Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Иркутский государственный университет»
(ФГБОУ ВО «ИГУ»)

Юридический институт
Кафедра **Судебного права**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине **Основы информационной безопасности**
код **Б1.В.ДВ.3.2**
направление подготовки **40.03.01 «Юриспруденция»**
направленность (профиль) подготовки **уголовно-правовой, гражданско-правовой, государственно-правовой, международно-правовой, административно-финансово-правовой**
Год набора **(2014-2016 гг.)**

Иркутск
2017

Разработан в соответствии с ФГОС ВО, утвержденным Приказом Министерства образования и науки РФ от 1 декабря 2016 г. № 1511

Одобрен Учебно-методической комиссией Юридического института ИГУ «24» мая 2017 г.

Зам. председателя УМК Георгиевский Э.В.,
профессор, к. ю. н., доцент
ФИО, должность, ученая степень, звание

подпись, печать

Разработчик Смирнов В.А., доцент кафедры судебного права ЮИ ИГУ, канд.юрид.наук

подпись

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине **Основы информационной безопасности**
код – **Б1.В.ДВ.3.2,**
направление подготовки **40.03.01 «Юриспруденция»,**
направленность (профиль) подготовки **– уголовно-правовой, гражданско-правовой, государственно-правовой, международно-правовой, административно-финансово-правовой**
наименование УГС (укрупненная группа специальностей) – **40.03.01**

1. **Компетенции (дескрипторы компетенций), формируемые в процессе изучения дисциплины** (курс **1** семестр **1 (очное);** курс **1** сессия **1-2 (заочное),** курс **1** сессия **2 (заочное ИГУП СПО)**:

Индекс и Наименование компетенции (в соответствии с ФГОС ВО (ВПО)	**Признаки проявления компетенции/ дескриптора (ов) в соответствии с уровнем формирования в процессе освоения дисциплины**
ОК-3 – владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	**Базовый уровень**: знает понятие и сущность информации и информационной безопасности, осознает значимость обеспечения информационной безопасности, понимает необходимость осторожного применения и хранения информации, знает законодательство об информационной безопасности и охраняемых законом тайнах **Повышенный уровень:** владеет полным комплексом методов и способов получения, хранения и переработки информации с учетом требований информационной безопасности; умеет пользоваться основными информационно-защитными системами компьютера как средства управления информацией
ОК-4 – способность работать с информацией в глобальных компьютерных сетях	**Базовый уровень:** умеет работать с нормативно-правовыми актами по защите информации в правовой системе «Консультант плюс», «Гарант», имеет представление о системе ГАС «Правосудие» и ГАС «Выборы», имеет практические навыки по основам безопасного поиска необходимой информации в глобальной компьютерной сети Интернет, в том числе правовой. **Повышенный уровень:** знает ключевые методы безопасной работы с информацией в глобальных компьютерных сетях; умеет находить и использовать информацию в глобальных компьютерных сетях без ущерба для безопасности своего компьютера, а также компьютерной сети организации; владеет навыками воспрепятствования распространения вредоносной информации на своем компьютере, а также в компьютерной сети организации
ОПК-6 - способность повышать уровень своей профессиональной компетентности.	**Базовый уровень:** владеет системой знаний и представлений об особенностях своей профессиональной деятельности; умеет применять методы и средства познания для интеллектуального развития, повышения профессиональной компетентности, демонстрирует способность продолжать обучение и развитие в течение всей профессиональной карьеры; **Повышенный уровень:** знает достоинства и недостатки, а также сильные и слабые стороны своей профессиональной деятельности; готов и умеет извлекать уроки как из успешных проектов, так и из

	неудач; способен получать знания от коллег, из книг и материалов, а также путем самостоятельной исследовательской работы; владеет навыками планирования процесса развития профессионального мастерства и повышения уровня квалификации
ПК-7 – владеть навыками подготовки юридических документов.	**Базовый уровень:** знать стадии, методы и порядок подготовки основных юридических документов, с учетом требований информационной безопасности; уметь самостоятельно разрабатывать юридические документы, применяя при этом знания правил информационной безопасности; владеть навыками информационной защиты при подготовке юридических документов **Повышенный уровень:** способен к грамотному составлению на русском и/или иностранном языке документов, имеющих юридическое значение, таким образом, который исключает возникновение правового спора по его форме и реквизитам, а также по существу изложенного в документе, признание его недействительным либо ничтожным.

