Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
_____ 2019 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Модуль	Код модуля
Информационно-правовые основы национальной безопасности	1150480

Екатеринбург, 2019

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа Правовое обеспечение национальной безопасности	**Код ОП** 40.05.01/33.01
Направление подготовки Правовое обеспечение национальной безопасности	**Код направления и уровня подготовки** 40.05.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Сивоволов Дмитрий Леонидович	к. с. н., доцент	доцент	кафедра теории, методологии и правового обеспечения ГМУ
2	Вафин Рашит Рафхатович	к. ю. н., доцент	доцент	кафедра теории, методологии и правового обеспечения ГМУ

Руководитель модуля Д. Л. Сивоволов

Рекомендовано учебно-методическим советом института государственного управления и предпринимательства

Протокол № 10 от 26 июня 2019г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

1. **ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ** «ИНФОРМАЦИОННО-ПРАВОВЫЕ ОСНОВЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ».

1.1. Аннотация содержания модуля

Модуль «Информационно-правовые основы национальной безопасности национальной безопасности» занимает особое место в системе подготовки управленческих кадров для различных сфер государственной и хозяйственной деятельности, которые должны понимать необходимость защиты национальных интересов государства в информационной сфере определяющихся совокупностью сбалансированных интересов личности, общества и государства. Именно на основе обеспечения национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политике государства по обеспечению информационной безопасности, без этого невозможно дальнейшее развитие нашего государства в условиях «цифровой экономики». По словам нашего президента В. В. Путина, «мы будем развивать цифровые технологии, цифровую экономику, потому что только благодаря этому сможем остаться конкурентно способными через 5,10 и 25 лет». К 2020 году должен быть «создан каркас инфраструктуры безопасности цифровой экономики и обеспечен цифровой суверенитет Российской Федерации, а ещё через четыре года Россия станет «одним из мировых лидеров в области информационной безопасности».

В состав модуля включены три взаимосвязанные дисциплины: «Информационная безопасность», «Информационное право», «Методы борьбы с киберпреступностью».

Дисциплина «Информационная безопасность». Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Дисциплина «Информационное право» является базовым предметом, это обусловлено специфическим предметом данной отрасли права – общественными отношениями в информационной сфере, т.е. отношениями, связанными с информацией, использованием информационных технологий и защитой информации. Осознавая все преимущества информационного общества в условиях развивающейся «цифровой экономики», нельзя не учитывать, что оно несёт с собой не только новые возможности, но и новые проблемы и риски. Следовательно, основными направлениями государственной политики в информационной сфере должны быть: обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы; формирование и защита государственных информационных ресурсов; создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве, а также решение других задач.

Информационная деятельность во всех сферах жизни общества регулирует информационное право. От эффективности такого регулирования в современных условиях зависит информационное обеспечение национальной безопасности, гарантированность дальнейшего развития нашего общества и государства.

Дисциплина «Методы борьбы с киберпреступностью». Как отмечается в концептуальных документах стран лидеров цифрового мира, важнейшим критерием перехода страны в цифровой мир является всеобщая связанность, интеграция личных,

общественных сетей, корпоративных систем и правительственных инфраструктур в единое целое – цифровой взаимосвязанный мир. Данное обстоятельство требует изменения подхода к национальной цифровой безопасности и кибербезопасности как несущей конструкции цифровой безопасности. Учитывая специфический характер самого цифрового мира, киберпреступность может рассматриваться как специфическая разновидность преступной деятельности, а также как самостоятельная наука предполагающая самостоятельную учебную дисциплину. В доктрине информационной безопасности РФ, отмечается, что различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое, и общественное сознание в целях нагнетания межнациональной и социальной напряжённости, разжигания этнической и религиозной ненависти и вражды, пропаганду экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Создаются средства деструктивного воздействия на объекты критической информационной структуры.

Особо подчёркнуто, что возрастают масштабы компьютерной преступности, прежде всего в кредитно- финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод гражданина и человека,, в том числе в части, касающийся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений постоянно совершенствуются. Поэтому необходимо изучать и совершенствовать методы борьбы с киберпреступность

правоохранительными органами государства, как одну из составляющих обеспечения национальной безопасности.

Дисциплины модуля могут быть реализованы в смешанной и традиционной технологии. Реализация дисциплин модуля с использованием смешанной технологии обучения предполагает применение разработанных электронных ресурсов, имеющих статус ЭОР УрФУ и размещенных на образовательной платформе УрФУ, включая учебные пособия, презентации, задания и тесты.

1.2. Структура и объем модуля, распределение объема времени по видам учебной работы по дисциплинам модуля

Таблица 1.

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1	*Информационная безопасность*	3 з.е/108час.	зачет
2	*Методы борьбы с киберпреступностью*	3 з.е./ 108час.	зачет
3	*Информационное право*	3 з.е./ 108час.	экзамен
	ИТОГО по модулю:	*9 з.е./* 324час.	*не предусмотрено*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Уголовно-правовое регулирование национальной безопасности.
Постреквизиты и корреквизиты модуля	Правовое обеспечение внутренней безопасности государства.

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения по модулю

Изучение дисциплин модуля предусматривает формирование компетенций посредством последовательного освоения результатов обучения на определенном уровне сложности содержания.

Результаты обучения по дисциплине – это конкретные знания, умения, опыт и другие результаты (содержательные компоненты компетенций), которых планируется достичь на этапе изучения дисциплины модуля и которые должны будут продемонстрированы обучающимися и оценены преподавателем по индикаторам/измеряемым критериям, включенным в формулировку результатов обучения.

