МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КОСТРОМСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ АКАДЕМИЯ»

Утверждаю:
Декан электроэнергетического факультета

Николай Александрович Климов
Подписано цифровой подписью: Николай Александрович Климов
Дата: 2026.02.11 12:12:24 +03'00'
_____ / Н.А. Климов /

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

«БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

Специальность 09.02.11 Разработка и управление программным обеспечением

Квалификация выпускника программист

Форма обучения очная

Срок освоения ППССЗ 3 года 10 месяцев

На базе основного общего образования

Караваево 2026

Фонд оценочных средств предназначен для контроля знаний и умений, обучающихся по ППССЗ (СПО) специальности: 09.02.11 Разработка и управление программным обеспечением.
Дисциплина: «Безопасность программного обеспечения»

Составитель Андрей Александрович Лобачев Подписано цифровой подписью: Андрей Александрович Лобачев DN: dc=int, dc=ksaa, ou=nw, cn=Андрей Александрович Лобачев _____/ А.А. Лобачев /

Фонд оценочных средств утвержден на заседании кафедры автомобилей, тракторов и технических систем, протокол № 6 от «5» февраля 2026.

Заведующий кафедрой Александр Николаевич Зинцов Подписано цифровой подписью: Александр Николаевич Зинцов DN: dc=int, dc=ksaa, ou=nw, cn=Александр Николаевич Зинцов Дата: 2026.02.05 11:52:00 +03'00' _____/ А.Н. Зинцов /

Согласовано:
Председатель методической комиссии электроэнергетического факультета,
протокол №1 от «10» февраля 2026 года.

Татьяна Михайловна Богданова Подписано цифровой подписью: Татьяна Михайловна Богданова Дата: 2026.02.10 16:03:47 +03'00' _____ / Т.М. Богданова /

Паспорт
фонда оценочных средств
Результаты освоения учебной дисциплины «Безопасность программного обеспечения»
ППССЗ (СПО) по специальности:
09.02.11 Разработка и управление программным обеспечением

№ п/п	Контролируемые дидактические единицы	Контролируемые компетенции (или их части)	Наименование оценочных средств		
			Тесты, кол-во заданий	Другие оценочные средства	
				вид	кол-во заданий
1	Тема 1. Основы безопасности программного обеспечения	ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках. ПК 2.1. Проектировать модули программного обеспечения. ПК 2.3. Выполнять интеграцию модулей и компонентов программного обеспечения	25	Опрос	10
2	Тема 2. Разработка безопасного ПО и прикладная криптография		25	Опрос	10
3	Экзамен по темам 1-2			Собеседование	20
Всего:			50		40

Методика проведения контроля по проверке базовых знаний по дисциплине «Безопасность программного обеспечения»

Тема 1 Основы безопасности программного обеспечения

Вопросы для устного опроса

1. Назначение и структура стека протоколов TCP/IP. Характеристика протокола TCP/IP с точки зрения информационной безопасности.
2. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: подслушивание (sniffing), подмена доверенного субъекта (IP – spoofing), посредничество в обмене незашифрованными ключами (Man-in-the-Middle).
3. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.
4. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Процедуры безопасности.
5. Основные понятия криптологии: криптография, криптоанализ, алфавит, текст, зашифрование, расшифрование, блочное и поточное шифрование, криптографическая система, ключ, симметричные и ассиметричные криптосистемы.
6. Обзор программных и программно-аппаратных средств криптографической защиты: пакет PGP, система криптографической защиты информации “Верба - О”, программный комплекс “Inter –PRO”, программно-аппаратный комплекс “Доверенный удостоверяющий центр”.
7. Понятие компьютерного вируса. Классификация вирусов.
8. Методы борьбы с вирусами: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”.
9. Антивирусные программы: утилита Dr. Web Curelt, программа Dr. Web., антивирус Avira AntiVir Personal, антивирус Avast! Home Edition.
10. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Показатели защищенности межсетевых экранов.

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который прочно усвоил программный материал в полном объеме, исчерпывающе, грамотно и логически стройно его излагает, четко формулирует основные понятия, приводит соответствующие примеры, уверенно владеет материалом.

Оценка «хорошо» выставляется обучающемуся, который твердо усвоил программный материал, грамотно и по существу излагает его без существенных ошибок, правильно применяет теоретические положения при решении конкретных задач, с небольшими погрешностями приводит формулировки определений, по ходу изложения допускает небольшие пробелы, не искажающие содержания ответа.

Оценка «удовлетворительно» выставляется обучающемуся, который не совсем твердо владеет программным материалом, знает основные теоретические положения изучаемой темы, при ответах допускает малосущественные погрешности, искажения логической последовательности при изложении материала, неточную аргументацию теоретических положений, испытывает затруднения при ответе на дополнительные вопросы.

Оценка «неудовлетворительно» выставляется обучающемуся, имеющему серьезные пробелы в знании учебного материала, допускающему принципиальные ошибки при ответе на вопросы.

Компьютерное тестирование

Выберите один правильный вариант ответа и нажмите кнопку «Далее»

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

+поддержка высшего руководства

эффективные защитные меры и методы их внедрения

актуальные и адекватные политики и процедуры безопасности

проведение тренингов по безопасности для всех сотрудников

Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

анализ рисков

+анализ затрат / выгоды

результаты ALE

выявление уязвимостей и угроз, являющихся причиной риска

Наиболее распространены угрозы информационной безопасности сети:

распределенный доступ клиент, отказ оборудования

моральный износ сети, инсайдерство

+сбой (отказ) оборудования, нелегальное копирование данных

вирусы

Основная масса угроз информационной безопасности приходится на черви

+троянские программы

шпионские программы

нет правильного ответа

Stuxnet – это:

+промышленный вирус

троянская программа

макровирус

сетевой червь

Почтовый ящик современного человека завален входящими сообщениями, среди которых попадаются опасные письма. Рассылку писем, сфабрикованных под видом разных форм общественной деятельности для получения конфиденциальной информации, называется:

мистификация

стримминг

+фишинг

хакинг

Как расшифровывается PGP?

Post Got Posted

+Pretty Good Privacy

Private Golden Pen

нет верного ответа

Программа, предназначенная для борьбы с вредоносными программами, называется:

таблетка

лекарство

вакцина

+антивирус

Современные антивирусы — это программные комплексы, состоящие из нескольких программ. Чаще всего они включают:

+антивирус-сканер и антивирус-монитор

антивирус-принтер и антивирус-мышь

антивирус-процессор и антивирус-клавиатура

антивирус-ноутбук и антивирус-моноблок
Главный недостаток антивирусов-сканеров:
+они не могут предотвратить заражение компьютера, потому что начинают работать только при ручном запуске
они встраиваются в операционную систему, поэтому ошибки разработчиков антивируса могут привести к выводу ОС из строя
они могут заразиться от вредоносоного ПО и стать вирусом
они не могут работать без интернета
Брандмауэр – это:
+это программа защиты компьютера, которая проверяет и контролирует исходящие и входящие данные между компьютером и сетью
это специальная программа для обеспечения работы устройств, подключаемых к компьютеру
это специальная программа, которая используется для отправки запросов, обработки и отображения страниц веб-сайтов
это специальная программа для редактирования системного реестра
Брандмауэр еще называют:
Браузер
+фаейрвол
райвер
вайфай
Можно улучшить безопасность компьютера при работе в сети Интернет:
пользоваться не WI-FI соединением с интернетом а проводным
осуществлять вход в интернет только через браузер
+включать антивирус-монитор и брандмауэр
включать специальные драйверы
При работе с электронной почтой необходимо принимать меры безопасности необходимы:
не открывать подозрительные сообщения электронной почты
не открывать сообщения электронной почты, полученные с неизвестных адресов, особенно файлы-приложения
не переходить по ссылкам в тексте писем, с большой вероятностью они ведут на сайты, зараженные вирусами
+все перечисленные выше
В виды угроз не входит:
угроза доступности
+угроза дублирования
угроза конфиденциальности
угроза целостности
Выберите виды информационных угроз:
контроль доступа, доступность, анонимность
сайты-подделки, взлом, целостность
+доступность, конфиденциальность, целостность
нет правильного ответа
Из представленного ниже, в файловых системах ОС UNIX права доступа к файлу определяются для:
конкретных заданных пользователей
+всех основных пользователей
конкретных заданных групп пользователей
нет правильного ответа
Преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС – это:
внутрипрограммные вирусы

компьютерные черви
+программные закладки
троянские программы

Право на подключение к общей базе данных предоставляется по умолчанию:
+системному администратору
всем пользователям
администратору сервера баз данных
никому

Из представленных ниже свойств безопасная система обладает:
восстанавливаемость
+доступность
детерминированность
нет правильного ответа

Некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении к компьютерной системе – это:
аутентификатор
+пароль
идентификатор
пароль

Правильно укажите точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов:
эвристические
+сигнатурные
проактивные
классические

Какое название носят полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать транзакции, процедуры или всю систему в целом:
аудит
аутентификация
+авторизация
шифрование

Нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей, называется:
прокси-сервер
+спам
программная закладка
нет правильного ответа

Метод ограничения доступа к объектам, основанный на сопоставлении меток безопасности субъекта и объекта, является таким управлением доступа:
+принудительное
произвольное
дискретное
индивидуальное

Методика проведения контроля

Параметры методики	Значение параметра
Предел длительности всего контроля	10 минут
Последовательность выбора вопросов	Случайная
Предлагаемое количество вопросов	10

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который правильно выполнил 9-10 тестовых заданий.

