроля, привлечением к административной ответственности подконтрольных субъектов;

определения направлений корректировки и примерного перечня административных регламентов и иных норм, принципиально допускающих автоматическое воздействие на юридические и физические лица, автоматическое исполнение (принципы автоматического исполнения, предметная направленность регламентов);

комплексного регулирования робототехники и киберфизических систем, в том числе: определения понятия киберфизических систем, порядка ввода их в эксплуатацию и гражданский оборот, определения ответственности; определения основных мер государственного содействия развитию сферы робототехники и киберфизических систем, в том числе по управлению национальной программой развития робототехники и кибер-физических систем.

2) *регулирование (модернизация регулирования) общественных отношений, связанных со сбором, передачей, хранением, обработкой и доступом к информации с использованием информационных технологий, в частности:*

– деятельности по сбору, передаче, хранению, обработке и доступу к данным, генерируемым в процессе использования информационных технологий физическими и юридическими лицами;

– единых стандартов сбора, хранения, обработки, обмена данными («интероперабельность данных»);

– порядка раскрытия информации, в том числе в форме открытых данных;

– определение возможности введения принципа раскрытия данных по умолчанию в деятельности органов государственного управления;

– определение условий и порядка обработки и доступа, в том числе коммерческого недискриминационного, к данным, генерируемым без участия человека (данные «интернета вещей» и «индустриального интернета»), при условии обязательного соблюдения прав создателей и изготовителей систем и баз данных;

– определение подходов и предложений по корректировке законодательства с целью обеспечения недискриминационного и равного доступа организаций к данным, которые аккумулируются в государственных информационных системах (ГИС) в силу закона, условия получения информации из ГИС в порядке оказания государственной услуги;

– определение принципов, условий и режима предоставления доступа к данным о работе промышленного оборудования в целях осуществления НИР и ОКР.

3) *регулирование (модернизация регулирования) общественных отношений, связанных с обработкой персональных данных:*

– модернизация правового режима персональных данных, обезличенных данных, пользовательских (поведенческих) и больших данных, а также сведений, составляющих тайну личной жизни, семейную тайну, тайну частной жизни;

– установление основ правового режима «общедоступных персональных данных», возможных действий и целей обработки общедоступных персональных данных;

– определение понятийного аппарата, в том числе понятия «общедоступные персональные данные».

4) *регулирование (модернизация регулирования) общественных отношений, связанных с режимом различных видов тайн:*

– определение основ правового режима сведений, составляющих банковскую тайну, тайну связи, врачебную, налоговую, коммерческую, государственную тайну и иные виды тайн;

– определение принципов обработки составляющих из сведений и возможность передачи третьим лицам при условии соблюдения и защиты прав субъектов.

5) *регулирование (модернизация регулирования) общественных отношений, связанных с оборотом больших данных:*

– процессов формирования, хранения, систематизации, обработки (в т.ч. без участия человека) и оборота больших данных, включая режимы доступа и права участников такого оборота и третьих лиц в части:

идентифицирующих и персональных данных, в том числе геолокационных, а также «цифровых двойников»;

пользовательского контента;

информации, формируемой пользователем опосредовано (т.н.  »цифровой след»);

информации о работе оборудования;

передачи данных между устройствами (т.н. «интернет вещей»);

механизмов правовой защиты указанной информации;

правил и механизмов обмена данными между субъектами цифровой экономики;

недискриминационного доступа к ним,

ответственности за несанкционированный доступ,

классификации данных с учетом требований по доступности и информационной безопасности,

определения подходов к созданию системы управления данными, в том числе исходя из источников и средств генерации данных (человек, машина);

регулирования прав на сбор данных в зависимости от волеизъявления субъектов, условий по обработке и коммерческому использованию таких данных, механизмов сбора и использования больших массивов данных.