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации

Таблица 2

Перечень дисциплин модуля	**Код и наименование компетенции**	**Планируемые результаты обучения (индикаторы)**
Информационная безопасность	ПК-1 Способен разрабатывать нормативные правовые акты в сфере обеспечения национальной безопасности	Знать: - основные законодательные, доктринальные и стратегические нормативные акты в сфере обеспечения информационной безопасности; Уметь: - самостоятельно определять значение нормативных правовых актов; - анализировать, толковать и правильно применять нормы права; Практический опыт, владение: - способностью исследовать научные основы теории методологии обеспечения информационной безопасности и защиты информации
	ПК-2 Способен юридически правильно квалифицировать факты, события и обстоятельства	Знать: - аппаратно-программные и организационные средства информационных ресурсов различного вида. Уметь: - исследовать методы аппаратно-программных средств формирования информационных ресурсов различного вида.

		Практический опыт, владение: - способностью использовать аппаратно-программные и организационные средства информационных ресурсов для обеспечения национальной безопасности.
	ПК-3 Способен принимать решения и осуществлять действия в соответствии с законодательством в целях обеспечения национальной безопасности	Знать: - методы и средства выявления и классификации угроз нарушения информационной безопасности. Уметь: - выявлять, идентифицировать угрозы нарушения информационной безопасности. Практический опыт, владение: - способами и средствами выявления, идентификации и классификации угроз нарушения информационной безопасности в целях обеспечения национальной безопасности.
	ПК-7 Способен выявлять, пресекать и квалифицировать преступления и иные правонарушения	Знать: - способы анализа данных для средств обеспечения информационной безопасности. Уметь: - анализировать данные для проектирования средств обеспечения информационной безопасности. Практический опыт, владение: - способностью анализировать данные для обеспечения информационной безопасности в целях обеспечения национальной безопасности.
	ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных актов в области защиты государственной тайны и информационной безопасности	Знать: -техническую документацию, нормативно-методические документы в сфере обеспечения информационной безопасности. Уметь: - оформлять техническую документацию с учётом действующих нормативных документов в сфере обеспечения информационной безопасности. Практический опыт, владение: -способностью оформлять необходимую документацию с учётом нормативных и

		методических документов в сфере обеспечения информационной безопасности.
	ПК-10 Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	Знать: - стандарты в области информационной безопасности. Уметь: - анализировать объекты и системы на соответствие требованием стандартов в области информационной безопасности. Практический опыт, владение: - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованием стандартов в области информационной безопасности.
Методы борьбы с киберпреступностью	ПК-1 Способен разрабатывать нормативные правовые акты в сфере обеспечения национальной безопасности	Знать: - принципы разработки нормативных правовых актов в сфере правового обеспечения цифровой экономики; - правила нормотворческой техники, регламентирующие внешнее оформление нормативных правовых актов, требования к их структуре и содержанию, а также существующие правила и приемы изложения норм права - язык нормативных актов; Уметь: - самостоятельно разрабатывать проекты нормативных правовых актов; - анализировать, толковать и правильно применять нормы права; Практический опыт, владение: - навыками и способами разработки нормативно-правовых актов в соответствии с профилем своей профессиональной деятельности.
	ПК-2 Способен юридически правильно квалифицировать факты, события и обстоятельства	Знать: -современную нормативно-правовую базу с учетом изменений, происходящих в законодательстве; - содержание Федеральных законов, иных нормативно-правовых актов, необходимых для реализации норм права в профессиональной деятельности по борьбе с киберпреступностью; Уметь:

		- квалифицированно применять нормативные правовые акты в сфере правового обеспечения цифровой экономики, реализовывать нормы материального и процессуального права в профессиональной деятельност по борьбе с киберпреступностьюи; Практический опыт, владение: - навыками работы со справочными правовыми системами, с нормативными правовыми актами и специальной юридической литературой при осуществлении правоприменительной, научно-исследовательской или иной юридической деятельности в сфере борьбы с киберпреступностью.
	ПК-3 Способен принимать решения и осуществлять действия в соответствии с законодательством в целях обеспечения национальной безопасности	Знать: - содержание должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства; - содержание Федеральных законов, иных нормативно-правовых актов, необходимых для обеспечения законности и правопорядка, безопасности личности, общества, государства в области борьбы с киберпреступностью; Уметь: - квалифицированно исполнять свои должностные обязанности; применять нормативно-правовые акты, необходимые для обеспечения законности и правопорядка, безопасности личности, общества, государства; Практический опыт, владение: - навыками выполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства– в сфере борьбы с киберпреступностью.
	ПК-7 Способен выявлять, пресекать и квалифицировать преступления и иные правонарушения	Знать: - понятие и виды нормативно-правовых актов; способы и правила толкования нормативно-правовых актов; - правовую природу актов толкования; стадии, методы подготовки юридических документов в сфере цифровой экономики;

		Уметь: - грамотно и квалифицировано толковать нормативно-правовые акты; - самостоятельно разрабатывать и готовить юридические документы в сфере цифровой экономики; Практический опыт, владение: -навыками подготовки юридических документов в сфере цифровой экономики и Борьбы с киберпреступностью
	ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных актов в области защиты государственной тайны и информационной безопасности	Знать: - принципы проведения юридической экспертизы проектов нормативных правовых актов; Уметь: - проводить юридическую экспертизу проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупций, - давать квалифицированные юридические заключения и консультации в сфере правового обеспечения цифровой экономики и борьбы с киберпреступностью; Практический опыт, владение: - способностью принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, - давать квалифицированные юридические заключения и консультации в сфере правового обеспечения цифровой экономики и борьбы с киберпреступностью.
	ПК-10 Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	Знать: - виды управленческих инноваций в сфере правового обеспечения борьбы с киберпреступностью; Уметь: - воспринимать, анализировать и реализовывать управленческие инновации в сфере борьбы с киберпреступностью; Практический опыт, владение: - способностью воспринимать,

