**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»**
**Казанский филиал**

Рабочая программа дисциплины (модуля)

# «Информационная безопасность в экономической деятельности»

**Набор 2023г.**

**Специальность: 38.05.01 Экономическая безопасность**

**Специализация: Экономико-правовое обеспечение экономической безопасности**

Рабочая программа разработана в соответствии с требованиями ФГОС

Разработчик: Шевко Н.Р., к.э.н., доцент

Рабочая программа рассмотрена и одобрена на заседании кафедры (протокол № 12 от 22.06.2023).

Зав.кафедрой Галяутдинова Л.Р., к.ф-м.н

Казань, 2023

# ПРОТОКОЛ ИЗМЕНЕНИЙ
## рабочей программы дисциплины (модуля)

_____

наименование дисциплины в соответствии с учебным планом

для набора ____ года на _____-_____уч.г.[1]

| Краткое содержание изменения | Дата и номер протокола заседания кафедры |
|---|---|
| | |
| | |

Актуализация выполнена[2]: _____

(ФИО, ученая степень, ученое звание)

_____ «__» _____ 202__г.

подпись

Зав. кафедрой _____

(ФИО, ученая степень, ученое звание)

_____ «__» _____ 20__г.

подпись

[1] Указанный протокол заполняется при актуализации РП по дисциплине (модулю) на учебный год, в течение которого соответствующая дисциплина (модуль) будет преподаваться (если год набора отличается от года преподавания дисциплины (модуля).

[2] Если отдельные элементы РП актуализированы разными педагогическими работниками, то необходимо указать соответствующую информацию, обеспечить подписание документа всеми педагогическими работниками.

Оглавление

**Аннотация рабочей программы дисциплины**
**«Информационная безопасность в экономической деятельности»**
Разработчик: Шевко Н.Р.

| | |
|---|---|
| **Цель изучения дисциплины** | Целью изучения дисциплины (модуля) является освоение компетенций, предусмотренных рабочей программой. |
| **Место дисциплины в структуре ООП** | Дисциплина «Информационная безопасность в экономической деятельности» относится к числу дисциплин обязательной части ОПОП (Б.1.О.17.) ОПОП высшего образования - программы специалитета, специальности 38.05.01 Экономическая безопасность |
| **Компетенции, формируемые в результате освоения дисциплины (модуля)** | ОПК - 6, ОПК - 7 |
| **Содержание дисциплины (модуля)** | Тема 1. Основные понятия и определения информационной безопасности.<br>Тема 2. Общий обзор законодательства Российской федерации в сфере информационной безопасности.<br>Тема 3. Персональные данные, личная и семейная тайна.<br>Тема 4. Государственная тайна.<br>Тема 5. Коммерческая тайна и иные виды тайн.<br>Тема 6. Криптография.<br>Тема 7. Техническая защита информации.<br>Тема 8. Особенности применения специальных технических средств при сборе информации.<br>Тема 9. Методы борьбы с киберпреступностью. |
| **Общая трудоемкость дисциплины (модуля)** | Общая трудоемкость дисциплины составляет 8 зачетных единиц, 288 часов. |
| **Форма промежуточной аттестации** | Экзамен |

## 1. Цели и планируемые результаты изучения дисциплины (модуля)

Целью изучения дисциплины (модуля) является освоение компетенций (индикаторов достижения компетенций), предусмотренных рабочей программой.

В совокупности с другими дисциплинами ОПОП дисциплина обеспечивает формирование следующих компетенций:

Таблица 1

| № п/п | Код компетенции | Название |
|---|---|---|
| | ОПК - 6 | Способен использовать современные информационные технологии и программные средства при решении профессиональных задач. |
| 1 | ИОПК 6.1. | Выбирает инструментальные средства для обработки экономической информации и обосновывать свой выбор |
| 2 | ИОПК 6.2 | Использует при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных |
| 3 | ИОПК 6.3. | Выполняет профессиональные задачи с использованием современных информационных технологий |
| | ОПК - 7 | Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. |
| 4 | ИОПК 7.1. | Обладает знаниями о современных информационных технологиях используемых при решении профессиональных задач |
| 5 | ИОПК 7.2. | Осуществляет сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач с использованием современных информационных технологий |
| 6 | ИОПК 7.3. | Обладает навыками обобщения и формулирования выводов, разработки рекомендаций при решении профессиональных задач с использованием современных информационных технологий в области экономической безопасности |

Планируемые результаты освоения дисциплины в части каждой компетенции указаны в картах компетенций по ОПОП.

## 2. Место дисциплины в структуре ООП

Дисциплина «Информационная безопасность в экономической деятельности» относится к числу дисциплин обязательной части ОПОП (Б.1.О.17.), формируемой участниками образовательных отношений.

## 3. Объем дисциплины и виды учебной работы

*Таблица 2.1*

*очная форма обучения*

| Вид учебной работы | | | Трудоемкость по семестрам | |
|---|---|---|---|---|
| | зач. ед. | час. | 4 | 5 |
| **Общая трудоемкость** дисциплины по учебному плану | 8 (4+4) | 288 | 144 | 144 |
| Контактная работа | | 64 | 34 | 30 |
| Самостоятельная работа под контролем преподавателя, НИРС | | 224 | 110 | 114 |
| Занятия лекционного типа | | 28 | 12 | 16 |
| Занятия семинарского типа | | 36 | 22 | 14 |
| в том числе с практической подготовкой (при наличии) | | 16 | 8 | 8 |
| **Форма промежуточной аттестации** | | | контрольное задание | экзамен |

## 4. Содержание дисциплины (модуля)

## 4.1. Текст рабочей программы по темам

**2 курс 4 семестр**

**Тема 1. Основные понятия и определения информационной безопасности.**

Понятие «информационная безопасность». Проблема информационной безопасности общества. Определение понятия «информационная безопасность». Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации. Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Угрозы информационной безопасности. Виды угроз. Приемы и методы защиты информации.

Обеспечение и защита прав и свобод граждан в части получения и использования информации, неприкосновенность частной жизни. Бесперебойное функционирование критической информационной инфраструктуры (КИИ). Развитие в России отрасли ИТ и электронной промышленности. Доведение до российской и международной общественности достоверной информации о государственной политике РФ. Содействие международной информационной безопасности.

**Тема 2. Общий обзор законодательства Российской федерации в сфере информационной безопасности**

Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.

Стратегические документы. ФЗ. Системообразующие документы. Государственные регуляторы – ФСТЭК России, ФСБ России. Постановления, затрагивающие – Минкомсвязь, Роскомнадзор , Банк России. Доктрина информационной безопасности России

**Тема 3. Персональные данные, личная и семейная тайна**

Конституции РФ ст. 23, 24,25; ФЗ №149. УК РФ ст. 137, 138. Закон по персональным данным – Федеральный закон от 27.07.2006 N 152-ФЗ (действ. ред.). Приказ ФСТЭК России №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных». Угроза нарушения целостности данных. Особенности и примеры реализации угрозы. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.

**Тема 4. Государственная тайна**

Распоряжение Президента РФ «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» (с изм.). История гостайны и Статья 283 УК РФ «Разглашение государственной тайны». Статья 284 УК РФ «Утрата документов, содержащих государственную тайну». Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.

