МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И ИННОВАЦИЙ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Межгосударственная образовательная организация высшего образования Кыргызско-Российский Славянский университет имени первого Президента Российской Федерации Б.Н. Ельцина.

Фонд оценочных средств

по дисциплине:

Правовые основы информационной безопасности

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

40.03.01 – РФ; 530500 – КР

(код и наименование направления подготовки)

Квалификация
бакалавр

Бишкек 2025 г.

Фонд оценочных средств предназначен для контроля знаний, обучающихся по направлению подготовки «Юриспруденция» 40.03.01. РФ; 530500 КР по дисциплине

Правовые основы информационной безопасности

Фонд оценочных средств рассмотрен и утвержден на заседании кафедры Уголовного права и процесса

протокол №10 от 19. 06. 2025 г.

Заведующий кафедрой профессор,

д.ю.н. Сулайманова Н.Н. 

Руководитель образовательной программы
и.о. декана юридического факультета,
к.ю.н., доцент Голобородько И.Л. 

Исполнители:

к.ю.н., доцент Смаилова А.А. 

КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-1: Способность осуществлять профессиональную деятельность на основе развитого правосознания, правового мышления и правовой культуры.

Знать:

Уровень 1 место и роль информационной безопасности в системе национальной безопасности Кыргызской Республики, основы государственной информационной политики, стратегию развития информационного общества в Кыргызской Республике;

Уровень 2 основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ГКНБ в области защиты информации;

Уровень 3 знать положения должностных инструкций основных направлений профессиональной деятельности органов национальной безопасности в Кыргызской Республике.

Уметь:

Уровень 1 обосновывать и принимать в пределах должностных полномочий решения, совершать действия, связанные с реализацией правовых норм;

Уровень 2 осуществлять правовую пропаганду и правовое воспитание в сфере обеспечения информационной безопасности;

Уровень 3 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации

Владеть:

Уровень 1 навыками сбора обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности;

Уровень 2 современными методами обеспечения защиты информации;

Уровень 3 навыками работы с информационными технологиями средством управления информацией.

В результате освоения дисциплины обучающийся должен

Знать:

-основные закономерности создания и функционирования информационных процессов в правовой сфере;

- основные положения в области информационной безопасности;

- меры борьбы с преступностью в информационной сфере, методы криминологического прогнозирования ее развития и планирования мер борьбы с ней.

Уметь:

-работать с нормативно-правовыми актами, осуществлять анализ, поиск информации по вопросам обеспечения информационной безопасности;

- применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа

-применять нормы гражданского, уголовного и других отраслей права для решения конфликтных ситуаций в сфере обеспечения информационной безопасности.

Владеть:

- навыками анализа и интерпретации информации, содержащейся в различных источниках;

- навыками осуществления правового воспитания в сфере обеспечения информационной безопасности;

навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности.

Методические указания для обучающихся по освоению дисциплины (модуля)

Модульный контроль по дисциплине включает:

1. Текущий контроль: усвоение учебного материала на аудиторных занятиях (лекциях, практических, лабораторных работах, в том числе учитывается посещение и активность) и выполнение обязательных заданий для самостоятельной работы.
2. Рубежный контроль: проверка полноты знаний и умений по материалу модуля в целом. Выполнение модульных контрольных заданий проводится в письменном виде и является обязательной компонентой модульного контроля.
3. Промежуточный контроль - завершенная задокументированная часть учебной дисциплины - совокупность тесно связанных между собой зачетных модулей.

Основные требования к промежуточному контролю.

При явке на зачет студенты обязаны иметь при себе зачетные книжки, которые они предъявляют экзаменатору в начале зачета. Преподавателю предоставляется право поставить зачет без опроса по билету тем студентам, которые набрали более 60 баллов за текущий и рубежный контроли.

На промежуточном контроле студент должен верно ответить на теоретические вопросы билета и решить ситуационную задачу.