		анализировать и реализовывать управленческие инновации в сфере борьбы с киберпреступностью.
Информационное право	ПК-1 Способен разрабатывать нормативные правовые акты в сфере обеспечения национальной безопасности	Знать: - принципы разработки нормативных правовых актов в сфере правового обеспечения национальной безопасности; Уметь: - самостоятельно разрабатывать проекты нормативных правовых актов; - анализировать, толковать и правильно применять нормы информационного права; Практический опыт, владение: - навыками и способами разработки нормативно-правовых актов в соответствии с профилем своей профессиональной деятельности.
	ПК-2 Способен юридически правильно квалифицировать факты, события и обстоятельства	Знать*:* - современную нормативно-правовую базу с учетом изменений, происходящих в законодательстве; - содержание Федеральных законов, иных нормативно-правовых актов, необходимых для реализации норм права в профессиональной деятельности; Уметь: - квалифицированно применять нормативные правовые акты информационного права в сфере правового обеспечения национальной безопасности; Практический опыт, владение: - навыками работы со справочными правовыми системами, с нормативными правовыми актами и специальной юридической литературой при осуществлении правоприменительной, научно-исследовательской или иной юридической деятельности в сфере национальной безопасности.
	ПК-3 Способен принимать решения и осуществлять действия в соответствии с законодательством в целях обеспечения национальной безопасности	Знать*:* - содержание должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства; - содержание Федеральных законов,

		иных нормативно-правовых актов, необходимых для обеспечения национальной безопасности; Уметь: - квалифицированно исполнять свои должностные обязанности; применять нормативно-правовые акты, необходимые для обеспечения национальной безопасности; Практический опыт, владение: - навыками выполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства– в сфере национальной безопасности
	ПК-4 Способен квалифицированно применять нормативные акты в профессиональной деятельности	Знать: - состав уголовных и административных деликтов в сфере национальной безопасности; - методы и способы выявления, пресечения, раскрытия и расследования правонарушений и преступлений; Уметь: - выявлять, раскрывать и расследовать преступления и административные проступки; Практический опыт, владение: - навыками выявления, пресечения, раскрытия и расследования правонарушений и преступлений;
	ПК-5 Способен разрабатывать и правильно оформлять юридические документы	Знать: - содержание нормативно-правовых актов, необходимых для осуществления предупреждения правонарушений, выявления и устранения причин и условий, способствующих их совершению– в части, касающейся способности выявлять причины и условия, способствующие совершению преступлений Уметь: - осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению Практический опыт, владение:

		- навыками подготовки юридических документов в сфере национальной безопасности
	ПК-7 – Способен выявлять, пресекать и квалифицировать преступления и иные правонарушения	Знать: - понятие и виды нормативно-правовых актов; способы и правила толкования нормативно-правовых актов; - правовую природу актов толкования; - стадии, методы подготовки юридических документов в сфере национальной безопасности; Уметь: - грамотно и квалифицировано толковать нормативно-правовые акты; - самостоятельно разрабатывать и готовить юридические документы в сфере национальной безопасности; Практический опыт, владение: - навыками предупреждения правонарушений, выявления и устранения причин и условий, способствующих их совершению.
	ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных актов в области защиты государственной тайны и информационной безопасности	Знать: - принципы защиты государственной тайны и информационной безопасности, а также требование нормативных правовых актов в этой области; Уметь: - осуществлять мероприятия по защите государственной тайны и информационной безопасности, давать квалифицированные юридические заключения и консультации в этой сфере; Практический опыт, владение: - способностью принимать участие в мероприятиях по защите государственной тайны и информационной безопасности, давать квалифицированные юридические заключения и консультации в этой сфере.
	ПК-10 Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	Знать: - виды управленческих инноваций в сфере правового обеспечения национальной безопасности; Уметь: - воспринимать, анализировать и реализовывать управленческие инновации в сфере правового

		обеспечения национальной безопасности; Практический опыт, владение: - способностью воспринимать, анализировать и реализовывать управленческие решения в сфере правового обеспечения национальной безопасности.

1.5 Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме.

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАЗДЕЛ 2 ПРОГРАММЫ МОДУЛЯ
«ИНФОРМАЦИОННО-ПРАВОВЫЕ ОСНОВЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Сивоволов Дмитрий Леонидович	к.с.н., доцент	доцент	кафедра теории, методологии и правового обеспечения ГМУ

Рекомендовано учебно-методическим советом Института государственного управления и предпринимательства.