6) *регулирование (модернизация регулирования) общественных отношений, связанных с техническим регулированием и стандартизации:*

– определение возможностей инструментов технического регулирования для развития цифровой экономики;

– совершенствование механизмов стандартизации, технического регулирования и единства измерений для целей развития цифровой экономики, включая формирование соответствующей нормативной правовой базы, а также библиотеки действующих национальных стандартов по приоритетным направлениям в машиночитаемом формате;

– определение механизмов государственной поддержки организаций, принимающих участие в разработке международных стандартов в рамках международных организаций по стандартизации;

– определение правового регулирования установления требований к формированию единых стандартов сбора, хранения, обработки, обмена данными («интероперабельность данных»);

– определение правовых подходов к формированию перечня стандартов по сквозным технологиям, определению возможности использования сквозных технологий в нормативном регулировании цифровой экономики;

– определение общих подходов к нормативному правового регулированию технологий в сфере «Умный город».

7) *регулирование (модернизация регулирования) общественных отношений, связанных с телекоммуникационной отраслью:*

– правовое регулирование телематических систем, в том числе систем автотранспортной телематики, включая требования о некорректируемости данных, формата сбора, передачи, обработки и хранения данных, юридической значимости данных, передаваемых от оборудования в телематические системы, а также круга субъектов, несущих обязанности по сбору и передаче данных в информационные системы для обеспечения государственных, муниципальных и иных нужд;

– изменение действующего законодательства в части установления требований к пользовательскому телекоммуникационному оборудованию по обеспечению возможности недискриминационного доступа программного обеспечения к функционалу оборудования.

8) *регулирование (модернизация регулирования) общественных отношений, связанных с развитием киберспорта, созданием благоприятных условий для взаимодействия между субъектами киберспорта*.

9) *регулирование (модернизация регулирования) общественных отношений, связанных с финансовыми технологиями:*

– совершенствование правового регулирования налогообложения в условиях цифровой экономики;

– цифровой учет финансовых ресурсов (бюджетный, налоговый, бухгалтерский);

– формирование предложений по цифровизации бюджетного процесса;

– определение понятийного аппарата, включая «цифровой бюджет», «цифровой налог».

10) *регулирование (модернизация регулирования) общественных отношений, связанных с цифровой экономикой 2.0:*

– определение механизма заключения смарт-контрактов;

– определение правовой природы токенов и криптовалюты, как платежных средств, опосредующих имущественный обмен в цифровой среде;

– определение понятийного аппарата, включая понятие «цифровой товар (объект)».

**5.1.2. Портфель проектов «Формирование доверенной среды информационного общества в условиях существования угроз различного характера»**.

Руководитель портфеля проектов: Колчерина Жанна Николаевна, ст. преподаватель кафедры информационной безопасности в управлении.

Сроки реализации портфеля проектов: до 2025 г.

**Компоненты портфеля проектов:**

Подготовка управленческих и инженерных кадров в области информационной безопасности в рамках программы «Кадры для цифровой экономики»;

Кибербезопасность детей в цифровом пространстве;

1. Пилотный проект «Создание частного облака на основе отечественного программного обеспечения (в рамках перехода на отечественное программное обеспечение)» в ФГБОУ ВО «Удмуртский государственный университет»;
2. Создание лаборатории на базе Института совместно с вендорами информационной безопасности для подготовки специалистов по защите информации (ВО и СПО) в Республике.

**Цель реализации портфеля проектов**: создание информационного пространства путем развития науки, реализации образовательных и просветительских проектов в Удмуртской Республике, создания для граждан общедоступной системы взаимоувязанных знаний и представлений, обеспечения безопасной информационной среды для детей в Удмуртской Республике.

**Задачи реализации портфеля проектов:**

- разработка программ дополнительного профессионального образования для управленческих и инженерных кадров в области информационной безопасности в Удмуртской Республике;

- повышение общего уровня культуры информационной безопасности и популяризация знаний в области информационной безопасности;

- минимизация рисков современной системы обеспечения информационной безопасности, связанных с развитием сети «Интернет» и информационных технологий, нарастающим противоправным контентом;

- тестирование отечественного программного обеспечения в образовательном процессе в рамках программы импортозамещения;

- формирование медиакомпетенций в области информационной безопасности детей, подростков и молодежи в процесс социально-экономического развития Удмуртской Республики в рамках цифровой экономики региона.

**Ключевые участники портфеля проектов:**

1. **Структурные подразделения университета – участники портфеля проектов:**

Институт права, социального управления и безопасности.

