

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Юридический институт

УТВЕРЖДЕНО:
Директор
О.И. Андреева

Оценочные материалы по дисциплине

Правовое обеспечение информационной безопасности

по специальности

40.05.01 Правовое обеспечение национальной безопасности

специализация:
Уголовно-правовая

Форма обучения
Заочная

Квалификация
Юрист

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
О.И. Андреева

Председатель УМК
Н.В. Багрова

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-9 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ПК-4 Способен соблюдать в профессиональной деятельности требования в области защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 9.1 Определяет задачи для поиска информации, необходимые источники информации

ИОПК 9.2 Осуществляет поиск, анализ и интерпретации информации необходимой для выполнения задач профессиональной деятельности

ИОПК 9.3 Планирует, структурирует информацию, выделяет значимое в информации, оценивает практическую значимость результатов поисков, оформляет результаты поиска

ИПК 4.1 Знает общие требования нормативных правовых актов в области защиты информации, основные способы соблюдения и обеспечения защиты информации; основные понятия, используемые при работе с персональными данными; ответственность за нарушение законодательства России в области защиты информации; базовые положения права интеллектуальной собственности

ИПК 4.2 Соблюдает в профессиональной деятельности основные требования нормативных правовых актов в области защиты информационной безопасности; обращения с документами, содержащими персональные данные

ИПК 4.3 Применяет в профессиональной деятельности требования нормативных правовых актов в области защиты информации; знания системы законодательства в области информационной безопасности; базовыми навыками правовой защиты информационных систем

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- тесты;
- контрольная работа;
- аналитический обзор;

Пример

Тест (ИПК-4.1, 4.2,4.3)

- 1) Объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы – это:
 - а) угроза информационной безопасности
 - б) угроза национальной безопасности
 - в) национальные интересы в военной сфере
 - г) национальные интересы в информационной сфере
- 2) информационная безопасность Российской Федерации – это:
 - а) осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

б) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

в) состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий;

г) состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны;

Ключи: 1 г), 2 б).

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно как минимум на 80% вопросов.

Контрольная работа (ИОПК 9.1, 9.2, 9.3 ИПК-4.2)

Контрольная работа состоит из 2 теоретических вопросов и 1 задачи.

Перечень теоретических вопросов:

Понятие информационной безопасности, основные задачи и методы ее обеспечения.

Национальные интересы РФ в информационной сфере и их обеспечение.

Угрозы информационной безопасности.

Государственная политика в сфере информационной безопасности.

Понятие информационной безопасности личности.

Информационно-психологическая безопасность личности.

Информационно-идеологическая безопасность личности.

Понятие информационной безопасности общества.

Угрозы информационной безопасности общества.

Понятие информационной безопасности государства. Угрозы информационной безопасности государства.

Понятие и предмет обеспечения информационной безопасности (ОИБ).

Организационные меры по обеспечению информационной безопасности на уровне международного сотрудничества, на уровне РФ, на уровне организации.

Объекты правового регулирования ОИБ.

Уровни правового регулирования ОИБ.

Понятие и характеристика информационной инфраструктуры. Ее элементы.

Понятие критической информационной инфраструктуры.

Объекты КИИ.

Категорирование объектов КИИ.

Требования к обеспечению безопасности КИИ.

Источники права в сфере обеспечения информационной безопасности.

Правовые режимы информации

Правовые средства обеспечения режимов информации

Роль локальных нормативных актов в обеспечении правового режима информации

Виды информации ограниченного доступа.

Конфиденциальная информация

Режим коммерческой тайны

Режим служебной тайны

Государственная тайна: понятие, режим, порядок засекречивания/рассекречивания
Понятие и виды информационных систем.

Требования к обеспечению безопасности информационных систем.

Особенности обеспечения информационной безопасности ГАС, ГИС и др. систем.

Общая характеристика и виды ответственности за правонарушения в
информационной сфере.