Протокол № 10 от 26 июня 2019 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучения.
о Базовый уровень

1.2. Планируемые результаты обучения по дисциплине

Таблица 1.2

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
ПК-1 Способен разрабатывать нормативные правовые акты в сфере обеспечения национальной безопасности	Знать: - основные законодательные, доктринальные и стратегические нормативные акты в сфере обеспечения информационной безопасности; Уметь: - самостоятельно определять значение нормативных правовых актов; - анализировать, толковать и правильно применять нормы права; Практический опыт, владение: - способностью исследовать научные основы теории методологии обеспечения информационной безопасности и защиты информации
ПК-2 Способен юридически правильно квалифицировать факты, события и обстоятельства	Знать: - аппаратно-программные и организационные средства информационных ресурсов различного вида. Уметь: - исследовать методы аппаратно-программных средств формирования информационных ресурсов различного вида. Практический опыт, владение: - способностью использовать аппаратно-программные и организационные средства информационных ресурсов для обеспечения национальной безопасности.
ПК-3 Способен принимать решения и осуществлять действия в соответствии с законодательством в целях обеспечения национальной безопасности	Знать: - методы и средства выявления и классификации угроз нарушения информационной безопасности. Уметь: - выявлять, идентифицировать угрозы нарушения информационной безопасности. Практический опыт, владение: - способами и средствами выявления, идентификации и классификации угроз нарушения информационной безопасности в

	целях обеспечения национальной безопасности.
ПК-7 Способен выявлять, пресекать и квалифицировать преступления и иные правонарушения	Знать: - способы анализа данных для средств обеспечения информационной безопасности. Уметь: - анализировать данные для проектирования средств обеспечения информационной безопасности. Практический опыт, владение: - способностью анализировать данные для обеспечения информационной безопасности в целях обеспечения национальной безопасности.
ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных актов в области защиты государственной тайны и информационной безопасности	Знать: -техническую документацию, нормативно-методические документы в сфере обеспечения информационной безопасности. Уметь: - оформлять техническую документацию с учётом действующих нормативных документов в сфере обеспечения информационной безопасности. Практический опыт, владение: -способностью оформлять необходимую документацию с учётом нормативных и методических документов в сфере обеспечения информационной безопасности.
ПК-10 Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	Знать: - стандарты в области информационной безопасности. Уметь: - анализировать объекты и системы на соответствие требованием стандартов в области информационной безопасности. Практический опыт, владение: - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованием стандартов в области информационной безопасности.

1.3. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1.	Информационная безопасность в системе Национальной безопасности РФ.	Правовые основы информационной безопасности РФ. Содержание понятий: информационная безопасность, информационно-психологическая война; сетевые войны. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Основные составляющие национальных интересов РФ в информационной сфере. Основные направления достижения национальных интересов в информационной

		сфере.
Р2.	Методы обеспечения информационной безопасности РФ	Общие методы обеспечения информационной безопасности РФ (правовые, организационно-технические, экономические). Основные меры обеспечения информационной безопасности в сфере внутренней и внешней политике государства. Обеспечение информационной безопасности в сфере духовной жизни, как фактор духовного единения народов многонациональной России.
Р3.	Организация обеспечения информационной безопасности РФ	Принципы обеспечения информационной безопасности РФ. Организационные основы системы обеспечения информационной безопасности РФ (функции, задачи, элементы. Международное сотрудничество РФ в обеспечении информационной безопасности.
Р4.	Правовые основы защиты компьютерной информации	Понятие и содержание защиты компьютерной информации. Способы защиты компьютерной информации. Особенности компьютерных преступлений. Сеть Интернет, как орудие совершения компьютерных преступлений. Основные правила зашиты компьютерной информации в компьютерах, их сетях и системах...
Р5.	Сущность правовой защиты компьютерной информации	Структура правовой защиты компьютерной информации Объекты и субъекты правовой зашиты компьютерной информации. Специальная правовая зашита компьютерной информации. Обязанности обладателя информации и оператора информационной системы. Дисциплинарная, административно-правовая, уголовно-правовая, гражданско-правовая защита компьютерной информации.
Р6.	Ответственность за правонарушения в информационной сфере	Понятие юридической ответственности за правонарушения в информационной сфере. Гражданско-правовая ответственность за правонарушения в информационной сфере (имущественный характер принудительных мер воздействия). Административная ответственность за правонарушения в информационной сфере. Дисциплинарная ответственность за правонарушения в информационной сфере. Уголовная ответственность, как наиболее строгий вид юридической ответственности.
Р7.	Особенности привлечения виновных лиц к уголовной ответственности за преступления в информационной сфере	Особенности деяний совершаемых в информационной сфере, которые признаются уголовно наказуемыми. Уголовная ответственность за преступления в сфере компьютерной информации.
Р8.	Международное сотрудничество в сфере информационно-коммуникационных технологий	Зарубежный опыт защиты национальной информационной сферы. Международное законодательство в сфере информационно-коммуникационных технологий. Основные направления использования информационных ресурсов и обеспечения информационной безопасности в информационном пространстве Содружества Независимых Государств и Евразийского экономического сообщества.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Электронные ресурсы (издания)

1. Федеральный закон РФ от 27 июля 2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция).- Текст: электронный // КонсультантПлюс: [сайт]. – URL.:http://www.consultant.ru/document/cons_doc_LAW_61798/
2. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации (последняя редакция).- Текст: электронный // КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_220885/
3. Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена". Текст: электронный //КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_75586/
4. Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации" (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет"). Текст: электронный // КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_179963/
5. Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 30.11.2019) "Об утверждении государственной программы Российской Федерации "Информационное общество". Текст: электронный // КонсультантПлюс: [сайт]. – URL.: http://www.consultant.ru/document/cons_doc_LAW_162184/
6. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729– Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.
7. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348– Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.
8. Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611084– Библиогр. в кн. – Текст : электронный.