Региональный учебно-научный центр по проблемам информационной безопасности в системе высшей школы «Информбезопасность».

**2) Внешние участники портфеля проектов:**

- Органы государственной власти.

- Органы местного самоуправления.

- Организации с государственным участием и организациях оборонно-промышленного комплекса.

- организации лицензиаты ФСТЭК и ФСБ России.

- операторы, осуществляющие обработку персональных данных.

- Управление ФСТЭК России по ПФО.

- ГНИИ ПТЗИ ФСТЭК России (Воронеж).

- ФСТЭК России.

- Управление Роскомнадзора по Удмуртской Республике.

- Региональный центр информатизации и оценки качества образования.

- Удмуртский филиал ПАО «Ростелеком».

- Федерация киберспорта.

- Министерство информатизации и связи Удмуртской Республики.

- МВД по Удмуртской Республике.

- Управление образования по Удмуртской Республике.

- Муниципальные образовательные учреждения среднего общего образования г. Ижевска.

Источники финансирования ИПСУБ, УДГУ, РУНЦ.

**5.1.3. Автоматизированная платформа обучения навыкам кибербезопасности: Kaspersky Automated Security Awareness Platform (ASAP).**

Стремительное развитие информационных и коммуникационных технологий, цифровизация общества, увеличение числа объектов информационной инфраструктуры, подключенных к сети Интернет, выводят на первый план вопросы обеспечения информационной безопасности. Деятельность по обеспечению безопасности информации в организациях любых форм собственности осуществляют специалисты по защиты информации. Сегодня это направление включает в себя виды деятельности, связанные с защитой информации в компьютерных системах и сетях, технической защитой информации, обеспечением безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере, и т.п. Выпускники направления «Информационная безопасность» должны уметь своевременно выявлять угрозы информационной безопасности, противодействовать атакам, предупреждать действия злоумышленников, обеспечивать безотказное функционирование информационной инфраструктуры, в условиях существования угроз различного характера. Учитывая, стремительное развитие ИТ отрасли необходимо пересмотреть подход к подходе выпускника по информационной безопасности и включать в процесс обучения разработки вендеров в части использования виртуальных стендов, программных продуктов для подготовки специалиста, в том числе для подготовки к WorldSkills Россия по компетенции «Корпоративная защита от внутренних угроз информационной безопасности», образовательных платформ для повышения осведомленности и т. п.

Результаты проекта могут использоваться в подготовке не только специалистов по защите информации, но и не относящихся к области информационной безопасности.

KIPS — это игровой тренинг, погружающий специалистов по IT-безопасности из коммерческих компаний и правительственных учреждений в симулированную бизнес-среду в которой возникает серия неожиданных киберугроз. В условиях реалистичных атак командам необходимо найти баланс между приоритетами технологического процесса, бизнеса и безопасности. Они анализируют данные и принимают стратегические решения на основе неполной информации и ограниченных ресурсов. Таким образом создается приближенная к жизни ситуация: в основе каждого сценария лежат события, которые могут произойти на самом деле.

Повысить осведомленность участников о рисках и проблемах безопасности, связанных с использованием современных компьютерных систем, выработать стратегический подход к проблемам кибербезопасности и научить представителей разных подразделений согласованным действи ям по предотвращению и отражению кибератак.

Ориентировочная стоимость проекта: 1 600 000 руб.

**5.1.4. Профориентационная работа**

Профориентационная работа со школьниками в Институте уже ведется по следующим направлениям и охватывает школьников с 7-11 классы:

1. Олимпиады школьников:

- региональная олимпиада по праву,

- межрегиональная олимпиада по информатике и компьютерной безопасности им. И.Я. Верченко и межрегиональная олимпиада по математике и криптографии им.И.Я. Верченко, проводимые Академией ФСБ России, Академией криптографии Российской Федерации, совместно с Федеральным учебно-методическим объединением в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (Институт выступает очной площадкой проведения олимпиады).

2. Участие в профориентационных мероприятиях проекта «ИТ вектор» Министерства информатизации и связи Удмуртской Республики, фестиваль «Мир ИТ профессий» на площадках образовательных организаций Удмуртской Республики.