2. В результате освоения дисциплины обучающийся должен:

Знать: Предпосылки формирования сферы знаний по информационной безопасности; законодательную и нормативную базу ИБ; основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия; иметь полное представление о значение информационной безопасности для современного бизнеса, о перспективах развития технологий обеспечения информационной безопасности.

Уметь: Анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ. Использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры. Применять эти методы и ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ.

Владеть: Способностью применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации ИБ. Способностью разрабатывать концепцию, программу, политику информационной безопасности предприятия; организовывать и проводить аудит ИБ; использовать современные инструментальные средства анализа рисков и разработки политики ИБ. Навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.

Программа оценивания контролируемой компетенции:

Критерии 1 (К1): Оценка знаний студентов при проведении текущего контроля с использованием тестовых заданий

- Оценка «отлично» выставляется, если студент правильно решил от 80 до 100 % заданий;
- Оценка «хорошо» выставляется, если студент решил правильно от 60 до 80 % заданий;
- Оценка «удовлетворительно» выставляется, если студент решил правильно от 50 до 60 % заданий;
- Оценка «зачтено» выставляется, если студент ответил более чем на 50 % заданий.
- Оценка «неудовлетворительно» и «незачтено» выставляется, если студент ответил менее чем на 50 % заданий

Критерий 2 (К2): Оценка знаний студентов при проведении текущего контроля с использованием вопросов по темам и разделам курса.

1. Оценка «отлично» ставится студенту, ответ которого содержит:
- глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
- знание концептуально-понятийного аппарата;
- знание монографической литературы по разделам и темам курса,

а также свидетельствует о способности:
- самостоятельно критически оценивать основные положения соответствующих тем и разделов курса;
- увязывать теорию с практикой.

2. Оценка «хорошо» ставится студенту, ответ которого свидетельствует:
- о полном знании материала по программе;
- о знании рекомендованной литературы,
- а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

3. Оценка «удовлетворительно» ставится студенту, ответ которого содержит:
- поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии курса;
- стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

4. Оценка «не удовлетворительно» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

Критерий 3 (К3).: О**ценка знаний студентов при проведении промежуточного контроля с использованием вопросов для зачета**

1. Оценка «**зачтено**» на зачете ставится при соблюдении условий, изложенных в критерии 2 применительно к оценкам «отлично», «хорошо», «удовлетворительно».

2. Оценка «**не зачтено**»:

Оценка «**не зачтено**» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

Тема или раздел дисциплины[1]	Форм-мый признак комп-ции	Показатель	Критерий оцени-вания	Наименование ОС[2]	
				ТК[3]	ПА[4]
Тема 1. Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия.	ОК-3, ОК-4, ОПК-6, ПК-7	**Знать:** цели и задачи дисциплины «основы информационной безопасности», понимать значение категории «информация», важность ее правильной обработки и хранения **Уметь:** характеризовать современное состояние информационных технологий, информационной безопасности **Владеть:** понятийным аппаратом данной дисциплины, правильно употреблять категории «информация», «правовая информация», «информационная безопасность» и т.д.	Критерии 1-3	Вопросы по темам и разделам. Фонд тестовых заданий	**Вопросы к зачету**

Тема 2. Защищенная информационная система. Уровни и структура информационной безопасности.	ОК-3, ОК-4, ОПК-6, ПК-7	**Знать:** понятие и основные виды защищаемой информации, понятие защищенной информационной системы **Уметь:** разрабатывать ориентировочную программу информационной безопасности **Владеть:** навыками характеристики политики информационной безопасности, навыками составления организационно-распорядительных документов в сфере информационной безопасности	Критерии 1-3	Вопросы по темам и разделам. Фонд тестовых заданий	**Вопросы к зачету**
Тема 3. Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.	ОК-3, ОК-4, ОПК-6, ПК-7	**Знать:** понятие информационных рисков, их классификацию, понятие и содержание стандартов в сфере информационной безопасности. **Уметь:** характеризовать модели систем и процессов защиты информации **Владеть:** представлением об основных сервисах информационной безопасности и защиты информации	Критерии 1-3	Вопросы по темам и разделам. Фонд тестовых заданий	**Вопросы к зачету**
Тема 4. Технологии и методы реализации информационной безопасности. Комплексная защита информационной инфраструктуры	ОК-3, ОК-4, ОПК-6, ПК-7	**Знать:** основные элементы технологий защиты от атак, критерии оценки эффективности средств защиты информации **Уметь:** характеризовать отдельные методы информационной защиты **Владеть:** навыками составления запросов, отыскания нужной информации о способах и средствах защиты информации	Критерии 1-3	Вопросы по темам и разделам. Фонд тестовых заданий	**Вопросы к зачету**