Печатные издания

Не предусмотрено

Профессиональные базы данных, информационно-справочные системы

1. http://www.biblioclub.ru/
2. http://archive.neicon.ru/
3. http://www.cyberpolice.ru (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)
4. http://www.infosecurity. report.ru/ (портал по информационной безопасности)
5. http://www.void.ru/ (портал по информационной безопасности)
6. http://www.infosec.ru/ (Сервер компании НИП «Информзащита»)
7. http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)
8. ru.wikipedia.org – википедия.
9. www.computerra.ru –журнал о компьютерах «Компьютера».
10. www.rsl.ru – российская научная библиотека

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

1. Справочно-правовая система «Консультант Плюс» www.consultant.ru
2. Справочно-правовая система «Гарант» www.garant.ru
3. Сайт раскрытия корпоративной информации www.e-disclosure.ru

3.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	Лекции;	Учебная аудитория для проведения занятий лекционного типа с мультимедийным оборудованием	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г.

			СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
2	Практические занятия	Учебная аудитория для проведения лекционных занятий, практических занятий с мультимедийным оборудованием Компьютерный класс	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Пакет Statistica 13, договор № 43-12/963-2017/1 от 26.12.2017г., срок действия до 25.12.2020г. Project Expert 7.55 Tutorial (серверная версия - 20 одновременных подключений), договор № 43-12 199-2013 от 23.04.2013г., срок действия –

			бессрочный. IBM SPSS Statistics Standard Authorized User Licence svp_ed (лицензия: бессрочная академическая), договор 43-12 1726 2014 от 22.10.2014г. (8 лицензий), срок действия – бессрочный. VORTEX 8.0, договор № 264V от 24.03.2009г., срок действия – бессрочный. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
3	Консультации	Учебная аудитория для проведения групповых и индивидуальных консультаций	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
4	Самостоятельная работа студентов	Учебная аудитория для проведения самостоятельной работы студентов	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office,

			подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
5	Текущий и промежуточный контроль	Учебная аудитория для текущего контроля и промежуточной аттестации	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное

			ПО Браузер Mozilla Firefox – свободное ПО

РАЗДЕЛ 2 ПРОГРАММЫ МОДУЛЯ
«ИНФОРМАЦИОННО-ПРАВОВЫЕ ОСНОВЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 3

МЕТОДЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Вафин Рашит Рафхатович	к.ю.н., доцент	доцент	кафедра теории, методологии и правового обеспечения государственного и муниципального управления.

Рекомендовано учебно-методическим советом Института государственного управления и предпринимательства.

Протокол № 10 от 26 июня 2019 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ «МЕТОДЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ»

1.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучения.
  о Базовый уровень

1.2. Планируемые результаты обучения по дисциплине

Таблица 1.2

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
ПК-1 Способен разрабатывать нормативные правовые акты в сфере обеспечения национальной безопасности	Знать: - принципы разработки нормативных правовых актов в сфере правового обеспечения цифровой экономики; - правила нормотворческой техники, регламентирующие внешнее оформление нормативных правовых актов, требования к их структуре и содержанию, а также существующие правила и приемы изложения норм права - язык нормативных актов; Уметь: - самостоятельно разрабатывать проекты нормативных правовых актов; - анализировать, толковать и правильно применять нормы права; Практический опыт, владение: - навыками и способами разработки нормативно-правовых актов в соответствии с профилем своей профессиональной деятельности.
ПК-2 Способен юридически правильно квалифицировать факты, события и обстоятельства	Знать: -современную нормативно-правовую базу с учетом изменений, происходящих в законодательстве; - содержание Федеральных законов, иных нормативно-правовых актов, необходимых для реализации норм права в профессиональной деятельности по борьбе с киберпреступностью; Уметь: - квалифицированно применять нормативные правовые акты в сфере правового обеспечения цифровой экономики, реализовывать нормы материального и процессуального права в профессиональной деятельност по борьбе с киберпреступностьюи; Практический опыт, владение: - навыками работы со справочными правовыми системами, с нормативными правовыми актами и специальной юридической литературой при осуществлении правоприменительной, научно-исследовательской или иной юридической

	деятельности в сфере борьбы с киберпреступностью.
ПК-3 Способен принимать решения и осуществлять действия в соответствии с законодательством в целях обеспечения национальной безопасности	Знать: - содержание должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства; - содержание Федеральных законов, иных нормативно-правовых актов, необходимых для обеспечения законности и правопорядка, безопасности личности, общества, государства в области борьбы с киберпреступностью; Уметь: - квалифицированно исполнять свои должностные обязанности; применять нормативно-правовые акты, необходимые для обеспечения законности и правопорядка, безопасности личности, общества, государства; Практический опыт, владение: - навыками выполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства– в сфере борьбы с киберпреступностью.
ПК-7 Способен выявлять, пресекать и квалифицировать преступления и иные правонарушения	Знать: - понятие и виды нормативно-правовых актов; способы и правила толкования нормативно-правовых актов; - правовую природу актов толкования; стадии, методы подготовки юридических документов в сфере цифровой экономики; Уметь: - грамотно и квалифицировано толковать нормативно-правовые акты; - самостоятельно разрабатывать и готовить юридические документы в сфере цифровой экономики; Практический опыт, владение: -навыками подготовки юридических документов в сфере цифровой экономики и Борьбы с киберпреступностью
ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных актов в области защиты государственной тайны и информационной безопасности	Знать: - принципы проведения юридической экспертизы проектов нормативных правовых актов; Уметь: - проводить юридическую экспертизу проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупций, - давать квалифицированные юридические заключения и консультации в сфере правового обеспечения цифровой экономики и борьбы с киберпреступностью; Практический опыт, владение: - способностью принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе

	в целях выявления в них положений, способствующих созданию условий для проявления коррупции, - давать квалифицированные юридические заключения и консультации в сфере правового обеспечения цифровой экономики и борьбы с киберпреступностью.
ПК-10 Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	Знать: - виды управленческих инноваций в сфере правового обеспечения борьбы с киберпреступностью; Уметь: - воспринимать, анализировать и реализовывать управленческие инновации в сфере борьбы с киберпреступностью; Практический опыт, владение: - способностью воспринимать, анализировать и реализовывать управленческие инновации в сфере борьбы с киберпреступностью.