3. Детский лагерь «Территория права».

4. Интерактивные игры со школьниками по направлению «Информационная безопасность» совместно с УНБ им. В.А. Журавлева.

5. Конкурс проектов по информационной безопасности в образовательных организациях Удмуртской Республики в рамках проекта «ИТ-вектор» Министерства информатизации и связи Удмуртской Республики.

**5.2. Научные проекты**

**5.2.1. Междисциплинарный проект «Анализ юридических рисков в сфере цифровизации образования**» За счет грантозаявительной деятельности (РФФИ, РНФ). Ответственные: к.ю.н., доцент Белокрылова Е.А, к.ю.н., доцент Люминарская С.В.

**Описание проекта:** в настоящее время цифровизация как основной тренд серьезно корректирует деятельность профессиональных юридических сообществ, а государственные институты стоят на пороге серьезных технологических преобразований. Эксперты отмечают, что бизнес и государство заинтересованы в алгоритмизации правовых процессов и нормотворчества, которая позволит снизить транзакционные издержки, а также повысить эффективность их деятельности. Тем не менее, по некоторым оценкам, уровень проникновения цифровых технологий в юриспруденцию в настоящее время составляет не более 30 процентов, а доля доступных юридических онлайн-услуг не превышает 4-5 процентов от общего рынка.

Сегодняшние юристы не могут представить свою работу без справочно-правовых систем, которые позволили повысить уровень законотворчества и правоприменения, а также сэкономить огромное количество времени и сил профессиональных юристов. Ведь если раньше юристам было необходимо выписывать газеты и журналы с официальными текстами нормативных актов, актуализировать их, систематизировать, формировать картотеки, то сегодня все эти функции выполняют справочно-правовые системы, позволяющие в несколько кликов получить полную фактуру по конкретному вопросу, сформировав подборку нормативно-правовых актов, судебной практики, доктринальных позиций («Консультант Плюс», «ГАРАНТ» - в России, «Judicata», «Everlaw» – в США,  »INFOLEX», «PRESTEL», «LEXIS» – в Великобритании и т.д.).

Все вышесказанное является не только преимуществами в области цифровизации юриспруденции, но и определёнными вызовами в сфере защиты прав, свобод и законных интересов граждан.

В настоящее время действующие правовые нормы не обеспечивают в полной мере системного подхода к формированию цифровой экономики. Применение несистематизированных правовых норм и требований, разработанных для традиционной экономики и соответствующих ее условиям, к отдельным механизмам цифровой экономики приводит к фрагментарности регулирования в этой области и не позволяет в полной мере реализовать заявленные преимущества цифровой экономики.

Общественные отношения, возникающие в связи с развитием цифровой экономики, обладают существенной спецификой в части их объекта и предмета, субъектного состава, условий возникновения, изменения и прекращения, что обуславливает необходимость их комплексного исследования, особенно в части имеющихся потенциальных рисков, связанных с защитой персональных данных, интеллектуальной собственности, чести и достоинства граждан, клеветой и пр.

**Существующие риски в сфере сбора, передачи, хранения, обработки и доступа к информации с использованием информационных технологий.**

– регулирование деятельности по сбору, передаче, хранению, обработке и доступу к данным, генерируемым в процессе использования информационных технологий физическими и юридическими лицами;

– правовому регулированию единых стандартов сбора, хранения, обработки, обмена данными («интероперабельность данных»);

– установление порядка раскрытия информации, в том числе в форме открытых данных;

– определение возможности введения принципа раскрытия данных по умолчанию в деятельности органов государственного управления;

– определение условий и порядка обработки и доступа, в том числе коммерческого недискриминационного, к данным, генерируемым без участия человека (данные «интернета вещей» и «индустриального интернета»), при условии обязательного соблюдения прав создателей и изготовителей систем и баз данных;

– определение подходов и предложений по корректировке законодательства с целью обеспечения недискриминационного и равного доступа организаций к данным, которые аккумулируются в государственных информационных системах (ГИС) в силу закона, условия получения информации из ГИС в порядке оказания государственной услуги;

– определение принципов, условий и режима предоставления доступа к данным о работе промышленного оборудования в целях осуществления НИР и ОКР.