[1] Раздел, тема дисциплины указываются в соответствии с рабочей программой дисциплины (модуля)

[2] ОС – оценочное средство

[3] ТК – текущий контроль

[4] ПА – промежуточная аттестация

Оценочные средства для проведения промежуточной аттестации:

Зачетно-экзаменационные материалы:

1. Вопросы для зачета:

1. Понятие информационных угроз.
2. Информационные войны.
3. Информационные угрозы безопасности РФ. Доктрина информационной безопасности РФ.
4. Виды противников. Хакеры.
5. Компьютерные вирусы. История. Определение по УК РФ.
6. Виды, принципы действия вирусов, демаскирующие признаки.
7. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
8. Угрозы ресурсам компьютерной безопасности. Угрозы, реализуемые на уровне локальной компьютерной системы. Человеческий фактор.
9. Угрозы компьютерной информации, реализуемые на аппаратном уровне.

10. Удаленные атаки на компьютерные системы. Причины уязвимостей компьютерных сетей.
11. Правовое урегулирование защиты информации.
12. Роль, задачи и обязанности администратора безопасности КС.
13. Защита данных криптографическими методами. Методы шифрования.
14. Защита данных криптографическими методами. Алгоритмы шифрования.
15. Требования к шифрам. Сравнение DES и ГОСТ 28147-89
16. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак.
17. Политика безопасности и ее составляющие.
18. Модели защиты информации в КС.
19. Технологии защиты и разграничения доступа.
20. Стандарты ИБ.

2. Билеты (вопросы) для экзамена:
Экзамен по дисциплине не предусмотрен

3. Критерии оценки на зачете:

Выставление оценок на зачете осуществляется на основе принципов объективности, справедливости, всестороннего анализа уровня знаний студентов.

При выставлении оценки преподаватель учитывает:

знание фактического материала по программе, в том числе; знание обязательной литературы, современных публикаций по программе курса, а также истории науки;

степень активности студента на семинарских занятиях;

логику, структуру, стиль ответа; культуру речи, манеру общения; готовность к дискуссии, аргументированность ответа; уровень самостоятельного мышления; умение приложить теорию к практике, решить задачи;

наличие пропусков семинарских и лекционных занятий по неуважительным причинам.

Оценка «зачтено»:

Оценка «зачтено» ставится на зачете студентам, уровень знаний которых соответствует требованиям, установленным в **Критерии 2 Программы оценивания контролируемой компетенции** применительно к п.п. «оценка удовлетворительно», «оценка хорошо», «оценка отлично».

Оценка «не зачтено»:

Оценки «не зачтено» ставятся студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

Оценочные средства для оценки остаточных знаний студентов, изучивших курс «Основы информационной безопасности»

Примерные тестовые задания на проверку остаточных знаний по дисциплине «Основы информационной безопасности»

Вариант 1

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....
    1. **информационная война**
    2. информационное оружие

3. информационное превосходство

2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.
    1. служебная информация
    2. коммерческая тайна
    3. банковская тайна
    4. **конфиденциальная информация**
3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
    1. **конфиденциальность**
    2. целостность
    3. доступность
    4. аутентичность
    5. аппелеруемость
4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
    1. **надежность**
    2. точность
    3. контролируемость
    4. устойчивость
    5. доступность
5. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
    1. принцип системности
    2. принцип комплексности
    3. принцип непрерывной защиты
    4. принцип разумной достаточности
    5. **принцип гибкости системы**
6. В классификацию вирусов по способу заражения входят
    1. опасные
    2. файловые
    3. **резидентные**
    4. загрузочные
    5. файлово-загрузочные
    6. **нерезидентные**
7. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...
    1. **комплексное обеспечение И Б**
    2. безопасность АС
    3. угроза И Б
    4. атака на АС
    5. политика безопасности
8. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:
    1. компаньон - вирусами
    2. **черви**
    3. паразитические
    4. студенческие
9. К видам системы обнаружения атак относятся :
    1. системы, обнаружения атаки на ОС

2. системы, обнаружения атаки на конкретные приложения
3. системы, обнаружения атаки на удаленных БД
4. **все варианты верны**

10. Автоматизированная система должна обеспечивать
    1. надежность
    2. **доступность**
    3. **целостность**
    4. контролируемость

