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

Институт гражданской защиты
Кафедра специальных технических средств

УТВЕРЖДАЮ
Директор _____ Малкин В. Ю.
(подпись)
«25» февраля 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

«Кибербезопасность БАС»
25.03.03 Аэронавигация
«Эксплуатация беспилотных авиационных систем»

Разработчики:
доцент _____ Сыровой Г.В.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры специальных технических средств от «25» 02 2025 г., протокол № 4

Заведующий кафедрой _____ Победа Т.В.
(подпись)

Луганск 2025 г.

Комплект оценочных материалов по дисциплине
«Кибербезопасность БАС»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. Выберите один правильный ответ.

Какой из следующих терминов описывает несанкционированный доступ к компьютерной системе:

А) Фишинг;

Б) Хакерство;

В) Вирус;

Г) Спам.

Правильный ответ: Б

Компетенции (индикаторы): ПК-11.

2. Выберите один правильный ответ.

Какой из следующих типов атак направлен на перехват данных, передаваемых между БАС и наземной станцией:

А) DDoS-атака;

Б) Атака "человек посередине" (MITM);

В) SQL-инъекция;

Г) Вредоносное ПО.

Правильный ответ: Б

Компетенции (индикаторы): ПК-11.

3. Выберите один правильный ответ.

Какой метод шифрования используется для защиты данных, передаваемых между БАС и наземной станцией:

А) AES (Advanced Encryption Standard);

Б) MD5 (Message-Digest Algorithm 5);

В) SHA-1 (Secure Hash Algorithm 1);

Г) DES (Data Encryption Standard).

Правильный ответ: А

Компетенции (индикаторы): ПК-11.

4. Выберите один правильный ответ.

Какой из следующих документов описывает правила и процедуры, касающиеся кибербезопасности в организации:

А) Политика конфиденциальности;

Б) Кодекс поведения;

В) Политика безопасности информации;

Г) Договор о неразглашении.
Правильный ответ: В
Компетенции (индикаторы): ПК-11.

5. Выберите один правильный ответ.
Какой метод аутентификации требует от пользователя предоставить два или более факторов для подтверждения своей личности:
А) Однофакторная аутентификация;
Б) Многофакторная аутентификация;
В) Биометрическая аутентификация;
Г) Парольная аутентификация.
Правильный ответ: Б
Компетенции (индикаторы): ПК-11.

Задания закрытого типа на установление соответствия

1. Определите соответствие терминов кибербезопасности и их определения

	ТЕРМИНЫ		ОПРЕДЕЛЕНИЯ
1)	Фишинг	А)	Процесс проверки подлинности пользователя или устройства.
2)	Вредоносное ПО	Б)	Метод, используемый для защиты данных путем их преобразования в неразборчивый формат.
3)	Атака DDoS	В)	Атака, направленная на перегрузку системы, чтобы сделать ее недоступной.
4)	Шифрование	Г)	Программное обеспечение, предназначенное для повреждения или получения несанкционированного доступа к системе.
5)	Аутентификация	Д)	Техника обмана пользователей для получения конфиденциальной информации.

Правильный ответ

1	2	3	4	5
Д	Г	В	Б	А

Компетенции (индикаторы): ПК-11.

2. Определите соответствие описания угрозы и уязвимости

	УГРОЗЫ		ОПИСАНИЕ
1)	Атака "человек посередине" (MITM)	А)	Метод, при котором злоумышленник перехватывает и изменяет коммуникации между двумя сторонами.
2)	SQL-инъекция	Б)	Техника, использующая человеческие факторы для получения конфиденциальной информации.
3)	Вредоносные ссылки	В)	Уязвимость, которая еще не была обнаружена и исправлена разработчиками.
4)	Уязвимость нулевого дня	Г)	Атака, при которой вредоносный код внедряется в базу данных через уязвимости в SQL-запросах.
5)	Социальная инженерия	Д)	Ссылки, которые ведут на вредоносные сайты или загружают вредоносное ПО.

Правильный ответ

1	2	3	4	5
А	Г	Д	В	Б

Компетенции (индикаторы): ПК-11.

3. Определите соответствие методов защиты информации и их описания

	МЕТОДЫ ЗАЩИТЫ		ОПИСАНИЕ
1)	Антивирусное ПО	А)	Программа, предназначенная для обнаружения и удаления вредоносного ПО.
2)	Брандмауэр	Б)	Система, контролирующая входящий и исходящий трафик для защиты сети.
3)	Многофакторная аутентификация	В)	Процесс, при котором данные преобразуются в неразборчивый формат для защиты.
4)	Резервное копирование	Г)	Метод, при котором пользователю требуется предоставить несколько факторов для подтверждения своей личности.
5)	Шифрование данных	Д)	Процесс создания копий данных для предотвращения их потери.

Правильный ответ

1	2	3	4	5
А	Б	Г	Д	В

Компетенции (индикаторы): ПК-11.

4. Определите соответствие политики и описание стандартов безопасности

	ПОЛИТИКА		ОПИСАНИЕ
1)	Политика безопасности информации	А)	Документ, описывающий правила и процедуры для защиты информации в организации.
2)	Политика управления инцидентами	Б)	Политика, регулирующая, кто и как может получать доступ к системам и данным.
3)	Политика доступа	В)	Процедуры, которые следует соблюдать при возникновении инцидентов безопасности.
4)	Политика конфиденциальности	Г)	Политика, касающаяся использования компьютерных ресурсов и оборудования.
5)	Политика использования ресурсов	ДЕ)	Документ, описывающий, как организация будет защищать личные данные пользователей.

Правильный ответ

1	2	3	4	5
А	В	Б	Д	Г

Компетенции (индикаторы): ПК-11.

Задания закрытого типа на установление правильной последовательности

Запишите правильную последовательность букв слева на право.

1. Установите правильную последовательность процессов реагирования на инциденты:

А) Оценка инцидента.
Б) Уведомление ответственных лиц.
В) Сбор доказательств.
Г) Устранение уязвимости.
Д) Анализ и отчет о инциденте.
Правильный ответ: Б, А, В, Г, Д
Компетенции (индикаторы): ПК-11.

2. Установите правильную последовательность процессов шифрования данных:

А) Выбор алгоритма шифрования.

Б) Доступ к зашифрованным данным.

В) Хранение зашифрованных данных.

Г) Применение шифрования к данным.

Д) Генерация ключа шифрования.

Правильный ответ: А, Д, Г, В, Б

Компетенции (индикаторы): ПК-11.

3. Установите правильную последовательность процесса оценки уязвимостей:

А) Приоритизация уязвимостей.

Б) Разработка плана устранения.

В) Сканирование системы на уязвимости.

Г) Анализ результатов сканирования.

Д) Реализация мер по устранению уязвимостей.

Правильный ответ: В, Г, А, Б, Д

Компетенции (индикаторы): ПК-11.

4. Установите правильную последовательность процесса обучения сотрудников кибербезопасности:

А) Обновление учебных материалов на основе обратной связи.

Б) Проведение тренингов.

В) Разработка учебных материалов.

Г) Оценка эффективности обучения.

Д) Определение потребностей в обучении.

Правильный ответ: Д, В, Б, Г, А

Компетенции (индикаторы): ПК-11.

Задания открытого типа

Задания открытого типа на дополнение

Напишите пропущенное слово (словосочетание).

1. Кибербезопасность БАС направлена на защиту от _____, _____и _____.

Правильный ответ: несанкционированного доступа, кибератак, утечки данных

Компетенции (индикаторы): ПК-11.

2. Одной из основных угроз для БАС является _____, которое может привести к _____и _____.

Правильный ответ: вмешательство в управление, потере контроля, аварии

Компетенции (индикаторы): ПК-11.

3. Для обеспечения кибербезопасности БАС необходимо внедрять _____, _____ и _____.

Правильный ответ: шифрование данных, многофакторную аутентификацию, системы обнаружения вторжений (IDS)

Компетенции (индикаторы): ПК-11.

4. Одной из мер защиты является _____-, которая _____.

Правильный ответ: регулярное обновление программного обеспечения, устраняет уязвимости

Компетенции (индикаторы): ПК-11.

5. Для оценки уровня киберугроз БАС применяются _____, и _____ - _____."

Правильный ответ: тесты на проникновение, аудит безопасности, анализ рисков

Компетенции (индикаторы): ПК-11.

Задания открытого типа с кратким свободным ответом

1._____ - злоумышленник перехватывает и изменяет данные, передаваемые между БАС и наземной станцией, что может привести к потере контроля над БАС.

Правильный ответ: Атака "человек посередине" (MITM)

Компетенции (индикаторы): ПК-11.

2) _____- может быть внедрено в систему, что приведет к повреждению данных или захвату управления БАС.

Правильный ответ: Вредоносное ПО

Компетенции (индикаторы): ПК-11.

3) _____- перегружают систему, делая ее недоступной для управления, что может привести к авариям.

Правильный ответ: DDoS-атаки

Компетенции (индикаторы): ПК-11.

4) _____- манипуляции с операторами для получения доступа к системам, что может привести к утечке конфиденциальной информации.

Правильный ответ: Социальная инженерия

Компетенции (индикаторы): ПК-11.

Задания открытого типа с развернутым ответом

1. Опишите основные угрозы кибербезопасности, с которыми могут столкнуться беспилотные авиационные системы. Укажите, как каждая угроза может повлиять на безопасность системы и ее операционные возможности.

Время выполнения – 5 мин.

Ожидаемый результат:

1) Атака "человек посередине" (MITM): Злоумышленник перехватывает и изменяет данные, передаваемые между БАС и наземной станцией. Это может привести к потере контроля над БАС и изменению маршрута.

2) Вредоносное ПО: Внедрение вредоносного программного обеспечения может повредить систему, украсть данные или захватить управление БАС. Это может привести к авариям или утечке конфиденциальной информации.

3) DDoS-атаки: Перегрузка системы запросами, что делает ее недоступной для управления. Это может привести к невозможности выполнения задач и потере контроля над БАС.

4) Социальная инженерия: Манипуляции с операторами для получения доступа к системам. Это может привести к утечке конфиденциальной информации и несанкционированному доступу.

Критерии оценивания:

-приведены минимум четыре основные угрозы кибербезопасности;

- приведена полная или краткая характеристика принципа.

Компетенции (индикаторы): ПК-11.

2. Перечислите и кратко опишите три метода защиты информации, используемые в БАС. Как каждый из них помогает обеспечить безопасность системы?

Время выполнения – 5 мин.

Ожидаемый результат:

1) Шифрование данных: Преобразует данные в неразборчивый формат, защищая их от несанкционированного доступа. Это гарантирует, что даже если данные будут перехвачены, они останутся недоступными для злоумышленников.

2) Многофакторная аутентификация: Требует от пользователей предоставления нескольких факторов для подтверждения своей личности. Это значительно снижает риск несанкционированного доступа, так как злоумышленнику необходимо получить доступ ко всем факторам.

3) Антивирусное ПО: Обнаруживает и удаляет вредоносное ПО, защищая систему от атак и повреждений. Регулярные обновления антивирусного ПО помогают защитить БАС от новых угроз.

Критерии оценивания:

-приведены минимум три метода защиты информации;

- приведена полная или краткая характеристика принципа.

Компетенции (индикаторы): ПК-11.

3. Объясните, почему наличие политики безопасности информации критично для эксплуатации БАС. Какие ключевые элементы должны быть включены в такую политику?

Время выполнения – 5 мин.

Ожидаемый результат:

Наличие политики безопасности информации критично для обеспечения защиты данных и систем от угроз. Ключевые элементы, которые должны быть включены:

1) Определение ролей и обязанностей: Установление, кто отвечает за безопасность и управление данными, что помогает избежать путаницы и недоразумений.

2) Процедуры реагирования на инциденты: Четкие шаги, которые необходимо предпринять в случае нарушения безопасности, помогают быстро и эффективно реагировать на инциденты.

3) Правила доступа к данным: Определение, кто и как может получать доступ к информации, что снижает риск несанкционированного доступа.

4) Обучение сотрудников: Регулярные тренинги по кибербезопасности для повышения осведомленности сотрудников о возможных угрозах и методах защиты.

Критерии оценивания:

-приведены минимум четыре ключевых элемента политики безопасности информации;

- приведена полная или краткая характеристика принципа.

Компетенции (индикаторы): ПК-11.

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Кибербезопасность БАС» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки «Аэронавигация».

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)