

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет
Кафедра

Юридический
Теории и истории государства и права

Аннотация рабочей программы дисциплины (модуля)

дисциплина *Информационная безопасность в предпринимательской деятельности*

Блок Б1, вариативная часть, Б1.В.14

цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

40.03.01

код

Юриспруденция

наименование направления

Программа

Гражданско-правовой

Форма обучения

Очно-заочная

Для поступивших на обучение в
2020 г.

Стерлитамак 2022

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

| |
|---|
| Владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) |
| Способностью работать с информацией в глобальных компьютерных сетях (ОК-4) |
| Способностью обеспечивать соблюдение законодательства Российской Федерации субъектами права (ПК-3) |

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| Формируемая компетенция (с указанием кода) | Этапы формирования компетенции | Планируемые результаты обучения по дисциплине (модулю) |
|---|---|---|
| Владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) | 1 этап: Знания | Обучающийся должен знать: основные источники и правила доступа, а также использования информации, в том числе в профессиональных целях; основные методы хранения, обработки и защиты информации |
| | 2 этап: Умения | Обучающийся должен уметь: классифицировать информацию по режиму доступа, видам и типам; определять уровень достоверности источников информации и давать ей критическую оценку |
| | 3 этап: Владения (навыки / опыт деятельности) | Обучающийся должен владеть навыками использования электронных средств обработки, использования и переработки информации в целях обеспечения информационной безопасности в предпринимательской сфере |
| Способностью обеспечивать соблюдение законодательства Российской Федерации субъектами права (ПК-3) | 1 этап: Знания | Обучающийся должен знать: основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации, а также нормативные методические документы ФСБ, ФСТЭК в данной области |
| | 2 этап: Умения | Обучающийся должен уметь составлять и правильно оформлять деловую и служебную документацию; разрабатывать нормативно-методические материалы по регламентации системы |

| | | |
|--|---|---|
| | | организационной защиты информации; организовывать профилактическую работу с сотрудниками, имеющими доступ к информации ограниченного доступа |
| | 3 этап: Владения (навыки / опыт деятельности) | Обучающийся должен владеть навыками определения направлений и видов защиты информации с учетом характера информации и задач по ее защите. |
| Способностью работать с информацией в глобальных компьютерных сетях (ОК-4) | 1 этап: Знания | Обучающийся должен знать: виды информации, распространение которой запрещается или ограничивается в силу вреда, которое распространение этой информации наносит законным интересам и нравам субъектов информационных отношений; опасности и угрозы основным правам и свободам субъектов отношений в сети Интернет |
| | 2 этап: Умения | Обучающийся должен уметь: применять отечественные и зарубежные стандарты в области информационной безопасности с целью обоснования проектирования, разработки и оценки защищенности информации в предпринимательской деятельности |
| | 3 этап: Владения (навыки / опыт деятельности) | Обучающийся должен владеть профессиональной терминологией, навыками анализа информационных угроз в предпринимательской деятельности |

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках вариативной части.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: Информационные технологии в юридической деятельности, Правовое обеспечение информационных процессов, Административное право, Земельное право, Экологическое право, Жилищное право, Коммерческое право, Ювенальная юстиция, Трудовые споры.

Параллельно изучаемые дисциплины – Предпринимательское право, Исполнительное производство,

К изучению дисциплины «Информационная безопасность в предпринимательской деятельности», обучающийся должен:

знать: сущность и содержание основных правовых понятий, категорий, институтов; сущность, содержание основных понятий действующего законодательства ;

уметь: анализировать нормативные правовые акты на основе их всестороннего изучения; анализировать юридические факты и возникающие в связи с ними информационные

правоотношения;

владеть: навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности.

Дисциплина изучается на 5 курсе в 9 семестре

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 2 зач. ед., 72 акад. ч.

| Объем дисциплины | Всего часов |
|--|-----------------------|
| | Очно-заочная обучения |
| Общая трудоемкость дисциплины | 72 |
| Учебных часов на контактную работу с преподавателем: | |
| лекций | 6 |
| практических (семинарских) | 8 |
| другие формы контактной работы (ФКР) | 0,2 |
| Учебных часов на контроль (включая часы подготовки): | |
| зачет | |
| Учебных часов на самостоятельную работу обучающихся (СР) | 57,8 |

| Формы контроля | Семестры |
|----------------|----------|
| зачет | 9 |

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

| № п/п | Наименование раздела / темы дисциплины | Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах) | | | |
|-------|---|---|--------|-----|----|
| | | Контактная работа с преподавателем | | | СР |
| | | Лек | Пр/Сем | Лаб | |
| 2.1 | Тема 8. Ответственность за правонарушения в информационной сфере | 2 | 0 | 0 | 4 |
| 2.7 | Тема 14. Реклама и предпринимательская деятельность: правовое регулирование, информационная безопасность. | 0 | 0 | 0 | 4 |
| 2.6 | Тема 13. СМИ как важный объект информационной безопасности в предпринимательской деятельности | 0 | 0 | 0 | 4 |
| 2.5 | Тема 12. Проблемы защиты личных имущественных и неимущественных прав в информационной сфере | 0 | 0 | 0 | 4 |

| | | | | | |
|----------|--|----------|----------|----------|-------------|
| 1.1 | Тема 1. Назначение и структура правового обеспечения информационной безопасности | 0 | 0 | 0 | 4 |
| 1.2 | Тема 2. Основы правового регулирования отношений в информационной сфере | 2 | 0 | 0 | 4 |
| 1.3 | Тема 3. Правовые основы защиты государственной и коммерческой тайны; персональных данных | 0 | 2 | 0 | 4 |
| 1.4 | Тема 4. История и современные направления развития информационной безопасности. | 0 | 0 | 0 | 5 |
| 1.5 | Тема 5. Система организационно-правового обеспечения информационной безопасности. | 2 | 0 | 0 | 3,4 |
| 1.6 | Тема 6. Правовая основа информационной безопасности | 0 | 0 | 0 | 5 |
| 1 | Раздел 1. Понятие, организация и правовые основы обеспечения информационной безопасности в предпринимательской деятельности | 4 | 4 | 0 | 28,8 |
| 2.4 | Тема 11. Понятие режима и защиты информации в деятельности коммерческой организации. | 0 | 2 | 0 | 4 |
| 2.3 | Тема 10. Содержание организационного обеспечения информационной безопасности. | 0 | 2 | 0 | 5 |
| 2.2 | Тема 9. Правовая защита обладателей информации. | 0 | 0 | 0 | 4 |
| 1.7 | Тема 7. Источники угроз защищаемой информации. | 0 | 2 | 0 | 3,4 |
| 2 | Раздел 2. Система защиты информации: структурная и функциональная часть | 2 | 4 | 0 | 29 |
| | Итого | 6 | 8 | 0 | 57,8 |

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

| № | Наименование раздела / темы дисциплины | Содержание |
|-----|--|--|
| 2.1 | Тема 8. Ответственность за правонарушения в информационной сфере | 1. Правовой статус печатных, электронных и телекоммуникационных СМИ. 2. Правовые основы организации деятельности средств массовой информации. 3. Правоотношения, возникающие по поводу документированной информации о гражданах, официальной документированной информации, информации, создаваемой СМИ. 4. Факторы угроз информационной безопасности через СМИ 5. Правовые основания мониторинга и блокирования доступа к рекламной информации в сети Интернет 6. Ответственность за нарушение законодательства о |

| | | |
|----------|--|---|
| | | средствах массовой информации. |
| 1.2 | Тема 2. Основы правового регулирования отношений в информационной сфере | Конституционные основы использования информационных технологий в Российской Федерации. Система законодательства, регулирующего общественные отношения, возникающие в процессах применения информационных технологий. Законодательное регулирование реализации права граждан, органов государственной власти, органов местного самоуправления и организаций на доступ к информации. Электронные источники опубликования актов. Концепция формирования в Российской Федерации электронного правительства. |
| 1.5 | Тема 5. Система организационно-правового обеспечения информационной безопасности. | 1. Система защиты информации. Структурная и функциональная часть защиты информации. 2. Государственная система организационно-правового обеспечения информационной безопасности. 3. Основные категории и функции органов защиты информации. 4. Правовые основы деятельности подразделений защиты информации на предприятии 5. Основные формы организации работ по защите информации в предпринимательской деятельности. |
| 1 | Раздел 1. Понятие, организация и правовые основы обеспечения информационной безопасности в предпринимательской деятельности | |
| 2 | Раздел 2. Система защиты информации: структурная и функциональная часть | |

Курс практических/семинарских занятий

| № | Наименование раздела / темы дисциплины | Содержание |
|----------|--|---|
| 1.3 | Тема 3. Правовые основы защиты государственной и коммерческой тайны; персональных данных | 1. Правовые основы обеспечения информационной безопасности в России. 2. Регламентирование вопросов защиты информации в ведомственных нормативных актах. 3. Правовое регулирование информационной безопасности в предпринимательской деятельности. 4. Ответственность и ее виды за нарушение требований к защите информации. 5. Уголовно-правовая защита коммерческой, налоговой и банковской тайн |
| 1 | Раздел 1. Понятие, организация и правовые основы обеспечения информационной безопасности в предпринимательской деятельности | |
| 2.4 | Тема 11. Понятие режима и | 1. Понятие и защита государственной и |

| | | |
|----------|--|--|
| | защиты информации в деятельности коммерческой организации. | <p>коммерческой тайны в системе защиты информации.</p> <p>2. Действующие нормативные правовые акты, нормативно-методические и методические документы в системе защиты государственной и коммерческой тайны.</p> <p>3. Принципы защиты. Отнесение сведений к коммерческой, служебной и профессиональной тайнам.</p> <p>4. Перечень сведений, составляющих государственную тайну. Сведения, которые не могут составлять государственную и коммерческую тайну.</p> <p>5. Степени и грифы секретности. Засекречивание и рассекречивание. Основания и порядок доступа к конфиденциальной информации. Государственное лицензирование деятельности, связанное с защитой информации.</p> |
| 2.3 | Тема 10. Содержание организационного обеспечения информационной безопасности. | <p>1. Система защиты информации. Структурная и функциональная часть защиты информации.</p> <p>2. Государственная система организационно-правового обеспечения информационной безопасности.</p> <p>3. Основные категории и функции органов защиты информации.</p> <p>4. Основные формы организации работ по защите информации в правоохранительной сфере.</p> |
| 1.7 | Тема 7. Источники угроз защищаемой информации. | <p>1. Классификация и содержание возможных угроз информации в предпринимательской деятельности.</p> <p>2. Причины и условия утечки защищаемой информации.</p> <p>3. Разглашение, раскрытие и распространение защищаемой информации.</p> <p>4. Способы незаконного получения защищаемой информации.</p> |
| 2 | Раздел 2. Система защиты информации: структурная и функциональная часть | |