Основные требования к текущему контролю:

Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня.
2. При подготовке к следующей лекции, нужно просмотреть текст предыдущего материала, подумать о том, какая может быть тема следующей лекции.
3. В течение недели выбрать время для работы с рекомендуемой литературой.
4. При подготовке к семинарским занятиям следующего дня, необходимо сначала прочитать основные понятия и подходы по теме домашнего задания. При выполнении задания нужно сначала понять, что в нем требуется, какой теоретический материал нужно использовать, наметить план решения.
5. Для подготовки к семинарским занятиям и выполнению самостоятельной работы необходимо сначала прочитать основные понятия и подходы по теме задания. Рекомендуется использовать методические указания по курсу, глоссарий, конспекты лекций, тезисы. При выполнении задания нужно сначала понять, что требуется в нем, какой теоретический материал нужно использовать, наметить план выполнения, а затем приступить.
6. Отработки пропущенных занятий.

Контроль над усвоением студентами материала учебной осуществляется систематически преподавателем кафедры. Отработка семинарских занятий и программы дисциплины отражается в журнале.

Каждое занятие, пропущенное студентом по уважительной причине, должно быть отработано. Отработки проводятся по расписанию кафедры, согласованному с деканатом.

Методические рекомендации по решению тестовых заданий

Тестовая система предусматривает вопросы/задания, на которые обучающийся должен дать один или несколько вариантов правильного ответа из предложенного списка ответов. При поиске ответа необходимо проявлять внимательность.

Ответы правильные выделяются в тесте подчеркиванием или любым другим допустимым символом. При самостоятельной подготовке к тестированию студенту необходимо:

а) готовясь к тестированию, проработайте информационный материал по дисциплине. Проконсультируйтесь с преподавателем по вопросу выбора учебной литературы;

б) четко выясните все условия тестирования заранее. Вы должны знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные. На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;
г) в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.
д) если Вы встретили чрезвычайно трудный для вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.
е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.
Тестирование - позволяет оценить знание фактического материала, умение логически мыслить, способность к рефлексии и творчески подходить к решению поставленной задачи.

Методические указания по подготовке докладов

Самостоятельную работу над темой доклада следует начать с изучения литературы. В поисках книг заданной тематики необходимо обратиться к библиотечным каталогам, справочникам, тематическим аннотированным указателям литературы, периодическим изданиям (газетам и журналам), электронным каталогам, Интернету. При подготовке текста доклада студент должен отобрать не менее 10 наименований печатных изданий (книг, статей, сборников). Предпочтение следует отдавать литературе, опубликованной в течение последних 5 лет. Допускается обращение к Интернет-сайтам.

Осуществив отбор необходимой литературы, студенту необходимо составить рабочий план доклада или сообщения. В соответствии с составленным планом производится изучение литературы и распределение материала по разделам доклада. Необходимо отмечать основные, представляющие наибольший интерес положения изучаемого источника. Изложение текста доклада должно быть четким, аргументированным. Не стоит увлекаться сложной терминологией, особенно если студент сам не совсем свободно ею владеет. Уяснить значение терминов можно в справочно- энциклопедических изданиях, словарях. Изучая литературу, студент неизбежно столкнется с научной полемикой разных авторов, с различными подходами в рассмотрении вопросов. Следует учитывать все многообразие точек зрения, а в случае выбора какой-либо одной из них - обосновывать, аргументировать свою позицию. При необходимости изложение своих взглядов на проблемы можно подтвердить цитатами. В заключение доклада студент должен сделать выводы по теме.

Продолжительность доклада не более 7 минут. Для получения положительной оценки наличие компьютерной презентации обязательно.
Объем доклада не более 15 страниц. Шрифт Times New Roman-14. Межстрочный интервал-1,5

Примерная тематика докладов для контрольного мероприятия №1:

1. Понятие безопасности и её составляющие. Безопасность информации.
2. Обеспечение информационной безопасности: содержание и структура понятия.
3. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
4. Система обеспечения информационной безопасности.
5. Понятие информационной войны. Проблемы информационной войны.
6. Информационное оружие и его классификация.
7. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
8. Виды защищаемой информации в сфере государственного и муниципального управления.
9. Обеспечение информационной безопасности в различных сферах общественной жизни.
10. Преступления в сфере компьютерной информации.
11. Правовое регулирование отношений, связанных с режимом коммерческой тайны.
12. Институт правовой защиты служебной тайны.
13. Институт правовой защиты банковской тайны.
14. Допуск к государственной тайне.
15. Виды защищаемой информации в сфере государственного и муниципального управления.
16. Обеспечение информационной безопасности в различных сферах общественной жизни.
17. Преступления в сфере компьютерной информации.
18. Правовое регулирование отношений, связанных с режимом коммерческой тайны.
19. Институт правовой защиты служебной тайны.
20. Институт правовой защиты банковской тайны.
21. Допуск к государственной тайне.
22. Организация подготовки и проведения конфиденциальных переговоров.
23. Виды защищаемой информации.
24. Угрозы утечки информации и угрозы несанкционированного доступа.
25. Информационная безопасность критически важных объектов.
26. Персональные данные как особый институт охраны прав на неприкосновенность частной жизни.
27. Правовое обеспечение информационной безопасности в сфере Интернета.
28. Организация подготовки и проведения конфиденциальных переговоров