Оценка «хорошо» выставляется обучающемуся, который: правильно выполнил 7-8 тестовых заданий.

Оценка «удовлетворительно» выставляется обучающемуся, который правильно выполнил 5-6 тестовых заданий.

Оценка «неудовлетворительно» выставляется обучающемуся, который правильно выполнил менее 4 тестовых заданий.

Тема 2. Разработка безопасного ПО и прикладная криптография

Вопросы для устного опроса

1. Что такое криптография, какие виды криптографии бывают и для чего применяются?
2. Что такое электронная подпись и чем она отличается от хэша?
3. Каким ключом нужно подписывать информацию, а каким шифровать, чтобы безопасно передать её получателю?
4. Какие уязвимости информационных систем или ПО известны? Например, из списка OWASP Top Ten или БДУ ФСТЭК России.
5. Какие средства и способы подходят для защиты удалённого доступа? Например, двухфакторная аутентификация, контроль действий пользователей, проверка безопасности подключённых устройств, проверка подлинности пользователя, который подключается к корпоративной сети.
6. Опишите процесс работы протокола безопасности, например, Kerberos или TLS.
7. Опишите процесс реализации атаки, например, подбор пароля, какой-то из видов спуфинга на один из протоколов модели OSI, DNS-тунель.
8. Основные характеристики и структура алгоритма DES.
9. Основные характеристики и структура алгоритма AES.
10. Описание алгоритма RSA.

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который прочно усвоил программный материал в полном объеме, исчерпывающе, грамотно и логически стройно его излагает, четко формулирует основные понятия, приводит соответствующие примеры, уверенно владеет материалом.

Оценка «хорошо» выставляется обучающемуся, который твердо усвоил программный материал, грамотно и по существу излагает его без существенных ошибок, правильно применяет теоретические положения при решении конкретных задач, с небольшими погрешностями приводит формулировки определений, по ходу изложения допускает небольшие пробелы, не искажающие содержания ответа.

Оценка «удовлетворительно» выставляется обучающемуся, который не совсем твердо владеет программным материалом, знает основные теоретические положения

изучаемой темы, при ответах допускает малосущественные погрешности, искажения логической последовательности при изложении материала, неточную аргументацию теоретических положений, испытывает затруднения при ответе на дополнительные вопросы.

Оценка «неудовлетворительно» выставляется обучающемуся, имеющему серьезные пробелы в знании учебного материала, допускающему принципиальные ошибки при ответе на вопросы.

Компьютерное тестирование

Выберите один правильный вариант ответа и нажмите кнопку «Далее»

Что такое шифрование?

+способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

удобная среда для вычисления конечного пользователя

нет правильного ответа

Шифры замены бывают:

+простые одноалфавитные

одноконтурные полиалфавитные.

многоконтурные полиалфавитные.

монофонические полиалфавитные.

Для восстановления защитного текста требуется:

+ключ

матрица

вектор

пароль

Криптографическая система представляет собой:

+семейство T преобразований открытого текста, члены его семейства индексируются символом k

программу

систему

список паролей

Пространство ключей k – это:

+набор возможных значений ключа

длина ключа

номер ключа

нет правильного ответа

Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:

+1

2

3

4

Количество используемых ключей в системах с открытым ключом:

2+

3

1

4

Выберите то, как связаны ключи друг с другом в системе с открытым ключом:

+математически

логически

алгоритмически
логарифмически
Электронной подписью принято называть:
+присоединяемое к тексту его криптографическое преобразование
+текст
зашифрованный текст
фото настоящей подписи
Криптостойкость – это:
+характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
свойство гаммы
все ответы верны
нет правильного ответа
Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
длина шифрованного текста должна быть равной лине исходного текста
зашифрованное сообщение должно поддаваться чтению только при наличии ключа
нет правильного ответа
+оба ответа верны
Основными современными методами шифрования являются:
алгоритм гаммирования
алгоритмы сложных математических преобразований
алгоритм перестановки
+все ответы верны
Символы исходного текста, складывающиеся с символами некой случайной последовательности, являются:
+алгоритмом гаммирования
алгоритмом перестановки
алгоритмом аналитических преобразований
алгоритмом сложных математических преобразований
Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:
+3
4
5
6
Таблицы Вижинера, применяемые для повышения стойкости шифрования:
во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке
в качестве ключа используется случайность последовательных чисел
нет правильного ответа
+оба ответа верны
Цель криптоанализа:
+определение стойкости алгоритма
увеличение количества функций замещения в криптографическом алгоритме
уменьшение количества функций подстановок в криптографическом алгоритме
определение использованных перестановок
Рост частоты применения брутфорс-атак произойдет по причине:
возросло используемое в алгоритмах количество перестановок и замещений
алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
+мощность и скорость работы процессоров возросла
длина ключа со временем уменьшилась