Дисциплинарная ответственность в информационной сфере.

Административная ответственность в информационной сфере.

Уголовная ответственность в информационной сфере.

Материальная ответственность в информационной сфере.

Примеры задач:

Задача 1

Организация эксплуатирует АСУ технологическим процессом выработки тепла, обеспечивающим теплом население ПГТ (более 75 000 человек). Относится ли АСУ к объектам КИИ?

Задача 2

Субъект КИИ провел процедуру категорирования объекта КИИ и присвоил 3 категорию значимости. Далее приступил к реализации мер по обеспечению информационной безопасности в соответствии с требованиями, установленными для объектов 3 категории. При проведении проверки установлено, что сведения о присвоении объекту категории значимости во ФСТЭК не подавались. К какой ответственности следует привлечь субъекта?

Ответы:

Задача 1. Да

Задача 2. К административной, по ст. 19.7.15 КоАП РФ.

Критерии оценивания:

Результаты контрольной работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если даны правильные ответы на все теоретические вопросы и все задачи решены без ошибок с обоснованием ответа.

Оценка «хорошо» выставляется, если ответы на теоретические вопросы содержат незначительные неточности, ответы на задачи верные, но без обоснования или с незначительными неточностями в обосновании.

Оценка «удовлетворительно» выставляется, если в ответах допущены ошибки, несоответствия законодательству, задачи решены, но с ошибками.

Оценка «неудовлетворительно» выставляется при несоответствии ответа законодательству или неверно решенной задаче.

Аналитический обзор . (ИПК 9.3, ИПК 4.2, 4.3)

(примерное задание): Сделайте аналитический обзор судебной практики (не менее 30 дел) по привлечению к ответственности за нарушение требований информационной безопасности. Проанализируйте собранные решения и составьте рекомендации по соблюдению требований законодательства в сфере информационной безопасности.

Критерии оценивания:

Результаты контрольной работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если анализ проведен корректно, дела подобраны в соответствии с заданием, в рекомендациях сформулированы практически применимые выводы, обеспечивающие соблюдение законодательства.

Оценка «хорошо» выставляется, если анализ практики проведен корректно, но в рекомендациях выводы судебной практики учтены фрагментарно.

Оценка «удовлетворительно» выставляется, если в работе проанализировано недостаточное количество дел и/или в рекомендациях допущены ошибки.

Оценка «неудовлетворительно» выставляется, если проанализированы дела, не соответствующие критериям задания или в рекомендациях допущены тезисы, не соответствующие законодательству, либо недостаточное количество дел проанализировано.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Зачет заданию. Билет содержит теоретический вопрос. Продолжительность зачета 1,5 часа.

Понятие информационной безопасности, основные задачи и методы ее обеспечения.

Национальные интересы РФ в информационной сфере и их обеспечение.

Угрозы информационной безопасности.

Государственная политика в сфере информационной безопасности.

Понятие информационной безопасности личности.

Информационно-психологическая безопасность личности.

Информационно-идеологическая безопасность личности.

Понятие информационной безопасности общества.

Угрозы информационной безопасности общества.

Понятие информационной безопасности государства. Угрозы информационной безопасности государства.

Понятие и предмет обеспечения информационной безопасности (ОИБ).

Организационные меры по обеспечению информационной безопасности на уровне международного сотрудничества, на уровне РФ, на уровне организации.

Объекты правового регулирования ОИБ.

Уровни правового регулирования ОИБ.

Понятие и характеристика информационной инфраструктуры. Ее элементы.

Понятие критической информационной инфраструктуры.

Объекты КИИ.

Категорирование объектов КИИ.

Требования к обеспечению безопасности КИИ.

Источники права в сфере обеспечения информационной безопасности.

Правовые режимы информации

Правовые средства обеспечения режимов информации

Роль локальных нормативных актов в обеспечении правового режима информации

Виды информации ограниченного доступа.

Конфиденциальная информация

Режим коммерческой тайны

Режим служебной тайны

Государственная тайна: понятие, режим, порядок засекречивания/рассекречивания

Понятие и виды информационных систем.

Требования к обеспечению безопасности информационных систем.

Особенности обеспечения информационной безопасности ГАС, ГИС и др. систем.

Общая характеристика и виды ответственности за правонарушения в информационной сфере.

Дисциплинарная ответственность в информационной сфере.

Административная ответственность в информационной сфере.

Уголовная ответственность в информационной сфере.

Материальная ответственность в информационной сфере.

Особенности ответственности в области массовой информации. Особенности ответственности в сети «Интернет».

Практические задания (примерные)

Составьте пакет документов, необходимый для обеспечения информационной безопасности объекта КИИ (вид объекта определяется преподавателем).

Составьте пакет документов, обеспечивающих правовой режим конфиденциальной информации в организации (вид конфиденциальной информации определяется преподавателем).

Результаты зачета определяются оценками «зачтено», «не зачтено». Оценка «зачтено» ставится в случае, если обучающийся грамотно, последовательно и логично излагает учебный материал, способен правильно применять законодательство в соответствии с конкретными обстоятельствами, по составленному пакету документов поясняет, почему в нем содержатся те или иные положения и как их следует применять. Оценка «не зачтено» ставится в случае, если обучающийся допускает ошибки при изложении материала, испытывает трудности в оценке фактических обстоятельств и применении права, составлении документов.

Собеседование по вопросам и выполнению заданий по составлению пакетов документов позволяют оценить достижение следующих индикаторов: ИОПК-9.1. ИОПК-9.2. ИОПК-9.3. ИПК-4.2. ИПК-4.3.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Тест

1. Что из перечисленного не является видом мер по обеспечению информационной безопасности: (ИОПК 9.1)

- а) организационные
- б) технические
- в) информационные
- г) правовые

2. Что из перечисленного не является объектом информационной инфраструктуры (ИОПК 9.2):

- а) автоматизированная система управления
- б) сеть электросвязи
- в) многофункциональный центр
- г) информационно-телекоммуникационная сеть

3. Целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации – это (ИПК 4.2)

- А) компьютерный инцидент
- Б) компьютерная атака
- В) телекоммуникационная атака

Г) сетевая авария

4. факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки – это: (ИПК 4.1)

- А) компьютерный инцидент
- Б) компьютерная атака
- В) телекоммуникационная атака
- Г) сетевая авария

5. По какому из данных объектов требуется проводить категорирование? (ИПК 4.3)

- а) бетономешалка
- б) АСУ банка
- в) база данных клиентов магазина (ок. 200 клиентов)
- г) локальная компьютерная сеть из 10 компьютеров

6. К средствам обеспечения информационной безопасности относятся: (ИОПК 9.3)

А) технические средства, используемые силами обеспечения информационной безопасности;

Б) правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

В) организационные средства, используемые силами информационной безопасности

Г) правовые средства, используемые средствами обеспечения информационной безопасности

7. Какой из документов необходимо оформить субъекту критической информационной инфраструктуры для исполнения обязанностей по информационной безопасности: (ИПК 4.1)

- А) Устав
- Б) Приказ о назначении начальника службы безопасности
- В) Положение о защите персональных данных
- Г) Сведения о категорировании объектов КИИ

8. Категорирование объектов КИИ осуществляется без учета: (ИПК 4.2)

а) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

б) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

в) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

г) значимости объекта критической информационной инфраструктуры для организации досуговых мероприятий и рекреационных целей.

Ключи: 1 в), 2 в), 3б); 4 а); 5 б); 6 б); 7 в); 8 б).

Информация о разработчиках

Мельникова Валентина Григорьевна, к.ю.н., доцент, доцент кафедры природоресурсного, земельного и экологического права ЮИ ТГУ