**Тема 5. Коммерческая тайна и иные виды тайн**

Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ (последняя редакция). Правовая основа допуска и доступа персонала к защищаемым сведениям. Порядок отнесения коммерческих сведений к коммерческой тайне. Защита коммерческой тайны. Ответственность за разглашение коммерческой тайны. Категорирование информации в РФ. Виды информации ограниченного доступа. Профессиональная тайна. Журналистская тайна. Личная и семейная тайна. Тайна страхования. Аудиторская тайна.

**3 курс 5 семестр**

**Тема 6. Криптография**

Аспекты при изучении старых шифров. Необходимость использования цифровой подписи. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94 Квантовая криптография. Передача секретных ключей по радиоканалу. Безопасное распределение ключей. Инфраструктура управления открытыми ключами.

Исторические шифры и первые шифраторы. Шифр сдвига. Шифр замены. Шифр Рихарда Зорге. Расшифрование. Криптоанализ.

**Тема 7. Техническая защита информации**

Функции и задачи защиты информации. Методы и системы защиты информации. Основные виды угроз безопасности и классификация атак. Компьютерные вирусы и антивирусные программы. Кодификатор компьютерных преступлений интерпола. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. Категории, содержащие информационные материалы.

**Тема 8. Особенности применения специальных технических средств при сборе информации**

Виды политик безопасности. Понятие «Специальная техника». Классификация специальной техники, используемой в государстве и правоохранительных органах. Каналы утечки информации, требующие применения специальных технических средств, для защиты информации. Пассивные и активные средства защиты информации. Требования, предъявляемые к защите информации. Меры по обеспечению безопасности информаци-

онных систем: правовые, организационные и технические. Основные положения нормативно-правовых документов по организации защиты информации.

Единые критерии безопасности информационных технологий. Вербальная и невербальная информация. Подслушивание. Перехват информации с помощью электронных средств.

**Тема 9. Методы борьбы с киберпреступностью**

Виды и методы киберпреступлений. Цели и методы работы современных киберпреступников. Портрет потенциального злоумышленника. Экосистема теневого сегмента сети Интернет. Основные причины роста числа киберпреступлений. Криптовалюты и анонимные сети. Краткий обзор методов сокрытия авторства преступления и способов обналичивания похищенных средств на примере технологий VPN, Tor и криптовалюты Bitcoin Классификация киберпреступлений. Компьютерные преступления, и согласовывание их с международными нормами права. Атрибуция кибератак. Понятие источника действий в сети Интернет. Методы атрибуции источника кибератак. Возможность однозначно установить источник кибератак. Обзор практических кейсов. Основы компьютерной криминалистики. Понятие доказательств в цифровом виде. Источники сбора доказательств в цифровом виде. Методы и правовые основы компьютернотехнических экспертиз. Взаимодействие с правоохранительными органами и экспертными организациями в части расследования киберпреступлений. Основные направления деятельности Управления «К» МВД РФ и порядок взаимодействия. Центры реагирования на кибер инциденты CSIRT/CERT.

## 4.2.Разделы и темы дисциплины, виды занятий (тематический план)

### Тематический план

*Таблица 3.1*
*очная форма обучения*

| № | Раздел дисциплины, тема | Код компетенции | Общая трудоёмкость дисциплины | в том числе | | | | | Наименование оценочного средства |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Самостоятельная работа под контролем преподавателя, НИРС | Контактная работа | Занятия лекционного типа | Занятия семинарского типа | Практическая подготовка | |
| | | | час. | час. | час. | час. | час. | час. | |
| 1. | Тема 1. Основные понятия и определения информационной безопасности. | ОПК - 6, ОПК - 7 | 28 | 22 | 6 | 4 | 2 | - | вопросы для семинара (практического занятия) |
| 2. | Тема 2. Общий обзор законодательства Российской федерации в сфере информационной безопасности. | ОПК - 6, ОПК - 7 | 30 | 22 | 8 | 4 | 2 | 2 | вопросы для семинара (практического занятия), практические задачи |
| 3. | Тема 3. Персональные данные, личная и семейная тайна. | ОПК - 6, ОПК - 7 | 28 | 22 | 6 | 2 | 2 | 2 | вопросы для семинара (практического занятия), практические задачи |
| 4. | Тема 4. Государственная тайна. | ОПК - 6, ОПК - 7 | 28 | 22 | 6 | 2 | 2 | 2 | вопросы для семинара (практического занятия), практические задачи |
| 5. | Тема 5. Коммерческая тайна и иные виды тайн | ОПК - 6, ОПК - 7 | 28 | 22 | 6 | 2 | 2 | 2 | вопросы для семинара (практического занятия), практические задачи |
| 6. | Тема 6. Криптография. | ОПК - 6, ОПК - 7 | 38 | 30 | 8 | 4 | 2 | 2 | вопросы для семинара (практического занятия), практические задачи |

| № | Раздел дисциплины, тема | Код компетенции | Общая трудоёмкость дисциплины | в том числе | | | | | Наименование оценочного средства |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Самостоятельная работа под контролем преподавателя, НИРС | Контактная работа | Занятия лекционного типа | Занятия семинарского типа | Практическая подготовка | |
| | | | час. | час. | час. | час. | час. | час. | |
| 7. | Тема 7. Техническая защита информации. | ОПК - 6, ОПК - 7 | 36 | 28 | 8 | 4 | 2 | 2 | вопросы для семинара (практического занятия), практические задачи |
| 8. | Тема 8. Особенности применения специальных технических средств при сборе информации | ОПК - 6, ОПК - 7 | 36 | 28 | 8 | 4 | 2 | 2 | вопросы для семинара (практического занятия), практические задачи |
| 9. | Тема 9. Методы борьбы с киберпреступностью. | ОПК - 6, ОПК - 7 | 36 | 28 | 8 | 2 | 2 | 4 | вопросы для семинара (практического занятия), практические задачи |
| **ВСЕГО** | | | 288 | 224 | 64 | 28 | 18 | 18 | |

## 4.3. Самостоятельное изучение обучающимися разделов дисциплины

*Таблица 4.1*
*очная форма обучения*

| № темы дисциплины | Вопросы, выносимые на самостоятельное изучение | Количество часов |
|---|---|---|
| 1. | Основные понятия и определения информационной безопасности. | 22 |
| 2. | Общий обзор законодательства Российской федерации в сфере информационной безопасности. | 22 |
| 3. | Персональные данные, личная и семейная тайна. | 22 |
| 4. | Государственная тайна. | 22 |
| 5. | Коммерческая тайна и иные виды тайн | 22 |
| 6. | Криптография. | 30 |
| 7. | Техническая защита информации. | 28 |

| | | |
|---|---|---|
| 8. | Особенности применения специальных технических средств при сборе информации | 28 |
| 9. | Методы борьбы с киберпреступностью. | 28 |
| | ИТОГО: | 224 |

### 4.4. Темы курсового проекта (курсовой работы)

Не предусмотрено

## 5.Учебно-методическое и информационное обеспечение дисциплины (модуля)

#### 5.1. Учебно-методические рекомендации по изучению дисциплины (модуля)

В рамках тем «Доктрина информационной безопасности России», «Общий обзор законодательства Российской федерации в сфере информационной безопасности», «Персональные данные, личная и семейная тайна», «Государственная тайна» и «Коммерческая тайна и иные виды тайн» изучается процесс формирования и развития науки информационной безопасности, влияния на этот процесс политических, социальных, экономических условий, в том числе цифровизации общества. Вопросы, изучаемые в указанных темах, формируют глубокое, целостное и системное понимание информационной безопасности, а также его базовых категорий, что является основой для проведения научных исследований. В рамках освоения указанных тем потребуется изучение трудов ученых – классиков информационной безопасности, а также научных статей и иных публикаций современных ученых, посвященных защите информации. Темы «Криптография», «Техническая защита информации», «Особенности применения специальных технических средств при сборе информации», «Методы борьбы с киберпреступностью» имеют прикладной характер, поскольку нацелены на формирование знаний, умений, навыков, необходимых для осуществления трудовых функций, связанных с применением средств и методов защиты информации. На практических занятиях по указанным темам будет осуществляться практическая подготовка обучающихся путем выполнения соответствующих заданий (решение практических задач, участие в деловой игре и др.). Освоение указанных тем потребует изучения нормативных правовых актов, регламентирующих использование цифровых технологий.

### 5.2. Перечень нормативных правовых актов, актов высших судебных органов, материалов судебной практики

#### 5.2.1. Нормативные правовые акты

1. Конституция Российской Федерации.
2. Уголовный кодекс РФ.
3. Гражданский кодекс Российской Федерации.
4. Налоговый кодекс РФ .

5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
6. Федеральный закон "О техническом регулировании" N 184-ФЗ (с изм.).
7. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ (последняя редакция).
8. Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ (последняя редакция).
9. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция).
10. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (последняя редакция).
11. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»
12. Указ Президента РФ от 13.05.2017 N 208»О Стратегии экономической безопасности Российской Федерации на период до 2030 года».
13. Указ Президента РФ от 06.08.2014 N 560 «О применении отдельных специальных экономических мер в целях обеспечения безопасности Российской Федерации».
14. Указ Президента РФ от 21.06.2019 N 287 «Об отдельных мерах по обеспечению национальной безопасности Российской Федерации и защите граждан Российской Федерации от преступных и иных противоправных действий».
15. Указ Президента РФ от 31.03.2000 N 616 «О дополнительных мерах по обеспечению безопасного функционирования важнейших отраслей экономики» ;
16. Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года (разработан Минэкономразвития России).

## 5.2.2. Официальные акты высших судебных органов, материалы судебной практики

17. Апелляционное определение СК по делам военнослужащих Верховного Суда РФ от 11 октября 2018 г. N 201-АПГ18-2 Суд оставил без изменения решение суда первой инстанции по делу об оспаривании действий командира войсковой части, связанных с лишением допуска к сведениям, составляющим государственную тайну, поскольку заявитель нарушил требования о защите информации, составляющей государственную тайну, что выразилось в обработке такой информации на компьютере, не учтенном в подразделении секретного делопроизводства.Информация Конституционного Суда РФ "Конституционно-правовая защита предпринимательства: актуальные аспекты (на основе решений Конституционного Суда Российской Федерации 2018 - 2020 годов)" (подготовлена Секретариатом Конституционного Суда Российской Федерации) (одобрено решением Конституционного Суда Российской Федерации от 17 декабря 2020 г.)
18. Обзор судебной практики Верховного Суда Российской Федерации .
19. Обзор судебной практики Верховного Суда Российской Федерации N 2 (2019) (утв. Президиумом Верховного Суда РФ 17 июля 2019 г.).Обзор по вопросам судебной практики, возникающим при рассмотрении дел о защите "Обзор судебной практики по вопросам, связанным с применением Федерального закона от 18.07.2011 N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц".
20. Обобщение практики и правовых позиций международных договорных и внедоговорных органов, действующих в сфере защиты прав и свобод человека, по вопросам защиты права лица на свободу собраний и объединений (подготовлено Верховным Судом РФ, июль 2021 г.).
21. Определение Конституционного Суда РФ от 28 декабря 2021 г. N 2929-О "Об отказе в принятии к рассмотрению жалобы гражданина Ишкова Виктора Михайловича на нарушение его конституционных прав пунктом 2 статьи 5 Федерального закона "О порядке рассмотрения обращений граждан Российской Федерации", а также частью 2 статьи 8 Федерального закона "Об информации, информационных технологиях и о защите информации".

22. Определение Конституционного Суда РФ от 30 ноября 2021 г. N 2360-О "Об отказе в принятии к рассмотрению жалобы гражданина Михайлова Олега Юрьевича на нарушение его конституционных прав частью 4 статьи 6 Федерального закона "Об информации, информационных технологиях и о защите информации" и пунктом 13 Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации".
23. Определение Конституционного Суда РФ от 19 октября 2021 г. N 2129-О "Об отказе в принятии к рассмотрению жалобы гражданина С. на нарушение его конституционных прав частью 1 статьи 10.3 Федерального закона "Об информации, информационных технологиях и защите информации".
24. Постановление Европейского Суда по правам человека от 30 апреля 2019 г. Дело "Каблис (Kablis) против Российской Федерации" (Жалобы NN 48310/16 и 59663/17) (Третья секция).
25. Постановление Суда по интеллектуальным правам от 2 октября 2020 г. N С01-1117/2020 по делу N А56-37859/2019 Суд оставил без изменения вынесенные ранее судебные решения по делу о защите исключительного права на базу данных, поскольку суды нижестоящих инстанций установили принадлежность истцу указанного исключительного права, его нарушение ответчиком, а также факт использования ответчиком сведений, составляющих коммерческую тайну истца, при наличии соглашения сторон о конфиденциальности соответствующих сведений.
26. Постановление Пленума Верховного Суда РФ от 17 декабря 2015 г. N 56 "О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)".

## 5.3. Информационное обеспечение освоения дисциплины (модуля)

Информационные, в том числе электронные ресурсы Университета, а также иные электронные ресурсы, необходимые для изучения дисциплины (модуля):

| № п./п. | Наименование | Адрес в сети Интернет |
|---|---|---|
| | Электронные библиотечные системы* | |
| 1. | ZNANIUM.COM | http ://znanium.com<br>Основная коллекция и<br>коллекция издательства Статут 2 |
| 2. | ЭБС ЮРАЙТ | www.biblio-online.ru<br>коллекция РГУП |
| 3. | ЭБС «BOOK.ru» | www.book.ru<br>коллекция издательства Проспект Юридическая литература; коллекции издательства Кнорус Право, Экономика и Менеджмент |
| 4. | East View Information Services | www.ebiblioteka.ru<br>Универсальная база данных периодики (электронные журналы) |
| 5. | НЦР РУКОНТ | http://rucont.ru/<br>Раздел Ваша коллекция - РГУП-периодика (электронные журналы) |
| | Интернет ресурсы | |
| 6. | Информационно-образовательный портал РГУП | www.op.rai.ru электронные версии учебных, научных и научно-практических изданий РГУП |
| 7. | Система электронного обучения Фемида | www.femida.raj/ru<br>Учебно-методические комплексы, |

| | | |
|---|---|---|
| | | Рабочие программы по направлению подготовки |
| 8. | Правовые системы | Гарант, Консультант, Кодекс |
| 9. | Официальный сайт Университета | www.rgup.ru |