Шкала оценивания доклада (25 баллов)

	Критерии оценивания	баллы
	Новизна текста (актуальность темы исследования; новизна и самостоятельность в постановке проблемы, формулирование нового аспекта известной проблемы в установлении новых связей (межпредметных, внутрипредметных, интеграционных); умение работать с исследованиями, критической литературой, систематизировать и структурировать материал; самостоятельность оценок и суждений)	**0-5**
	Степень раскрытия сущности вопроса (соответствие плана теме доклада; соответствие содержания теме и плану доклада; полнота и глубина знаний по теме; умение обобщать, делать выводы, сопоставлять различные точки зрения по одному проблеме)	**0-15**
	Соблюдение требований к оформлению (насколько верно оформлены ссылки на используемую литературу, список литературы; оценка грамотности и культуры изложения, в т.ч. орфографической, пунктуационной, стилистической культуры, владение терминологией; соблюдение требований к объему вклада)	**0-5**
Сумма баллов		**0-25**

Тестовые задания для контрольного мероприятия №2:

1.Главными целями деятельности по обеспечению ИБ являются:
А. Ликвидация угроз объектам информационной безопасности
Б. Минимизация возможного ущерба
В. Исполнение законодательства в области ИБ
Г.Минимизация производственных издержек
Д. Повышение культуры производства

2.Негативные воздействия на объекты ИБ различают:
А. По степени изменения свойств объекта безопасности
Б. По возможности ликвидации последствий проявления угрозы
В. По величине затрат на предотвращение негативного воздействия

3. Укажите свойства угроз:
А.Избирательность
Б. Массовость
В.Стохастичность
Г.Предсказуемость
Д. Вредоносность

4.Выберите верное утверждение(я): Опасность …
А. Это совокупность факторов и условий, возникающих в процессе взаимодействия различных объектов (их элементов) и способных оказывать негативное воздействие на конкретный объект информационной безопасности.
Б. Это состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту.
В. Свойство объекта взаимодействия или находящихся во взаимодействии элементов объекта безопасности, выступающих в качестве источника угроз
Г. Является свойством объекта информационной безопасности и характеризует его способность противостоять проявлению угроз.

5. ИБ направлена на обеспечение:
А. Целостности данных
Б. Репрезентативности данных
В. Адекватности данных
Г. Конфиденциальности данных
Д. Достоверности данных
Е. Доступности данных

6.Укажите виды классификаций угроз ИБ:
А.По источнику (его местонахождению)
Б. По вероятности реализации
В. По вероятности избежания угрозы ИБ
Г. По размерам наносимого ущерба
Д. По природе происхождения
Е. По природе средств защиты
Ж.По предпосылкам возникновения
З. По видам объектов безопасности

7. К прямому ущербу ИБ относится:
А. Потери из-за реализации «стартапа» компании конкурентами
Б. Затраты на закупку сканеров отпечатков пальцев для доступа к рабочему месту
В. Замедление бизнес-процессов в виду запрета доступа некоторым категориям сотрудников к документам данного бизнес-процесса и, как следствие, возросшая нагрузка на сотрудников и увеличение фонда оплаты труда
Г. Использование конкурентами корпоративного механизма доступа к данным
Д. Проигрыш заявки на гос. закупку в виду утечки сведений по данной заявке

8.Цели информационной безопасности – своевременное обнаружение, предупреждение:
А. Несанкционированного доступа, воздействия в сети
Б. Инсайдерства в организации
В. Чрезвычайных ситуаций

9.Основными рисками информационной безопасности являются:
А. Искажение, уменьшение объема, перекодировка информации
Б. Техническое вмешательство, выведение из строя оборудования сети В. Потеря, искажение, утечка информации