1.3. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Современная киберпреступность	Международно-правовое определение киберпреступности. Классификация киберпреступлений. Современные тенденции развития киберпреступности.
Р2	Особенности современной киберпреступности в России	Киберпреступность как угроза национальной безопасности России. Внешние угрозы (кибервойна, кибервойска потенциального противника) и т.п. Возрастание опасности от небольших негосударственных групп и повышение потенциала террористов. Основные направления внутренних угроз от киберпреступности
Р3	Современный кибертерроризм и киберэкстремизм	Пропаганда как главный метод, используемый террористами и экстремистами в Интернете. Инструментарий, используемый террористами и экстремистами при совершении преступлений, связанных с Интернетом. Террористические угрозы в киберпространстве, направленные на важнейшие объекты инфраструктуры
Р4	Новые тенденции в совершении киберпреступлений	Киберпрестепления в финансовой сфере (кибермошенничество). Организованная преступность цифрового мира. Хакеры. Хактивисты. Преступники в сфере детской порнографии. «Группы смерти» В Интернете. Сетевые «тролли» и иные группы травли в Интернете. Деструктивные сети в Интернете
Р5	Предупреждение и основные методы борьбы с кибертерроризмом и киберэкстремизмом	Основные направления предупреждения кибертерроризма и киберэкстремизма. Превентивное устранение угроз кибертерроризма. Защита от терроризма критической информационной инфраструктуры.
Р6	Предупреждение и основные методы борьбы с киберпреступностью.	Основные требования по защите граждан, общества и государства от киберпреступлений в РФ. Предупреждение виктимизации, связанной с киберпреступностью.

		Деятельность провоохранительных органов по предупреждению, выявлению, раскрытию и расследованию киберпреступлений
Р7	Использование новейших технологий цифрового мира в предупреждение и борьбе с киберпреступностью.	Стратегический подход в использовании новейших технологи Использование искусственного интеллекта, больших данных и квантовой криптографии для предупреждения финансового мошенничества. Борьба с биткойн-преступностью и использование технологий блокчейн. Распознание лиц преступников на базе нейронных сетей. Новые технологии прогнозирования преступного поведения.
Р8	Основные направления разработки технологий цифрового мира в борьбе с киберпреступность в США, КНР	Разработка новых технологий и новых моделей правового регулирования. Значение крупнейших международных цифровых корпораций в разработке новейших технологий и роль государственных структур в обеспечении безопасности в условиях цифрового мира. Значение обеспечения национального суверенитета и национальной безопасности в условиях цифрового общества 21века.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации.

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «МЕТОДЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ»

Электронные ресурсы (издания)

1. Федеральный закон РФ от 27 июля 2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция).- Текст: электронный // КонсультантПлюс: [сайт]. – URL.:http://www.consultant.ru/document/cons_doc_LAW_61798/
2. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации (последняя редакция).- Текст: электронный // КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_220885/
3. Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена". Текст: электронный //КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_75586/
4. Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации" (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет"). Текст: электронный // КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_179963/
5. Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 30.11.2019) "Об утверждении государственной программы Российской Федерации "Информационное общество". Текст: электронный // КонсультантПлюс: [сайт]. – URL.: http://www.consultant.ru/document/cons_doc_LAW_162184/
6. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по

подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.
7. Степанов-Егиянц, В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации / В. Г. Степанов-Егиянц. – Москва : Статут, 2016. – 190 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=452481 Библиогр. в кн. – ISBN 978-5-8354-1279-2. – Текст : электронный.
8. Компьютерная криминалистика: лабораторный практикум : [16+] / авт.-сост. И. А. Калмыков, В. С. Пелешенко. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. – 84 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=466995 – Библиогр. в кн. – Текст : электронный.

Печатные издания
Не предусмотрено

Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечная система IPR BOOKS
2. http://www.biblioclub.ru/
3. http://archive.neicon.ru/
4. http://www.cyberpolice.ru (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)
5. http://www.infosecurity. report.ru/ (портал по информационной безопасности)
6. http://www.void.ru/ (портал по информационной безопасности)
7. http://www.infosec.ru/ (Сервер компании НИП «Информзащита»)
8. http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)
9. ru.wikipedia.org – википедия.
10. www.computerra.ru –журнал о компьютерах «Компьютера».
11. www.rsl.ru – российская научная

Базы данных, информационно-справочные и поисковые системы
1. Справочно-правовая система «Консультант Плюс» www.consultant.ru
2. Справочно-правовая система «Гарант» www.garant.ru
3. Сайт раскрытия корпоративной информации www.e-disclosure.ru

Материалы для лиц с ОВЗ
Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «МЕТОДЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ».