Оценочные средства для оценки текущей успеваемости студентов

- **Характеристика ОС для обеспечения текущего контроля по дисциплине**

Тема/ Раздел	**Индекс и уровень формируемой компетенции или дескриптора**	**ОС**	**Содержание задания**
Тема 1. Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия	ОК-3, ОК-4, ОПК-6, ПК-7	Контрольные вопросы Фонд тестовых заданий	1. Предпосылки становления предметной области информационной безопасности. 2. Ключевые вопросы информационной безопасности. 3. Концепция информационной безопасности Российской Федерации. 4. Разработка корпоративной концепции информационной безопасности. 5. Правовые аспекты информационной безопасности. 6. Международное и российское законодательство в сфере информационной безопасности.
Тема 2. Защищенная информационная система. Уровни и структура информационной безопасности	ОК-3, ОК-4, ОПК-6, ПК-7	Контрольные вопросы Фонд тестовых заданий	1. Виды защищаемой информации. 2. Модель угроз и модель информационной безопасности. 3. Понятие защищенной информационной системы. 4. Программа информационной безопасности. 5. Организационно-распорядительные документы в сфере информационной безопасности. 6. Политика информационной безопасности.
Тема 3. Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности	ОК-3, ОК-4, ОПК-6, ПК-7	Контрольные вопросы Фонд тестовых заданий	1. Управление информационными рисками. 2. Стандартизация в сфере информационной безопасности. 3. Математические модели систем и процессов защиты информации. 4. Сервисы информационной безопасности и защита от инсайдеров
Тема 4. Технологии и методы реализации информационной безопасности. Комплексная защита информационной инфраструктуры.	ОК-3, ОК-4, ОПК-6, ПК-7	Контрольные вопросы Фонд тестовых заданий	1. Криптографические методы защиты информации. 2. Защита информационной инфраструктуры от атак. 3. Антивирусные средства защиты. 4. Комплексная защита информационной инфраструктуры и ресурсов. 5. Оценка эффективности СЗИ

Критерии оценки знаний студентов при проведении текущего контроля с использованием тестовых заданий

Оценка «отлично» выставляется, если студент правильно решил от 80 до 100 % заданий;
Оценка «хорошо» выставляется, если студент решил правильно от 60 до 80 % заданий;
Оценка «удовлетворительно» выставляется, если студент решил правильно ль 50 до 60 % заданий;
Оценка «неудовлетворительно» и «незачтено» выставляется, если студент ответил менее, чем на 50 % заданий;
Оценка «зачтено» выставляется, если студент ответил более чем на 50 % заданий.

Критерии оценки знаний студентов при проведении текущего контроля с использованием вопросов по темам и разделам курса, а также при собеседовании по дискуссионным вопросам.

1. Оценка «отлично» ставится студенту, ответ которого содержит:
   - глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
   - знание концептуально-понятийного аппарата;
   - знание монографической литературы по разделам и темам курса,

а также свидетельствует о способности:
   - самостоятельно критически оценивать основные положения соответствующих тем и разделов курса;
   - увязывать теорию с практикой.

2. Оценка «хорошо» ставится студенту, ответ которого свидетельствует:
   - о полном знании материала по программе;
   - о знании рекомендованной литературы,
   - а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

3. Оценка «удовлетворительно» ставится студенту, ответ которого содержит:
   - поверхностные знания важнейших разделов программы и содержания лекционного курса;
   - затруднения с использованием научно-понятийного аппарата и терминологии курса;
   - стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

4. Оценка «не удовлетворительно» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала

- **Оценочные средства, обеспечивающие диагностику сформированности компетенций, заявленных в рабочей программе дисциплины (модуля)**

Результат диагностики сформированности компетенций	**Показатели**	**Критерии**	**Соответствие / несоответствие**	**Зачет**
Компетенции сформированы полностью	Владеет информацией о понятии, видах, назначении информационной безопасности, знает особенности функционирования основных средств информационной защиты. Может	Определение назначения, целей, задач и особенностей информационной безопасности, средств и методов защиты. Уяснение основ работы со	Понимание назначение информационной безопасности. Способность поиска необходимой информации о средствах и методах	Зачтено / не зачетно

	охарактеризовать особенности концепции информационной безопасности, политики информационной безопасности. Имеет навыки работы с системами информационной защиты	средствами защиты	информационной защиты, умение работать с простейшими средствами информационной защиты / отсутствие системных навыков работы с инструментами информационной защиты, неспособность быстрого отыскания нужных данных и правильного применения средств информационной защиты	