10.Основными субъектами информационной безопасности являются:
А. Руководители, менеджеры, администраторы компаний
Б. Органы права, государства, бизнеса
В. Сетевые базы данных

11.Утечкой информации в системе называется ситуация, характеризуемая:
А. Потерей данных в системе
Б. Изменением формы информации
В. Изменением содержания информации

12.Основными объектами защиты при обеспечении информационной безопасности являются:
А. Все виды информационных ресурсов;
Б. Права граждан, юридических лиц и государства на получение, распространение и использование информации;
В. Информационные системы и технологии;
Г. Операторы распространители, обладатели информации

13.К служебной тайне не относится:
А. Профессиональная тайна
Б. Тайна деятельности соответствующего органа
В. Вред, причиненный здоровью работника в связи с производственной травмой

14.Засекречиванию подлежат сведения о …
А. Состоянии преступности
Б. Фактах нарушения прав и свобод человека и гражданина
В. Силах и средствах гражданской обороны

15.С точки зрения информационного права информация – это …
А. Сведения независимо от формы их представления
Б. Сведения о законодательстве, правовых явлениях, правоприменительной деятельности
В. Данные о развитии конкретной правовой науки и ее практическом применении

16.Какие степени секретности и грифы секретности носителей сведений, установлены законодательством КР. Отметьте правильный вариант:
А. Для служебного пользования
Б. Совершенно секретно
В. Конфиденциально
Г. Особой важности
Д. Строго конфиденциально

Е. Секретно

17.Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:
А. О безопасности пищевых продуктов
Б. Об использовании новых технологий, позволяющих получить коммерческую выгоду
В. Об использовании безвозмездного труда граждан в деятельности некоммерческой организации

18.Засекречивание информации это -…
А. Совокупность мероприятий, установленных государством по ограничению распространения информации
Б. Установленный нормативными правовыми актами Кыргызской Республики единый порядок обеспечения сохранности государственных секретов, включающий в себя систему административно-правовых, организационных, инженерно-технических, криптографических и иных мер
В. Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственные секреты, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов

19.Разглашение секретной информации это…
А. Противоправные умышленные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по службе или работе, выразившиеся в сообщении, передаче, представлении, пересылке, опубликовании или доведении иным способом секретной информации до лиц, не допущенных к ней
Б. Выход, в том числе временный, сведений, составляющих государственные секреты, из законного владения или пользования в результате нарушения установленных правил обращения с ними, утери либо хищения, вследствие чего эти сведения стали или могли стать достоянием посторонних лиц
В. Совокупность мероприятий, установленных государством по снятию ограничений на распространение информации

20.Сведения, не подлежащие засекречиванию:
А. О положении дел в экологии, использовании природных ресурсов, здравоохранении, санитарии, культуре, сельском хозяйстве, образовании, торговле и обеспечении правопорядка
Б. Составляющие военную тайну
В. Составляющие государственную тайну

Шкала оценивания тестирования (20 баллов)

Оценка в баллах	**выполнения**	**Оценка по традиционной системе**

20-17	90-100	Отлично
16-11	75-89	Хорошо
10-8	50-74	Удовлетворительно
0-7	0-49	Неудовлетворительно
Количество вопросов		20
Всего		Сумма баллов

Технологическая карта

Дисциплина: Правовые основы информационной безопасности
Направление/профиль: Юриспруденция
Курс/семестр: 4 курс, 8 семестр
Количество кредитов (ЗЕ): 2
Отчетность: Зачетно-экзаменационная ведомость (зачет с оценкой)
Преподаватель: к.ю.н., доцент Смаилова А.А.

Название модулей дисциплины	**Контроль**	**Форма контроля**	**Зачетный минимум**	**Зачетный максимум**	**График контроля**
Модуль 1					
Правовое регулирование отношений в области информационной безопасности	Текущий контроль	Активность, посещаемость	10	12	26
Рубежный контроль	Доклад	10	25		
Модуль 2					
Защита информационной безопасности	Текущий контроль	Активность, посещаемость	10	13	29
Рубежный контроль	Тест	10	20		
ВСЕГО за семестр			**40**	**70**	
Промежуточный контроль			**20**	**30**	
Семестровый рейтинг по дисциплине			**60**	**100**	