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего

		самостоятельной работы	документа
1	Лекции;	Учебная аудитория для проведения занятий лекционного типа с мультимедийным оборудованием	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
2	Практические занятия	Учебная аудитория для проведения лекционных занятий, практических занятий с мультимедийным оборудованием Компьютерный класс	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL

			w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Пакет Statistica 13, договор № 43-12/963-2017/1 от 26.12.2017г., срок действия до 25.12.2020г. Project Expert 7.55 Tutorial (серверная версия - 20 одновременных подключений), договор № 43-12 199-2013 от 23.04.2013г., срок действия – бессрочный. IBM SPSS Statistics Standard Authorized User Licence svp_ed (лицензия: бессрочная академическая), договор 43-12 1726 2014 от 22.10.2014г. (8 лицензий), срок действия – бессрочный. VORTEX 8.0, договор № 264V от 24.03.2009г., срок действия – бессрочный. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
3	Консультации	Учебная аудитория для проведения групповых и индивидуальных консультаций	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY

			FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
4	Самостоятельная работа студентов	Учебная аудитория для проведения самостоятельной работы студентов	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
5	Текущий и промежуточный контроль	Учебная аудитория для текущего контроля и промежуточной аттестации	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL

			Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО

РАЗДЕЛ 2 ПРОГРАММЫ МОДУЛЯ
«ИНФОРМАЦИОННО-ПРАВОВЫЕ ОСНОВЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

ИНФОРМАЦИОННОЕ ПРАВО

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Вафин Рашит Рафхатович	к.ю.н.,доцент	доцент	кафедра теории, методологии и правового обеспечения государственного и муниципального управления.

Рекомендовано учебно-методическим советом Института государственного управления и предпринимательства.

Протокол № 10 от 26 июня 2019 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННОЕ ПРАВО»

1.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучения.
о Базовый уровень

1.2. Планируемые результаты обучения по дисциплине

Таблица 1.2

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
ПК-1 Способен разрабатывать нормативные правовые акты в сфере обеспечения национальной безопасности	Знать: - принципы разработки нормативных правовых актов в сфере правового обеспечения национальной безопасности; Уметь: - самостоятельно разрабатывать проекты нормативных правовых актов; - анализировать, толковать и правильно применять нормы информационного права; Практический опыт, владение: - навыками и способами разработки нормативно-правовых актов в соответствии с профилем своей профессиональной деятельности.
ПК-2 Способен юридически правильно квалифицировать факты, события и обстоятельства	Знать*:* - современную нормативно-правовую базу с учетом изменений, происходящих в законодательстве; - содержание Федеральных законов, иных нормативно-правовых актов, необходимых для реализации норм права в профессиональной деятельности; Уметь: - квалифицированно применять нормативные правовые акты информационного права в сфере правового обеспечения национальной безопасности; Практический опыт, владение: - навыками работы со справочными правовыми системами, с нормативными правовыми актами и специальной юридической литературой при осуществлении правоприменительной, научно-исследовательской или иной юридической деятельности в сфере национальной безопасности.
ПК-3 Способен принимать решения и осуществлять действия в соответствии с законодательством в целях обеспечения национальной безопасности	Знать*:* - содержание должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства; - содержание Федеральных законов, иных нормативно-правовых актов, необходимых для обеспечения национальной

	безопасности; Уметь: - квалифицированно исполнять свои должностные обязанности; применять нормативно-правовые акты, необходимые для обеспечения национальной безопасности; Практический опыт, владение: - навыками выполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства– в сфере национальной безопасности
ПК-4 Способен квалифицированно применять нормативные акты в профессиональной деятельности	Знать: - состав уголовных и административных деликтов в сфере национальной безопасности; - методы и способы выявления, пресечения, раскрытия и расследования правонарушений и преступлений; Уметь: - выявлять, раскрывать и расследовать преступления и административные проступки; Практический опыт, владение: - навыками выявления, пресечения, раскрытия и расследования правонарушений и преступлений;
ПК-5 Способен разрабатывать и правильно оформлять юридические документы	Знать: - содержание нормативно-правовых актов, необходимых для осуществления предупреждения правонарушений, выявления и устранения причин и условий, способствующих их совершению– в части, касающейся способности выявлять причины и условия, способствующие совершению преступлений Уметь: - осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению Практический опыт, владение: - навыками подготовки юридических документов в сфере национальной безопасности
ПК-7 – Способен выявлять, пресекать и квалифицировать преступления и иные правонарушения	Знать: - понятие и виды нормативно-правовых актов; способы и правила толкования нормативно-правовых актов; - правовую природу актов толкования; - стадии, методы подготовки юридических документов в сфере национальной безопасности; Уметь: - грамотно и квалифицировано толковать нормативно-правовые акты; - самостоятельно разрабатывать и готовить юридические документы в сфере национальной безопасности;

	Практический опыт, владение: - навыками предупреждения правонарушений, выявления и устранения причин и условий, способствующих их совершению.
ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных актов в области защиты государственной тайны и информационной безопасности	Знать: - принципы защиты государственной тайны и информационной безопасности, а также требование нормативных правовых актов в этой области; Уметь: - осуществлять мероприятия по защите государственной тайны и информационной безопасности, давать квалифицированные юридические заключения и консультации в этой сфере; Практический опыт, владение: - способностью принимать участие в мероприятиях по защите государственной тайны и информационной безопасности, давать квалифицированные юридические заключения и консультации в этой сфере.
ПК-10 Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	Знать: - виды управленческих инноваций в сфере правового обеспечения национальной безопасности; Уметь: - воспринимать, анализировать и реализовывать управленческие инновации в сфере правового обеспечения национальной безопасности; Практический опыт, владение: - способностью воспринимать, анализировать и реализовывать управленческие решения в сфере правового обеспечения национальной безопасности.