**Ресурсы сети Интернет**

1) сервер органов государственной власти российской Федерации «Официальная Россия» (www.gov.ru),
2) официальный сайт Совета Федерации Федерального Собрания Российской Федерации (www.council.gov.ru),
3) официальный сайт Конституционного Суда Российской Федерации (ks.rfnet.ru),
4) официальный сайт Верховного суда Российской Федерации (www.supcourt.ru, www.arbitr.ru),
5) официальный сайт Банка России (www.cbr.ru),
6) официальный Интернет-портал Правительства Российской Федерации (www.government.gov.ru),
7) официальный сайт Министерства финансов Российской Федерации (www.minfin.ru),
8) официальный сайт Федерального казначейства (www.roskazna.ru),
9) официальный сайт Федеральной налоговой службы Российской Федерации (www.nalog.ru),
10) официальный сайт Федеральной таможенной службы Российской Федерации (www.customs.ru),
11) официальный сайт Фонда социального страхования Российской Федерации (www.fss.ru),
12) официальный сайт Пенсионного фонда Российской Федерации (www.pfrf.ru),
13) официальный сайт Фонда обязательного медицинского страхования Российской Федерации (www.ffoms.ru).

**Основная и дополнительная литература** указана в Карте обеспеченности литературой.

## 6. Материально-техническое обеспечение

Для материально-технического обеспечения дисциплины используются специальные помещения. Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочим программам дисциплин. Демонстрационное оборудование представлено в виде мультимедийных средств. Учебно-наглядные пособия представлены в виде экранно-звуковых средств, печатных пособий, слайд-презентаций, видеофильмов, макетов и т.д., которые применяются по необходимости в соответствии с темами (разделами) дисциплины.

Для самостоятельной работы обучающихся помещения оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.

Перечень специальных помещений ежегодно обновляется и отражается в справке о материально-техническом обеспечении основной образовательной программы.

Состав необходимого комплекта лицензионного программного обеспечения ежегодно обновляется, утверждается и отражается в справке о материально-техническом обеспечении основной образовательной программы.

| **Наименование дисциплины (модуля), практик в соответствии с учебным планом** | **Наименование специальных* помещений и помещений для самостоятельной работы** | **Оснащенность специальных помещений и помещений для самостоятельной работы** | **Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа** | |
|---|---|---|---|---|
| Информационная безопасность в экономической деятельности | Кабинет информатики: доступ к сети Internet<br><br>Лаборатория информационных технологий в профессиональной деятельности: доступ к сети Internet<br><br>Лаборатория технических средств обучения: доступ к сети Internet (помещение 1001 – комната 16,17,18) | Информационные стенды, дидактические материалы, проектор, ноутбук, столы, стулья, доска<br>Информационные стенды, дидактические материалы, проектор, ноутбук, столы, стулья, доска<br>Информационные стенды, дидактические материалы, проектор, ноутбук, столы, стулья, доска | 1. бессрочный договор №527Р/2022 от 11.04.2022г,,<br>2. договор от 23.12.19г.<br>3. номер лицензии 46289495 договор №16к от 18.12.2009г.,<br>4. по договорам №293 от 24.12.2012г., №13 от 13.12.2013г.<br>5. по договорам №16k от 18.12.2009г., №7к от 12.12.2011г., №13 от | 1.СПС КонсультантПлюс<br>2.Сопровождение ЭПС "Система Гарант"<br>3.Офис MS Office Professional Plus 2007<br>4. Microsoft Office Professional Plus 2013 RUS<br>5..MS WinPro 7, 8, 8.1 |

| | | | | |
|---|---|---|---|---|
| | | | 13.12.2013г., №293 от 24.12.2012г., | |

# 7. Карта обеспеченности литературой

Кафедра правовой информатики, информационного права и естественно-научных дисциплин
Специальность:38.05.01 «Экономическая безопасность» (уровень специалитета)
Профиль (специализация): Экономико-правовое обеспечение экономической безопасности
Дисциплина: **«Информационная безопасность в экономической деятельности»**
Курс: 2 и 3

| **Наименование, Автор или редактор, Издательство, Год издания, кол-во страниц** | **Вид издания** | |
|---|---|---|
| | **ЭБС (указать ссылку)** | **Кол-во печатных изд. в библиотеке вуза** |
| **1** | **2** | **3** |
| **Основная литература** | | |
| Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 216 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1784437 (дата обращения: 18.04.2023). – Режим доступа: по подписке. | https://znanium.com/catalog/document?id=379717 | |
| Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения: 26.05.2023). – Режим доступа: по подписке. | https://znanium.com/catalog/document?id=427455#bib | |
| **Дополнительная литература** | | |

| | | |
|---|---|---|
| Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 26.05.2023). – Режим доступа: по подписке. | https://znanium.com/catalog/document?id=393765#bib | |
| Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2019. - 83 с. - ISBN 978-5-7782-3918-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1866895 (дата обращения: 26.05.2023). – Режим доступа: по подписке. | https://znanium.com/catalog/document?id=396938#bib | |
| Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-М, 2021. - 223 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178148 (дата обращения: 18.04.2023). – Режим доступа: по подписке. | https://znanium.com/catalog/document?id=364728 | |

Зав. библиотекой  Зав. кафедрой 

## 8. Фонд оценочных средств

## 8.1. Паспорт фонда оценочных средств по дисциплине «Информационная безопасность в экономической деятельности»

| № п/п | Контролируемые разделы (темы) дисциплины | Код контролируемой компетенции (или ее части) | Наименование оценочного средства |
|---|---|---|---|
| 1. | Тема 1. Основные понятия и определения информационной безопасности. | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 2. | Тема 2. Общий обзор законодательства Российской федерации в сфере информационной безопасности. | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 3. | Тема 3. Персональные данные, личная и семейная тайна. | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 4 . | Тема 4. Государственная тайна. | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 5. | Тема 5. Коммерческая тайна и иные виды тайн | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 6. | Тема 6. Криптография. | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 7. | Тема 7. Техническая защита информации. | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 8. | Тема 8. Особенности применения специальных технических средств при сборе информации | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |
| 9. | Тема 9. Методы борьбы с киберпреступностью. | ОПК - 6, ОПК - 7 | Практические задания<br>тесты<br>вопросы для семинара<br>доклады по рефератам<br>вопросы для экзамена |

В целях применения балльно-рейтинговой системы баллы за результаты учебной работы между заявленными оценочными средствами распределяются:

| Форма обучения | Очная |
|---|---|
| Всего баллов, в том числе: | 0-26 |
| Вопросы для семинаров | 0-6 |
| Доклад с презентацией | 0-10 |
| Практические задачи | 0-10 |

При каждом применении оценочного средства преподаватель выставляет баллы в установленных пределах.

По итогам семестра по каждому оценочному средству определяется (1) общая сумма баллов и (2) средний балл (общая сумма баллов / количество семинаров (практических занятий), на которых оценочное средство применялось).

Сумма средних баллов по всем оценочным средствам формирует баллы, выставляемые обучающимся за результаты учебной работы в каждом семестре.

## 8.2.Оценочные средства

## Вопросы для семинаров (практических занятий)

Вопросы для семинаров предназначены для устного опроса обучающихся. Устный опрос проводится преподавателем по вопросам соответствующей темы дисциплины.

Обучающийся обязан подготовиться к устному опросу, руководствуясь Учебно-методическими рекомендациями по изучению дисциплины.

С учетом того, что в рамках текущего контроля проверяется подготовленность обучающихся по всем вопросам, преподаватель - исходя из количества обучающихся, присутствующих на семинаре (практическом занятии), а также объема отдельных вопросов темы - формулирует на семинаре (практическом занятии) вопрос для каждого обучающегося, который может объединять несколько вопросов темы. Сформулированный вопрос адресуется обучающемуся в устной форме.

Обучающийся устно отвечает на заданный вопрос. Ответ дается без подготовки; в ходе ответа обучающийся не вправе использовать учебные и учебно-методические материалы, за исключением настоящей рабочей программы. После ответа обучающегося преподаватель может задать уточняющие вопросы, если ответ на вопрос был неполным либо содержал ошибки.

Ответ на сформулированный вопрос оценивается в соответствии с критериями, установленными в настоящей рабочей программе.

**Тема 1. Основные понятия и определения информационной безопасности.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 1. | Понятие информации. Виды информации.<br>Угрозы информации: понятие и классифткация.<br>Россия в международных рейтингах ИБ<br>Эволюция правовых основ обеспечения информационной безопасности | ОПК - 6, ОПК - 7 |

**Тема 2. Общий обзор законодательства Российской Федерации в сфере информационной безопасности**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|

| | | |
|---|---|---|
| 2. | Рынок аппаратного обеспечения для ИБ.<br>Оборудование для защиты информации (рынок России)<br>Рынок ПО для защиты информации<br>Тренды российского рынка информационной безопасности | ОПК - 6, ОПК - 7 |

**Тема 3. Персональные данные, личная и семейная тайна**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 3. | В чем сходство, а в чем принципиальные отличия в определении понятия «экономическая безопасность государства» у разных авторов<br>Основные документы в сфере экономической безопасности в России.<br>Проблема экономической безопасности на региональном уровне применительно к условиям Российской Федерации<br>Устойчиво безопасное социально-экономическим развитие территории. Какова взаимосвязь этого понятия с понятием «экономическая безопасность»? | ОПК - 6, ОПК - 7 |

**Тема 4. Государственная тайна**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 4. | Государственная тайна - важный элемент информационных ресурсов страны.<br>Структура системы защиты государственной тайны. Методы защиты государственной тайны<br>Правовая основа законодательства Российской Федерации о государственной тайне и защите информации | ОПК - 6, ОПК - 7 |

**Тема 5. Коммерческая тайна и другие виды тайн**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 5. | Понятие коммерческой тайны. Механизм функционирования КТ<br>Правовой режим коммерческой тайны. Экономическая оценка КТ.<br>Механизмы обеспечения и защиты КТ. Охрана коммерческой тайны в трудовых отношениях. Защита прав на коммерческую тайну. | ОПК - 6, ОПК - 7 |

**Тема 6. Криптография**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 6. | История криптографии<br>Шифрование и криптоанализ<br>Виды и способы криптографических преобразований<br>Шифры, их виды и свойства<br>Симметричные криптографические системы<br>Асимметричные криптографические системы | ОПК - 6, ОПК - 7 |

| | | |
|---|---|---|
| | . Электронная подпись | |

**Тема 7. Техническая защита информации**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 7. | Технические средства защиты информации<br>Программные средства защиты информации<br>Аппаратные средства защиты информации<br>Организационно-технические средства защиты информации<br>Инженерно-технические средства защиты информации<br>Требования по технической защите данных<br>Лицензирование | ОПК - 6, ОПК - 7 |

**Тема 8. Особенности применения специальных технических средств при сборе информации**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 8. | Понятие, назначение и классификация специальной техники<br>Правовая основа применения специальной техники<br>Способы применения специальных технических средств | ОПК - 6, ОПК - 7 |

**Тема 9. Методы борьбы с киберпреступностью**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 9. | Виды и методы киберпреступлений<br>Портрет потенциального злоумышленника<br>Криптовалюты и анонимные сети<br>Краткий обзор методов сокрытия авторства преступления и способов обналичивания похищенных средств на примере технологий VPN, Tor и криптовалюты Bitcoin<br>Классификация киберпреступлений<br>Понятие доказательств в цифровом виде. Источники сбора доказательств в цифровом виде. Методы и правовые основы компьютернотехнических экспертиз.<br>Взаимодействие с правоохранительными органами и экспертными организациями в части расследования киберпреступлений. | ОПК - 6, ОПК - 7 |

Критерии оценивания:

| **Критерии** | **Баллы** |
|---|---|
| | **очная** |
| Знания отсутствуют либо имеют фрагментарный характер | 0-1,5 |
| Неполные знания | 1,6-3 |
| Сформированные знания, имеющие незначительные пробелы | 3,1-4,5 |
| Полностью сформированные знания | 4,6-6 |

# Практические задачи

1. Методические рекомендации.

В рамках практических задачах проверяется сформированность умений и навыков.

Поскольку выполнение задач требует сформированности определенных знаний, преподаватель осуществляет текущий контроль за сформированностью знаний путем устного опроса по вопросам темы.

1. Перечень компетенций (части компетенции), проверяемых оценочным средством (наименование, код):

| № п/п | Код компетенции | Название |
|---|---|---|
| 1 | ОПК - 6 | ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач. |
| 2 | ОПК - 7 | ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. |

**Тема 1. Основные понятия и определения информационной безопасности**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 1 | Менеджер компании «Ника» имеет доступ к корпоративной электронной почте, для того чтобы менеджер компании не забыл пароль он прикрепил стикер на клавиатуру. Также менеджер компании в рабочее время пользуется социальными сетями (Вконтакте, Одноклассники, Instagramm и т.д). При этом он закрывает браузер не нажимая кнопку "выход", использует Яндекс браузер, имеет 1-2 несложных пароля на все ресурсы с датой рождения и именем.<br>Менеджер - коммуникабельная, активная девушка, участница форумов. На сайтах регистрируется под ником Mari.<br>ООО «Ника» занимается перевозкой грузов на территории РФ.<br>Определите основные риски и угрозы в сфере информационной безопасности для компании. Перечислите основные методы защиты и предотвращения от уничтожения информации организации, в том числе предотвращения утечки коммерческой тайны. | ОПК-6, ОПК-7 |

**Тема 2. Общий обзор законодательства Российской Федерации в сфере информационной безопасности**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 2 | Менеджер компании «Ника» имеет доступ к корпоративной электронной почте, для того чтобы менеджер компании не забыл пароль он прикрепил стикер на клавиатуру. Также ме- | ОПК-6, ОПК-7 |

| | | |
|---|---|---|
| | неджер компании в рабочее время пользуется социальными сетями (Вконтакте, Одноклассники, Instagramm и т.д). При этом он закрывает браузер не нажимая кнопку "выход", использует Яндекс браузер, имеет 1-2 несложных пароля на все ресурсы с датой рождения и именем.<br>Менеджер - коммуникабельная, активная девушка, участница форумов. На сайтах регистрируется под ником Mari.<br>ООО «Ника» занимается перевозкой грузов на территории РФ.<br>Вопросы:<br>1. Охарактеризуйте были ли соблюдены требования по обеспечению информационной безопасности, какие требования правовых актов в области защиты информационной безопасности были нарушены?<br>2. Напишите какими внутренними документами должна быть обеспечена организация для защиты информационных данных исходя из вида деятельности.<br>3. Какие юридические аспекты необходимо учитывать для внесения изменений в политику безопасности компании, чтобы предотвратить утечки конфиденциальной информации? | |

**Тема 6. Криптография**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 6 | Расшифровать текст<br>«В_ОН,_Т_ОЭЗКНОА_УОРСЗКНОА»,<br>КЛЮЧ 1 - КРУТО, КЛЮЧ 2 - СТУЖА. | ОПК-6, ОПК-7 |

Критерии оценивания:

| Критерии | Баллы |
|---|---|
| | Очная |
| Умение не сформировано / Навык не сформирован | 0-2,5 |
| Умение сформировано частично / Навык сформирован частично | 2,6-5 |
| Умение сформировано, но имеет несущественные недостатки / Навык сформирован, но имеет несущественные недостатки | 5,1-7,5 |
| Умение сформировано полностью / Навык сформирован полностью | 7,6-10 |

## Темы докладов с выступлениями в форме интерактивных презентаций по дисциплине

1. Методические рекомендации.

Посредством заслушивания выступлений обучающихся с докладами проверяется сформированность углубленных знаний, а также умений и навыков по формируемым компетенциям.

При подготовке докладов с выступлениями в форме интерактивных презентаций обучающимся следует руководствоваться учебно-методическими материалами по дисциплине.

Подготовка докладов, посвященных проводимым в России реформам в сфере цифровизации, требует следующего структурирования материала:

- описание условий и причин проведения реформы;
- цели проводимой реформы;
- инициаторы реформы;
- содержание реформы;
- результаты реформы;
- правовые основы реформы.

В процессе подготовки обучающиеся учатся анализировать и давать оценку решениям, направленным на совершенствование государственного управления в сфере защиты информации.

Подготовка докладов, посвященных цифровым инновациям в России, требует следующего структурирования материала:

- описание инновации;
- цель внедрения инновации;
- инициаторы реформы;
- полученные результаты проведенной реформы;
- правовые основы реформы.

1. Перечень компетенций (части компетенции), проверяемых оценочным средством (наименование, код):

| № п/п | Код компетенции | Название |
|---|---|---|
| 1 | ОПК - 6 | ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач. |
| 2 | ОПК - 7 | ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. |

**Тема 1. Основные понятия и определения информационной безопасности.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 1. | 1) Россия в международных рейтингах ИБ | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| 6. | 2) Интересы личности, общества и государства в информационной сфере. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| 7. | 3) Интернет и информационная безопасность | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| 8. | 4) Методы и механизмы обеспечения информационной безопасности. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| 9. | 5) Кадры цифровой экономики | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., |

| | | |
|---|---|---|
| | | ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| 10. | 6) Нейротехнологии и искусственный интеллект (Банковская программа) | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 2. Общий обзор законодательства Российской федерации в сфере информационной безопасности.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 2. | 1) Россия в международных рейтингах ИБ | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Эволюция правовых основ обеспечения информационной безопасности | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) История появления концепций национальной безопасности. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Концепция информационной безопасности<br>5) Россия в мировом сообществе | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 3. Персональные данные, личная и семейная тайна.**

| | | |
|---|---|---|
| 3. | 1) Персональные данные: понятие, виды. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Персональные данные: хранение и обработка. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) Личная тайна. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Семейная тайна. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 4. Государственная тайна.**

| | | |
|---|---|---|
| 4. | 1) Перечень сведений, составляющих государственную тайну. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Сведения, которые не могут относиться к государственной тайне. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) Оформление допуска и предоставление доступа к государственной тайне. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Рассекречивание сведений и их носителей. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 5) Процедура отнесения сведений к государственной тайне и их засекречивания. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 5. Коммерческая тайна и иные виды тайн.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 5. | 1) Конституционные основы защиты коммерческой тайны. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Предоставление доступа к коммерческой тайне. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) Охрана коммерческой тайны в трудовых отношениях. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Служебная тайна. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., |

| | | |
|---|---|---|
| | | ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 5) Виды тайн. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 6. Криптография.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 6. | 1) История криптографии. Шифрование и криптоанализ | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Виды и способы криптографических преобразований | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) Электронная подпись | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Симметричные и асимметричные криптографические системы | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 7. Техническая защита информации.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 7. | 1) Технические средства защиты информации | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Требования по технической защите данных | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) Лицензирование | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Правовая основа применения специальной техники | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 8. Особенности применения специальных технических средств при сборе информации.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 8. | 1) Виды политик безопасности. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Классификация специальной техники, используемой в государстве и правоохранительных органах. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) Каналы утечки информации, требующие применения специальных технических средств, для защиты информации. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Меры по обеспечению безопасности информационных систем: правовые, организационные и технические. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 5) Подслушивание. Перехват информации с помощью электронных средств. | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

**Тема 9. Методы борьбы с киберпреступностью.**

| № темы | Вопросы | Код компетенции (части) компетенции |
|---|---|---|
| 9. | 1) Основные виды киберпреступности | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., |

| | | |
|---|---|---|
| | | ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 2) Особенности расследования киберпреступлений | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 3) Уголовная ответственность за совершение киберпреступлений | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |
| | 4) Противодействие киберпреступности | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

Критерии оценивания:

| **Критерии** | **Баллы** |
|---|---|
| Умение не сформировано / Навык не сформирован | 0-2,5 |
| Умение сформировано частично / Навык сформирован частично | 2,6-5 |
| Умение сформировано, но имеет несущественные недостатки / Навык сформирован, но имеет несущественные недостатки | 5,1-7,5 |
| Умение сформировано полностью / Навык сформирован полностью | 7,6-10 |

## Комплект заданий для контрольного задания

При выполнении контрольной работы следует руководствоваться методическими рекомендациями по подготовке докладов с выступлениями в форме интерактивных презентаций, а также выполнения практических заданий.

Каждый из обучающихся выполняет один вариант контрольной работы. Варианты распределяются между обучающимися исходя из первой буквы фамилии: обучающиеся, чьи фамилии начинаются на буквы от «А» до «Ж» выполняют первый вариант контрольного задания; обучающиеся, чьи фамилии начинаются на буквы от «З» до «Р» - второй вариант, обучающиеся, чьи фамилии начинаются на буквы от «С» до «Я» - третий вариант.

Задания контрольного задания оформляются в письменном виде на бумаге формата А4, шрифт 14, интервал 1,5.

1. Перечень компетенций (части компетенции), проверяемых оценочным средством (наименование, код):

| № п/п | Код компетенции | Название |
|---|---|---|
| 1 | ОПК - 6 | ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач. |
| 2 | ОПК - 7 | ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. |

| Вариант | Задание | Формируемая компетенция |
|---|---|---|
| **1** | **1 задание - дать правильный ответ**<br>1**.** Информационное общество и его основные черты.<br>2. В чем отличие угрозы от опасности?<br>3. Что такое экономическая безопасность?<br>4. Приведите классификацию и дайте определение видам экономической безопасности.<br>5. Что является объектом, субъектами и предметом экономической безопасности?<br>6. Должны ли (если «да» — то как часто) пересматриваться Концепция и Государственная<br>стратегия экономической безопасности России?<br>7. Каков механизм обеспечения экономической безопасности России?<br>8. Назовите основные угрозы экономической безопасности России.<br>**2 задание.**<br>«Систему свободного предпринимательства можно сравнить с гигантским компьютером, способным решать свои собственные проблемы автоматически. Но каждый, кто имел дело с большими компьютерами, знает, что иногда они дают сбой и не могут | ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3. |

<table>
<tr><td></td><td>действовать без присмотра» (В. Леонтьев).<br>Используя свои знания, охарактеризуйте экономические проблемы, которые экономическая система способна решать самостоятельно, и экономические проблемы, которые требуют вмешательства государства.<br>3 задание.<br>Расшифруйте «ЬЯД_!-_ _ ЭТАКЗОН_НОЕМЙ_ОЕУ», КЛЮЧ 1 - СУДЬЯ, КЛЮЧ 2 - ЮРИСТ.</td><td></td></tr>
<tr><td>2</td><td>1задание - дать правильный ответ<br>1.Общие условия осуществления бизнеса.<br>2. Конкретные угрозы бизнесу.<br>3. Методы обеспечения юридической безопасности<br>4. Механизм обеспечения экономической безопасности бизнеса.<br>5. Государственное регулирование мер по экономической безопасности бизнеса.<br>6. Внутригосударственные проблемы экономической безопасности и развития бизнеса.<br>7. Система мер по обеспечению экономической безопасности бизнеса.<br>8. Пороговые значения индикаторов экономической безопасности и их обоснование.<br>2 задание.<br>Работник обратился в суд по поводу нарушения сотрудниками отдела кадров предприятия его права на защиту персональной информации (зафиксирована утечка сведений персонального характера).<br>Оцените ситуацию, определите виновных и причины.<br>Разработайте меры по предотвращению подобных ситуаций.<br>3 задание.<br>Расшифруйте «ТЛ_ЬЕЙЗКА_ВСИШЫООААДН-УЫНГ», КЛЮЧ 1 - КРУТО, КЛЮЧ 2 - СПОРТ.</td><td>ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3.</td></tr>
<tr><td>3</td><td>1задание - дать правильный ответ<br>1. Свойства информации.<br>2.Общие положения концепции безопасности коммерческого предприятия.<br>3. Цели и задачи экономической безопасности предприятия.<br>4.Факторы и источники угроз ЭБП.<br>5. Какова общая схема обеспечения ЭБП?<br>6.Что такое «функциональная составляющая ЭБП»? Назовите виды функциональных составляющих.<br>7. Какими способами можно обеспечить управление ЭБП?<br>8. Укажите основные пороговые значения ЭБП.<br>2 задание. Заполните таблицу<br>Таблица .Основные методы и средства несанкционированного получения информации и возможная защита от них<br><table><tr><td>№ п/п</td><td>Действие человека (типовая ситуация)</td><td>Каналы утечки информации</td><td>Методы и средства получения информации</td><td>Методы и средства защиты информации</td></tr><tr><td>1</td><td>Разговор в помещении или на</td><td></td><td></td><td></td></tr></table></td><td>ИОПК 6.1., ИОПК 6.2., ИОПК 6.3., ИОПК 7.1., ИОПК 7.2., ИОПК 7.3.</td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| | улице | | | |
| 2 | Разговор по проводному телефону | | | |
| 3 | Разговор по Радиотелефону | | | |
| 4 | Документ на бумажном носителе | | | |
| 5 | Изготовление документа на бумажном носителе | | | |
| 6 | Документ на небумажном носителе | | | |
| 7 | Изготовление документа на небумажном носителе | | | |
| 8 | Передача документа по каналу связи | | | |

**3 задание.**

Расшифруйте «Н!АО_ _КЗЯАИВНВООСИБТТ_ЫАЙ», КЛЮЧ 1 - ДРЕВО, КЛЮЧ 2 - ТРАВА.

Критерии оценивания:

| **Критерии** | **Баллы** |
|---|---|
| | **Очная** |
| Умение не сформировано / Навык не сформирован | 0-5 |
| Умение сформировано частично / Навык сформирован частично | 6-10 |
| Умение сформировано, но имеет несущественные недостатки / Навык сформирован, но имеет несущественные недостатки | 11-15 |
| Умение сформировано полностью / Навык сформирован полностью | 16-20 |

## Тестовые задания

## Содержание банка тестовых заданий

I:
S: К правовым методам, обеспечивающим информационную безопасность, относятся:
-: Разработка аппаратных средств обеспечения правовых данных
-: Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+: Разработка и конкретизация правовых нормативных актов обеспечения безопасности

I:
S: Основными источниками угроз информационной безопасности являются все указанное в списке:
-: Хищение жестких дисков, подключение к сети, инсайдерство
+: Перехват данных, хищение данных, изменение архитектуры системы
-: Хищение данных, подкуп системных администраторов, нарушение регламента работы

I:
S: Виды информационной безопасности:
+: Персональная, корпоративная, государственная
-: Клиентская, серверная, сетевая
-: Локальная, глобальная, смешанная

I:
S: Цели информационной безопасности – своевременное обнаружение, предупреждение:

+: несанкционированного доступа, воздействия в сети

-: инсайдерства в организации

-: чрезвычайных ситуаций

I:

S: Основные объекты информационной безопасности:

+: Компьютерные сети, базы данных

-: Информационные системы, психологическое состояние пользователей

-: Бизнес-ориентированные, коммерческие системы

I:

S: Какой вид идентификации и аутентификации получил наибольшее распространение:

-: системы PKI:

+: постоянные пароли

-: одноразовые пароли

I:

S: Под какие системы распространение вирусов происходит наиболее динамично:

-: WIndows

-: Mac OS

+: Android

I:

S: Заключительным этапом построения системы защиты является:

+: сопровождение

-: планирование

-: анализ уязвимых мест

I:

S: Какие угрозы безопасности информации являются преднамеренными:

-: ошибки персонала

-: открытие электронного письма, содержащего вирус

+: не авторизованный доступ

I:

S: Какой подход к обеспечению безопасности имеет место:

-: теоретический

+: комплексный

-: логический

I:

S: Из перечисленного в обязанности сотрудников группы информационной безопасности входит:

-: устранение дефектов аппаратной части

-: исправление ошибок в программном обеспечении

+: управление доступом пользователей к данным

I:

S: При передаче по каналам связи на канальном уровне избыточность вводится для:

-: реализации проверки со стороны получателя

+: контроля ошибок

-: контроля канала связи

I:

S: Проверка подлинности пользователя по предъявленному им идентификатору:

-: идентификация

-: аудит

+: аутентификация

I:

S: Согласно “Европейским критериям” минимальную адекватность обозначает уровень:

+: E0

-: E1

-: E6

I:

S: Из перечисленного подсистема управления криптографическими ключами структурно состоит из:

-: подсистемы защиты ключей

-: подсистемы генерации ключей

+: центра распределения ключей

I:

S: Из перечисленного на транспортном уровне рекомендуется применение услуг:

-: контроля графика

+: аутентификации

-: контроля трафика

I:

S: Из перечисленного на транспортном уровне рекомендуется применение услуг:

+: конфиденциальности

-: контроля трафика

-: контроля графика

I:

S: Обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней:

+: шифрование

-:  зашифровка

-:  закрытость

I:

S: Сколько лет назад появилось шифрование:

-: три тысячи лет назад

+: четыре тысячи лет назад

-: шесть тысяч лет назад

I:

S: Первое известное применение шифра:

-:  индийский текст

-:  русский текст

+: египетский текст

I:

S: Какое ещё определение можно дать шифрованию:

+: преобразовательный процесс исходного текста в зашифрованный

-:  упорядоченный набор из элементов алфавита

-:  неупорядоченный набор из элементов алфавита

I:

S: Что такое дешифрование:

-: пароли для доступа к сетевым ресурсам

-: сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

+: на основе ключа шифрованный текст преобразуется в исходный

I:

S: Пользователи являются авторизованными, если они обладают определённым:

-: математическим ключом

+: аутентичным ключом

-: паролем

КАЗАНСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
**«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»**

## Вопросы, выносимые на экзамен, по дисциплине

## «Информационная безопасность в экономической деятельности»

1. Информационная безопасность
2. Нормативно-правовое обеспечение информационной безопасности
3. Угрозы и риски информационной безопасности.
4. Экономика информационной безопасности.
5. Принципы криптографии.
6. Асимметричное шифрование и электронная подпись.
7. Понятия экономической безопасности, опасности, угрозы.
8. Виды опасностей. Постоянные источники опасностей.
9. Общие характеристики видов угроз.
10. Сущность риска. Понятие вызова.
11. Классификация безопасности.
12. Национальные интересы России в области информационной безопасности.
13. Национальные приоритеты России в обеспечении экономической безопасности.
14. Содержание угроз национальной безопасности.
15. Классификация угроз национальной безопасности: по масштабу, по влиянию, по характеру возникновения, по нахождению источника.
16. Классификация угроз национальной безопасности: по вероятности и времени возникновения, по формам, по вероятности реализации и ожидаемого ущерба, по точности оценки.
17. Внутренние угрозы национальной безопасности России.
18. Внешние угрозы национальной безопасности России.
19. Обеспечение национальной безопасности: типы, стратегии, этапы.
20. Механизм обеспечения национальной безопасности.
21. Принципы обеспечения национальной безопасности в РФ.
22. Принципы построения и функционирования системы обеспечения национальной безопасности.
23. Государственная и общественная системы обеспечения национальной безопасности.
24. Функции, силы и средства обеспечения национальной безопасности.
25. Институты обеспечения национальной безопасности России.
26. Задачи и функции Совета Безопасности России.
27. Внутренние факторы, влияющие на экономическую безопасность государства: экономические, организационные.
28. Внутренние факторы, влияющие на экономическую безопасность государства: правовые, социальные.
29. Внешние факторы, влияющие на экономическую безопасность государства.
30. Внутренние угрозы экономической безопасности России.
31. Основные внешние угрозы экономической безопасности России до 2030 года.
32. Показатели экономической безопасности государства: макроэкономические, частные социально-экономические, функционального и отраслевого уровня.
33. Оценка уровня экономической безопасности государства.
34. Перспективы повышения уровня экономической безопасности России.
35. Закономерности развития форм обеспечения экономической безопасности государства.
36. Индикаторы цифровой экономики

37. Россия в международных рейтингах.
38. Техническая защита информации.
39. Электронное государство.
40. .Обеспечение безопасности личности в информационном пространстве на современном этапе.
41. Угрозы информационной безопасности Российской Федерации (факторы, создающие опасность нанесения ущерба национальным интересам в информационной сфере).
42. Информационная безопасность Российской Федерации (состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз).
43. Законодательный уровень обеспечения информационной безопасности.
44. Обработка персональных данных, с помощью организационных и технических мер.
45. Тайна переписки и других сообщений, личная тайна, и забота о сохранении конфиденциальности.
46. Перечень сведений, составляющих государственную тайну.
47. Порядок засекречивания сведений и их носителей.
48. Особый порядок допуска к государственной тайне.
49. Отнесение информации к категории коммерческой тайны.
50. Ответственность за разглашение коммерческой тайны.
51. Сведения ограниченного доступа и открытая информация.
52. Регламент работы по определению сведений, составляющих коммерческую тайну.
53. Система и классификация тайн в российском
54. Криптографические методы защиты информации
55. Алгоритмы формирования и проверки электронной подписи
56. Средства защиты информации от несанкционированного доступа.
57. Средства межсетевого экранирования.
58. Средства обнаружения и предотвращения вторжений
59. Средства анализа и контроля защищенности информации
60. Комплексные средства защиты информации
61. Средства антивирусной защиты информации.
62. Специальные технические средства, предназначенные для негласного получения информации, применяемые в оперативно-разыскной деятельности органов внутренних дел.
63. Особенности использования специальных технических средств, ограничивающих конституционные права граждан при раскрытии и расследовании киберпреступлений.
64. Киберпреступления, преступления в сфере телекоммуникаций и компьютерной информации, совершаемые с использованием высоких технологий.
65. Методы борьбы с киберпреступлениями.

Заведующий кафедрой __ / Галяутдинова Л.Р.

Критерии оценивания экзамена:

| **Критерии** | **Баллы** |
|---|---|
| Знание не сформировано / Умение не сформировано / Навык не сформирован | 1-15 |
| Знание сформировано частично / Умение сформировано частично / Навык сформирован частично | 16-40 |
| Знание сформировано, но имеет несущественные недостатки / Умение сформировано, но имеет несущественные недостатки / | 41-50 |

| | |
|---|---|
| Навык сформирован, но имеет несущественные недостатки | |
| Знание сформировано полностью / Умение сформировано полностью / Навык сформирован полностью | 51-60 |

Оценка на экзамене выставляется с учетом баллов, выставленных обучающемуся по итогам текущего контроля – за ответы на семинарах: для этого баллы, полученные за ответы на семинарах и за ответ на вопросы экзамена суммируются и делятся.

Критерии оценивания:

| **Баллы** | **Оценка** |
|---|---|
| 1-36 | неудовлетворительно |
| 37-58 | удовлетворительно |
| 59-79 | хорошо |
| 80-100 | отлично |

КАЗАНСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
**«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»**
**Казанский филиал**

Дисциплина: **«Информационная безопасность в экономической деятельности»**

Экзамен

**БИЛЕТ №**

1. Критерии оценки уровня информационной безопасности государства.
2. Государственная тайна.
3. Используя алгоритмы двойной перестановки строк и столбцов выполнить дешифрование шифрограммы

| | | |
|---|---|---|
| В ОН, Т ОЭЗКНОА УОРСЗКНОА | КРУТО | СТУЖА |

В шифротексте следует обратить внимание на наличие пробелов в тексте, длина текста равняется 25 символам.

Зам.заведующего кафедрой _____/ Галяутдинова Л.Р. /