Общественные отношения, связанные со сбором, передачей, хранением, обработкой и доступом к информации, базируются на конституционной норме статьи 29 Конституции Российской Федерации: «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Российское законодательство достаточно полно регулирует указанные отношения, однако активное использование современных информационно-телекоммуникационных технологий выявило проблемы, требующие своего решения.

**Риски в области реализации деятельности по сбору, передаче, хранению, обработке и доступу к данным, генерируемым в процессе использования информационных технологий физическими и юридическими лицами.**

В процессе использования информационных технологий физическими и юридическими лицами возникает новая информация, правовой статус которой не определен. Между тем эта информация представляет интерес для различных субъектов, в том числе коммерческий, с одной стороны, и потенциальную опасность, с другой. Данных, генерируемых устройствами в автоматическом режиме без непосредственного участия человека в процессе использовании человеком информационных технологий становится все больше. При подключении к Интернету «умных» вещей информация, генерируемая устройствами в автоматическом режиме, отправляется без согласия владельца по адресам, заложенным в программе этого устройства. Это могут быть данные о местонахождении человека или определенного объекта, в том числе план помещения, данные о состоянии окружающей среды, данные о состоянии здоровья человека, состоянии оборудования, устройств, параметрах его функционирования и т.п.

В связи с этим актуальными становятся проблемы обеспечения информационной безопасности, установление применимого к ним правового режима, включая определение условий и границ такого использования, предоставления информации об адресате и объеме передаваемых сведений и др. Указанные вопросы должны быть решены законодательным путем. Обязательным условием должно быть согласие владельца такого оборудования, полученное производителями таких устройств.

Учитывая возможности «умных» устройств, подключенных к Интернету, требуется минимизировать риски несанкционированного доступа к персональным данным, иной охраняемой законом тайны, риски, связанные с блокировкой иных устройств, либо с возможностью причинения вреда жизни и здоровью граждан, их имуществу.

Другой аспект использования генерируемых «умными» устройствами данных, возможность их коммерциализации, условия которой и субъект также должны быть определены законодательно. Кроме того, должен быть обеспечен доступ государственных органов в целях контроля к этим данным.

**Риски, связанные с обработкой персональных данных.**

- модернизация правового режима персональных данных, обезличенных данных, пользовательских (поведенческих) и больших данных, а также сведений, составляющих тайну личной жизни, семейную тайну, тайну частной жизни;

- установление основ правового режима «общедоступных персональных данных», возможных действий и целей обработки общедоступных персональных данных;

- определение понятийного аппарата, в том числе «общедоступные персональные данные» (персональные данные, сделанные субъектом персональных данных общедоступными).

В настоящее время правовое регулирование отношений, связанных с оборотом персональных данных, основано на нормах Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных» и принятых во его исполнения постановлений Правительства Российской Федерации, приказов Роскомнадзора, ФСБ России и ФСТЭК России.

Вместе с тем, развитие информационных технологий оказывает серьезное влияние на содержание общественных отношений, связанных с обработкой персональных данных и требует модернизации их правового регулирования, включающей уточнение базовых понятий данного правового института, а также требований к обработке персональных данных, устранение правовой неопределенности в части возможностей гражданского оборота деперсонализированных данных, а также использования общедоступных персональных данных.

**Риски, связанные с режимом различных видов охраняемых законом интересов/тайн.**

Модернизация существующего правового регулирования законодательства об отдельных видах тайн, а также конфиденциальной информации должна учитывать современные тенденции качественного изменения способов обработки информации, в том числе составляющих отдельные виды тайн. К конфиденциальной информации относятся любые сведения, доступ к которым ограничен законодательством: персональные данные, информация, составляющая профессиональную (адвокатскую, банковскую, аудиторскую и пр.), коммерческую тайну. В значительной степени тайны, конфиденциальная информация могут пересекаться. В некоторых случаях для придания информации статуса тайны или конфиденциальной нужно совершить определенные действия (ввести режим) тайны.