1.3. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1.	Информационное право как отрасль российского права.	Понятие, предмет, метод, система и функции информационного права. Информационно-правовые нормы и информационно-правовые отношения. Источники и субъекты информационного права.
Р2.	Государственное управление в информационной сфере и правовое регулирование распространения информации.	Сущность и содержание государственного управления в информационной сфере. Правовое положение органов исполнительной власти, осуществляющих управление в информационной сфере. Правовое регулирование распространения информации и доступа к ней.
Р3.	Правовой режим государственной, коммерческой, служебной и иной охраняемой законом тайны.	Понятие и защита государственной тайны. Полномочия органов государственной власти в области защиты государственной тайны. Правовой режим коммерческой тайны. Правой режим служебной и иной охраняемой законом тайны. Правовое регулирование использования

		электронной цифровой подписи в электронных документах.
Р4.	Особенности правового регулирования отношений, связанных с доступом к персональным данным и их обработкой.	Понятие персональных данных. Правовое регулирование отношений, связанных с персональными данными и их обработкой. Особенности защиты персональных данных при их предоставлении и обработке в условиях цифровой экономики.
Р5.	Правовое регулирование деятельности средств массовой информации.	Сущность, содержание и распространение массовой информации. Взаимодействие средств массовой с обществом. Права и обязанности журналиста. Ответственность за нарушение законодательства о средствах массовой информации.
Р6.	Правовые основы применения информационных технологий в условиях современного цифрового мира.	Понятие информации и е правовые основы. Правовое регулирование создания и эксплуатации информационных систем. Правовые основы использования информационно-телекоммуникационных сетей и связи.
Р7.	Правовые основы информационной безопасности в РФ.	Понятие информационной безопасности РФ. Организационно-правовые методы обеспечения информационной безопасности РФ. Правовые основы и методы защиты информационного пространства РФ.
Р8.	Ответственность за правонарушения в информационной сфере.	Понятие юридической ответственности за правонарушения в информационной сфере. Виды ответственности: уголовная, административная, дисциплинарная и гражданвско-правовая за правонарушения в информационной сфере.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации.

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННОЕ ПРАВО»

Электронные ресурсы (издания)

1. Федеральный закон РФ от 27 июля 2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция).- Текст: электронный // КонсультантПлюс: [сайт]. – URL.:http://www.consultant.ru/document/cons_doc_LAW_61798/
2. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации (последняя редакция).- Текст:
3. Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена". Текст: электронный //КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_75586/
4. Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации" (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет"). Текст: электронный // КонсультантПлюс: [сайт] – URL.: http://www.consultant.ru/document/cons_doc_LAW_179963/
5. Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 30.11.2019) "Об утверждении государственной программы Российской Федерации "Информационное

общество". Текст: электронный // КонсультантПлюс: [сайт]. – URL.: http://www.consultant.ru/document/cons_doc_LAW_162184/

6. Килясханов, И. Ш. Информационное право в терминах и понятиях : учебное пособие / И. Ш. Килясханов, Ю. М. Саранчук. – Москва : Юнити, 2015. – 135 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=115167– Библиогр. в кн. – ISBN 978-5-238-01369-5. – Текст : электронный.
7. Актуальные проблемы информационного права: практикум : [16+] / сост. Л. Э. Боташева, М. С. Трофимов, О. А. Проводина, А. С. Кирпа и др. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 92 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562817– Библиогр. в кн. – Текст : электронный.
8. Лапина, М. А. Информационное право : учебное пособие / М. А. Лапина, А. Г. Ревин, В. И. Лапин ; ред. И. Ш. Килясханов. – Москва : Юнити, 2015. – 336 с. – (Высшее профессиональное образование: Юриспруденция). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=118624 Библиогр. в кн. – ISBN 5-238-00798-1. – Текст : электронный.
9. Васюк, А. В. Информационное право: практикум-тренинг для студентов направления подготовки 40.03.01 Юриспруденция : [16+] / А. В. Васюк ; Российская таможенная академия, Владивостокский филиал, Кафедра административного и таможенного права. – Владивосток : Российская таможенная академия, Владивостокский филиал, 2015. – 48 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438349– Библиогр. в кн. – Текст : электронный.

Печатные издания
Не предусмотрено

Профессиональные базы данных, информационно-справочные системы
1. http://www.biblioclub.ru/
2. http://archive.neicon.ru/
3. http://www.cyberpolice.ru (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)
4. http://www.infosecurity. report.ru/ (портал по информационной безопасности)
5. http://www.void.ru/ (портал по информационной безопасности)
6. http://www.infosec.ru/ (Сервер компании НИП «Информзащита»)
7. http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)
8. ru.wikipedia.org – википедия.
9. www.computerra.ru –журнал о компьютерах «Компьютера».
10. www.rsl.ru – российская научная библиотека
11. Электронно-библиотечная система IPR BOOKS

Базы данных, информационно-справочные и поисковые системы
1. Справочно-правовая система «Консультант Плюс» www.consultant.ru
2. Справочно-правовая система «Гарант» www.garant.ru
3. Сайт раскрытия корпоративной информации www.e-disclosure.ru

Материалы для лиц с ОВЗ
Весь контент ЭБС представлен в виде файлов специального формата для

воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

3.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННОЕ ПРАВО»

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	Лекции	Учебная аудитория для проведения занятий лекционного типа с мультимедийным оборудованием	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
2	Практические занятия	Учебная аудитория для проведения лекционных занятий, практических занятий с мультимедийным оборудованием	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г.

			Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
3	Консультации	Учебная аудитория для проведения групповых и индивидуальных консультаций	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно.

			Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
4	Самостоятельная работа студентов	Учебная аудитория для проведения самостоятельной работы студентов	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
5	Текущий и промежуточный контроль	Учебная аудитория для текущего контроля и промежуточной аттестации	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок

			действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО