

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Институт гражданской защиты
Кафедра Прокурорско-следственной деятельности



УТВЕРЖДАЮ

Директор Института гражданской защиты
Малкин В.Ю.

«25» 02 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
Правовое обеспечение информационной безопасности

40.05.01 Правовое обеспечение национальной безопасности
Государственно-правовая

Разработчик (разработчики):

доцент кафедры _____ Машуков Р.А.

старший преподаватель кафедры _____ Хамутовская Ю.П.

ФОС рассмотрен и одобрен на заседании кафедры прокурорско-
следственной деятельности
от «25» 02. 2025 г., протокол № 6

Заведующий кафедрой _____ Машуков Р.А.

Луганск 2025 г.

**Комплект оценочных материалов по дисциплине
«Правовое обеспечение информационной безопасности»**

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

Выберите один правильный ответ.

1. Какой закон регулирует вопросы информационной безопасности в России?
А) Закон о персональных данных;
Б) Закон о защите информации;
В) Закон об информации, информационных технологиях и о защите информации.
Правильный ответ: В
Компетенции (индикаторы): ОПК-9
2. Какой из перечисленных актов является основным международным документом в области кибербезопасности?
А) Декларация прав человека;
Б) Конвенция о киберпреступности;
В) Хартия ООН.
Правильный ответ: Б
Компетенции (индикаторы): ОПК-9
3. Какое из перечисленных понятий относится к информационной безопасности?
А) Конфиденциальность информации;
Б) Легальность данных;
В) Глобализация интернета.
Правильный ответ: А
Компетенции (индикаторы): ОПК-9
4. Какой из следующих принципов не является частью правового обеспечения информационной безопасности?
А) Законность;
Б) Справедливость;
В) Принцип экономии ресурсов.
Правильный ответ: В
Компетенции (индикаторы): ОПК-9
5. Какой из перечисленных органов отвечает за координацию деятельности в области кибербезопасности в России?
А) ФСБ России;
Б) Министерство связи и массовых коммуникаций;

В) Роскомнадзор.

Правильный ответ: А

Компетенции (индикаторы): ОПК-9

Задания закрытого типа на установление соответствия

Установите правильное соответствие.

Каждому элементу левого столбца соответствует только один элемент правого столбца.

1. Установите соответствие между понятием и его определением.

Понятие		Определение	
1) Информационная безопасность	А)	способность информации сохранять свою ценность и быть доступной только для авторизованных пользователей	
2) Конфиденциальность	Б)	гарантированное отсутствие несанкционированных изменений информации	
3) Целостность	В)	обеспечение постоянного и безопасного доступа к информации для уполномоченных пользователей	
4) Доступность	Г)	мера, направленная на защиту информации от несанкционированного доступа и воздействия	

Правильный ответ:

1	2	3	4
Г	А	Б	В

Компетенции (индикаторы): ОПК-9

2. Установите соответствие между понятием и его определением.

Понятие		Определение	
1) Киберугроза	А)	мошенническая практика получения конфиденциальной информации через поддельные сайты или электронные письма	
2) Фишинг	Б)	действия, направленные на подрыв информационной среды страны через использование компьютерных технологий	

- 3) Вредоносное ПО В) совокупность методов и средств, направленных на сохранение и защиту данных от угроз
- 4) Защита информации Г) программа, разработанная с целью причинения вреда пользователям и их данным

Правильный ответ:

1	2	3	4
Б	А	Г	В

Компетенции (индикаторы): ОПК-9

3. Установите соответствие между понятием и его обозначением.

- | Понятие | Определение |
|----------------------------|---|
| 1) Аутентификация | А) преобразование информации в неразборчивый вид для обеспечения её конфиденциальности |
| 2) Шифрование | Б) меры, направленные на защиту оборудования и информационных систем от физического доступа и повреждений |
| 3) Логическая безопасность | В) процесс проверки подлинности пользователя или системы |
| 4) Физическая безопасность | Г) безопасность, обеспечиваемая средствами программного обеспечения и операционной системы |

Правильный ответ:

1	2	3	4
В	А	Г	Б

Компетенции (индикаторы): ОПК-9

Задания закрытого типа на установление правильной последовательности

Установите правильную последовательность.

Запишите правильную последовательность букв слева направо.

1. Установите правильную последовательность этапов оценки рисков в информационной безопасности:

- А) Выявление уязвимостей
- Б) Определение ценности информации
- В) Анализ потенциальных угроз
- Г) Оценка вероятности и последствий инцидентов

Правильный ответ: Б, В, А, Г

Компетенции (индикаторы): ОПК-9

2. Установите правильную последовательность действий при инциденте информационной безопасности:

- А) Уведомление ответственных лиц
- Б) Анализ инцидента
- В) Устранение последствий инцидента
- Г) Обнаружение инцидента

Правильный ответ: Г, А, Б, В

Компетенции (индикаторы): ОПК-9

3. Установите правильную последовательность этапов подготовки к проверке системы управления информационной безопасностью:

- А) Определение критериев оценки
- Б) Сбор и анализ документации
- В) Проведение тестирования системы
- Г) Формирование отчета о проверке

Правильный ответ: А, Б, В, Г

Компетенции (индикаторы): ОПК-9

Задания открытого типа

Задания открытого типа на дополнение

Напишите пропущенное слово (словосочетание).

1. Одна из основных задач законодательства в области информационной безопасности — это _____ прав граждан на доступ к информации.

Правильный ответ: обеспечение.

Компетенции (индикаторы):

2. В рамках международного права акты, регулирующие кибербезопасность, часто основаны на _____.

Правильный ответ: конвенциях.

Компетенции (индикаторы): ОПК-9

3. К основным угрозам информационной безопасности можно отнести _____ избыточного доступа к данным.

Правильный ответ: утечку.

Компетенции (индикаторы): ОПК-9

Задания открытого типа с кратким свободным ответом

Напишите пропущенное слово (словосочетание).

1. Важным аспектом правового обеспечения информационной безопасности является _____.

Правильный ответ: защита данных/ защита личных данных.

Компетенции (индикаторы): ОПК-9

2. Одним из главных принципов информационной безопасности является _____.

Правильный ответ: законность обработки информации/ законность обработки данных.

Компетенции (индикаторы): ОПК-9

3. _____ — это комплекс мер, которые нужны, чтобы защитить от утечки или взлома программы, компьютерные системы и данные

Правильный ответ: Информационная безопасность/ ИБ.

Компетенции (индикаторы): ОПК-9

Задания открытого типа с развернутым ответом

1. Ваша команда работает над проектом, связанным с разработкой программного обеспечения для обработки персональных данных граждан. В соответствии с ФЗ-152 «О персональных данных», какие меры должны быть предусмотрены для обеспечения защиты этих данных?

Приведите конкретные статьи закона и объясните их применение в вашем проекте.

Время выполнения – 30 мин.

Ожидаемый результат: Статья 19 ФЗ-152 «О персональных данных» требует от операторов соблюдения принципов конфиденциальности и безопасности обработки персональных данных, а также применения необходимых мер для защиты этих данных от несанкционированного доступа, уничтожения или искажения. Важно внедрить такие меры, как шифрование, регулярные аудиты безопасности и обучение сотрудников. Нужно также указать, что передача данных третьим лицам должна регламентироваться законом и соглашениями.

Критерии оценивания: возможно перефразирование с отражением содержательной составляющей

Компетенции (индикаторы): ОПК-9

2. Представьте, что ваша организация получила уведомление о возможном кибератаке. Какие действия необходимо предпринять согласно требованиям законодательства и внутренней политики организации, чтобы обеспечить информационную безопасность? Опирируйте ФЗ № 149 «Об информации, информационных технологиях и о защите информации».

Время выполнения – 25 мин.

Ожидаемый результат: Согласно статье 17 ФЗ № 149, необходимо провести оценку текущего состояния системы безопасности, идентифицировать

уязвимости и потенциальные угрозы. Затем, в соответствии с внутренними регламентами, следует создать комиссию для реагирования на инцидент и уведомить всех сотрудников о необходимости усиления мер безопасности. Важно также задействовать меры по информированию пользователей об инциденте и организовать восстановительные работы после атаки, следуя требованиям безопасности.

Критерии оценивания: возможно перефразирование с отражением содержательной составляющей

Компетенции (индикаторы): ОПК-9

3. В вашей компании планируется внедрение новой информационной системы, в которой будут обрабатываться служебные и персональные данные сотрудников. Какие права имеют сотрудники в отношении своих данных, и как организация должна соблюдать требования ФЗ № 152 «О персональных данных»? Опишите необходимые действия.

Время выполнения – 30 мин.

Ожидаемый результат: Согласно статье 14 ФЗ № 152, сотрудники имеют право на доступ к своим персональным данным, их исправление и удаление в случае недостоверности. Поэтому организация должна разработать и утвердить политику конфиденциальности, в которой будут прописаны права сотрудников. Необходимо обеспечить прозрачность обработки их данных, информируя о цели обработки, сроках хранения и условиях передачи третьим лицам. Важно также внедрить процедуры для реализации этих прав, включая механизм подачи запросов на доступ или исправление данных

Критерии оценивания: возможно перефразирование с отражением содержательной составляющей

Компетенции (индикаторы): ОПК-9

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Правовое обеспечение информационной безопасности» соответствует требованиям ФГОС ВО.

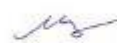
Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по специальности 40.05.01 – Правовое обеспечение национальной безопасности.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины представлены в полном объеме.

Виды оценочных средств, включенные в представленный фонд, отвечают основным принципам формирования ФОС.

Разработанный и представленный для экспертизы фонд оценочных средств рекомендуется к использованию в процессе подготовки обучающихся по указанному направлению

Председатель учебно-методической комиссии
института



Михайлов Д. В.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)