Общемировая тенденция на расширение сферы и объема открытой информации не исключает существования информации ограниченного доступа. Ограничение доступа к информации направлено на охрану сведений, свободное распространение которых нарушает права и законные интересы общества, государства, личности. Требуется нахождение компромисса, который выражается в установлении «пределов осуществления прав», превышение которых следует рассматривать как «злоупотребление правами». Применительно к информации вытекает необходимость установления пределов ее открытости и доступности в целях недопустимости нарушения прав и свобод других лиц в процессе осуществления конституционных прав на свободу поиска, получения, передачи, производства и распространения информации любым законным способом.

Это достигается при помощи следующих средств:

– установления дополнительных запретов и обязываний, ограничение определенных действий;

– принятие специальных мер, направленных на установление и поддержание введенных правил;

– разрешительный способ и тип реализации прав и свобод;

– система контроля и надзора за выполнением требований;

– установление ответственности за нарушение установленных требований.

Существует общая тенденция формирования универсального характера доступа к информации и ее использования, расширения сферы открытой информации. Наличие различного вида тайн направлено на обеспечение прав и законных интересов различных субъектов: от гражданина и его личной тайны, неприкосновенности частной жизни до государства и его государственной тайны.

Упорядочивание видов тайн и формирование некой иерархии необходимо для того, чтобы выстроить оптимальную систему ответственности за их разглашение и оптимальную систему требований по защите каждого вида тайн. В отсутствие такой иерархии и системы нарушается принцип разумной достаточности.

Совершенствование правового регулирования должно происходить не столько «точечным» способом, сколько путем устранения явных неточностей, пробелов и противоречий, сколько путем упорядочения и согласования установленных правовых режимов, детальной их проработки, проведения систематизации и подготовки кодифицированного законодательного акта.

В этих целях необходимо разработать федеральный закон, устанавливающий иерархию режимов конфиденциальности с приоритетом государственной тайны; критерии отнесения информации к какому-либо виду тайн, общие подходы к условиям и порядку введения режима тайн, его действия и прекращения, императивность или диспозитивность требований для отдельных категорий субъектов.

**Риски в сфере соблюдения правового режима сведений, составляющих различного вида тайн в ходе судопроизводства с использованием цифровых технологий.**

В соответствии с действующим законодательством судопроизводство в Российской Федерации осуществляется во всех судах открыто, за исключением случаев, когда разбирательство дела в суде может привести к разглашению государственной или иной охраняемой действующим законодательством тайны.

Применительно к уголовному судопроизводству на законодательном уровне охраняется тайна предварительного расследования. В соответствии со ст. 161 УПК РФ данные предварительного расследования не подлежат разглашению без специального на то разрешения следователя или дознавателя, определяющих также допустимый объем тех сведений, которые дозволяется предавать огласке. За разглашение данных предварительного расследования законом предусмотрена уголовная ответственность (ст. 310 УК РФ). Также на законодательном уровне закреплено уголовное наказание за разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст. 311 УК РФ).

В целях надежной и эффективной правовой среды, соблюдения правового режима сведений, составляющих различного вида тайн в ходе судопроизводства с использованием цифровых технологий, необходимо:

- разработать системы надлежащей защиты электронного дела и электронных баз данных от вредоносных программ, несанкционированного доступа, возможных «хакерских» атак в целях недопущения различных утечек информации из электронной формы дела, составляющей государственную или иную охраняемую действующим законодательством тайну. В этих целях следует использовать шифровальное устройство, соответствующее минимум третьему уровню безопасности и сертифицированное на государственном уровне в порядке, установленном действующим законодательством Российской Федерации;

- на законодательном уровне определить круг лиц, имеющих допуск к процессуальной информации, составляющей государственную или иную охраняемую действующим законодательством тайну и содержащейся в электронном деле;

- обеспечить накопление, хранение и воспроизведение процессуальной информации, составляющей государственную или иную охраняемую действующим законодательством тайну и хранящейся в электронном деле, а также ее защиту от модификации;

- определить способы и каналы передачи электронных дел, в которых содержатся сведения, составляющие государственную или иную охраняемую действующим законодательством тайну заинтересованным лицам (судье, прокурору, следователю, эксперту и т.п.) и предусмотреть соответствующие гарантии их защиты.

**Риски, связанные с оборотом больших данных.**

Основные риски в данной сфере связаны с регламентацией процессов формирования, хранения, систематизации, обработки (в т.ч. без участия человека) и оборота больших данных, включая режимы доступа и права участников такого оборота и третьих лиц в части:

- идентифицирующих и персональных данных, в том числе геолокационных, а также «цифровых двойников»;

- пользовательского контента;

информации, формируемой пользователем опосредовано (т.н. «цифровой след»);

- информации о работе оборудования;

- передачи данных между устройствами (т.н. «интернет вещей»);

- механизмов правовой защиты указанной информации;

- правил и механизмов обмена данными между субъектами цифровой экономики;

- недискриминационного доступа к ним,

- ответственности за несанкционированный доступ,

- классификации данных с учетом требований по доступности и информационной безопасности,

- определения подходов к созданию системы управления данными, в том числе исходя из источников и средств генерации данных (человек, машина);

- регулирования прав на сбор данных в зависимости от волеизъявления субъектов, условий по обработке и коммерческому использованию таких данных, механизмов сбора и использования больших массивов данных.

В Российской Федерации предпринимаются попытки регулирования оборота больших данных, в частности, путем внесения изменений в Федеральный закон «Об информации, информационных технологиях и защите информации» путем определения правового режима «больших пользовательских данных», в том числе определения данного понятия, определение оператора больших пользовательских данных, его прав и обязанностей, формирования реестра операторов больших пользовательских данных и контроля за их деятельностью. Однако указанные попытки регулирования не охватывают всего круга общественных отношений, связанных с обработкой больших данных и содержат избыточные и обременительные для организаций требования (в том числе создание реестра операторов), не обеспечивающие реальной защиты прав граждан.

Основными рисками, связанные с применением технологии обработки больших объемов данных, являются:

- обработка неточных или неполных данных;

- утечка данных;

- дискриминация граждан на основе результатов обработки больших данных.

**Риски, связанные с цифровыми следами.**

С развитием информационных технологий в Российской Федерации все большее развитие получают общественные отношения, связанные с цифровым следом и его использованием. На это указывает рост российского сегмента рынка коммерческих центров хранения и обработки данных.

В условиях цифровой экономики данные, образующие цифровой след, становятся ценным активом, позволяющим получать информацию о пользователях информационно-коммуникационных сетей, их интересах, устремлениях, предпочтениях, потребностях, а также обрабатывать полученные данные в публичных и частных интересах.

В некоторых зарубежных государствах, в частности, в Великобритании и в США цифровой след активно используется не только в коммерческих целях, но также и в рамках избирательных компаний, например, в предвыборной кампании Д. Трампа в интернете, и в кампании в поддержку Brexit (например, исследования компании, Cambridge Analytica). Использование цифрового следа порождает новые общественные отношения, субъектами которых становятся пользователи информационно-коммуникационных сетей, владельцы интернет-сайтов, провайдеры и иные организации, органы власти.

Риски, возникающие по поводу использования цифрового следа, связаны:

- с юридически значимой идентификацией личности в виртуальном пространстве;

- с реализацией прав человека в виртуальном пространстве (право на доступ в Интернет, право на забвение, право на «цифровую смерть» и др.);

- с защитой хранением, обработкой и распространением информации, составляющей цифровой след, в том числе в целях обеспечения безопасности;

- с обеспечением рационального использования энергетических и иных ресурсов, размещением и утилизацией оборудования, необходимого для хранения и работы с данными, составляющими цифровой след.

Серьезной проблемой является обеспечение соблюдения иностранными компаниями требований российского законодательства о хранении персональных данных российских граждан на территории России. В настоящее время в реестре организаторов распространения информации не зарегистрированы такие компании, как Facebook, Twitter и Instagram.

Подводя итог вышесказанному, следует подчеркнуть, что комплексное исследование юридических рисков, связанных с цифровизацией, предствляет собой крайне актуальную научно-исследовательскую проблему.

**6. Дорожная карта программы стратегического развития**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Мероприятие | Срок | Ответственный | Финансирование, тыс.руб. | | | Результат |
| УдГУ | Софинанирование | Всего |
| 1. | Создание ЦК | до 2025 г. | Белокрылова Е.А.  Люминарская С.В. |  |  |  | Создание ЦК |
| 2. | Создание НОЦ | до 2025 г. | Белокрылова Е.А.  Люминарская С.В. |  |  |  | Создание НОЦ |
| 3. | IT- Юрист | до 2025 г. | Колчерина Ж.Н.  Белокрылова Е.А.  Люминарская С.В. |  |  |  | новая модель выпускника |
| 4. | Профориентационная работа | до 2025 г. | Колчерина Ж.Н. |  |  |  | увеличение контингента |
| 5. | Междисциплинарный научный проект «Анализ юридических рисков в сфере цифровизации юридического образования» | до 2025 г. | Белокрылова Е.А.  Люминарская С.В. |  |  |  | Разработка критериев оценки рисков в сфере цифровизации юридического образования |
| 6. | Автоматизированная платформа обучения навыкам кибербезопасности: Kaspersky Automated Security Awareness Platform (ASAP). | до 2025 г. | Колчерина Ж.Н. |  |  |  | новая модель выпускника, повышение востребованности выпускников на рынке труда |
| 7. | Портфель проектов «Формирование доверенной среды информационного общества в условиях существования угроз различного характера». | до 2025 г. | Колчерина Ж.Н. |  |  |  | создание информационного пространства, создания для граждан общедоступной системы взаимоувязанных знаний и представлений, обеспечения безопасной информационной среды для детей в Удмуртской Республике |

**7. Ресурсное обеспечение**

Для создания условий внедрения показателей цифровой экономики в образовательную среду в сфере юриспруденции, а также для реализации заявленных выше проектов Институту требуется:

**1. Создание виртуальной среды для поддержки учебных (образовательных) стендов.**

Требуется создание «фермы серверов» для реализации виртуальной среды. Необходима модернизация программных и аппаратных ресурсов, увеличение пропускной способности каналов связи, увеличение мощности серверов, приобретение программного обеспечения в управлении виртуальными ресурсами.

**2. Расширение деятельности лаборатории «Информационно правовой центр», в части подготовки цифровизации образовательных программ в сфере юриспруденции.**

Требуется увеличение штата, дополнительное финансирование, программное аппаратное обеспечение.Необходимо исследование рынка специализированных интеллектуальных экспертных систем, включающее тестирование продуктов в условиях образовательной среды ИПСУБ, а также внедрение протестированных интеллектуальных экспертных систем в образовательный процесс).

**3. Реализация процесса перехода на открытое отечественное программное обеспечение.**

Требуется: проведение внутреннего, программно-аппаратного аудита. Приобретение лицензий на отечественное программное обеспечение (в рамках Приказа Минкомсвязи России от 08.05.2019 N 184 «Об утверждении методических рекомендаций по переходу предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской Федерации, органам местного самоуправления и государственным внебюджетным фондам, на преимущественное использование отечественного программного обеспечения, в том числе офисного программного обеспечения»).

**4. Для организации учебного процесса необходимо:**

1) Модернизация учебных классов, специализированных помещений, лабораторий (замена оборудования, обновление ПО).

2) Модернизация мультимедийных ресурсов.

3) Модернизация системы видеоконференцсвязи.

4) Обновление парка программного обеспечения ИПСУБ.

5) Модернизация коммуникационной системы, создание сетевых сервисов, направленных на обеспечение перехода к цифровой экономике.

**5. Обеспечение деятельности ИПСУБ:**

1) Обновление парка вычислительной техники, парка офисной техники и программного обеспечения ИПСУБ.

2) Модернизация коммуникационной системы, замена сетевого оборудования (нацеленное на увеличение пропускной способности с учетом роста доли мультимедиа трафика в сети).

3) Обновление парка программного обеспечения ИПСУБ в соответствии с Приказом Минкомсвязи России от 08.05.2019 N 184 «Об утверждении методических рекомендаций по переходу предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской Федерации, органам местного самоуправления и государственным внебюджетным фондам, на преимущественное использование отечественного программного обеспечения, в том числе офисного программного обеспечения».

4). Расширение взаимодействия с производителями отечественных программных и программно-аппаратных комплексов.