Не будет являться свойством или характеристикой односторонней функции хэширования:
она преобразует сообщение произвольной длины в значение фиксированной длины
имея значение дайджеста сообщения, невозможно получить само сообщение
получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
+она преобразует сообщение фиксированной длины в значение переменной длины
Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений:
Data Encryption Algorithm
Digital Signature Standard
+Secure Hash Algorithm
Data Signature Algorithm
Определите преимущество RSA над DSA.
+он может обеспечить функциональность цифровой подписи и шифрования+
он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
это блочный шифр, и он лучше поточного
он использует одноразовые шифровальные блокноты
Многими странами происходит ограничение использования и экспорта криптографических систем с целью:
без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
эти системы могут использоваться некоторыми странами против их местного населения
+криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования
законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему
Выберите то, что используют для создания цифровой подписи:
закрытый ключ получателя
открытый ключ отправителя
+закрытый ключ отправителя
открытый ключ получателя
Выберите высказывание, которое лучше всего описывает цифровую подпись:
это метод переноса собственноручной подписи на электронный документ
это метод шифрования конфиденциальной информации
это метод, обеспечивающий электронную подпись и шифрование
+это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения
Эффективная длина ключа в DES:
+56
64
32
16
8
Причина, по которой удостоверяющий центр отзывает сертификат:
если открытый ключ пользователя скомпрометирован
если пользователь переходит на использование модели PEM, которая использует сеть доверия
+если закрытый ключ пользователя скомпрометирован
если пользователь переходит работать в другой офис

Методика проведения контроля

Параметры методики	Значение параметра
Предел длительности всего контроля	10 минут
Последовательность выбора вопросов	Случайная
Предлагаемое количество вопросов	10

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который правильно выполнил 9-10 тестовых заданий.

Оценка «хорошо» выставляется обучающемуся, который: правильно выполнил 7-8 тестовых заданий.

Оценка «удовлетворительно» выставляется обучающемуся, который правильно выполнил 5-6 тестовых заданий.

Оценка «неудовлетворительно» выставляется обучающемуся, который правильно выполнил менее 4 тестовых заданий.

Вопросы собеседования к экзамену по темам 1-2

1. Какие документы регулируют безопасность программного обеспечения?
2. Какие меры направлены на ограничение доступа третьих лиц к конфиденциальной информации?
3. Какие меры по регистрации событий безопасности предусмотрены в информационных системах?
4. Какие меры по управлению доступом используются в информационных системах?
5. Какие меры по выявлению инцидентов и реагированию на них предусмотрены в информационных системах?
6. Системы обнаружения предотвращения вторжений (IPS/IDS или СОВ).
7. Антивирусы — программы для обнаружения и нейтрализации вредоносных скриптов.
8. Средства защиты от несанкционированного доступа (СЗИ от НСД).
9. Средства или модули доверенной загрузки (СДЗ или МДЗ).
10. Какие методы используются при тестировании безопасности программного обеспечения?
11. Каковы особенности операционных систем в защищенном исполнении?
12. В чем состоят достоинства и недостатки статистических и динамических способов исследования ПО? Каковы принципы работы дизассемблеров, декомпиляторов, трассировщиков, следящих систем при исследовании ПО?
13. Какие методы и практики разработки применяются для повышения безопасности программных модулей?
14. Какие существуют способы проведения испытаний ПО, оценки качества и сертификации программных средств? Каков состав методического обеспечения проведения испытаний программ?
15. Какие основные этапы включают испытания ПО? Приведите последовательность действий при этих испытаниях.
16. Какова технология создания сложных программных комплексов? Охарактеризуйте действия разработчиков при обеспечении технологической безопасности ПО.
17. Приведите структурно-функциональную схему инструментальных средств поддержки создания безопасного программного обеспечения.
18. Каковы этапы контроля безопасности общего и специального ПО на этапе исследования и испытаний ПО?
19. Как обеспечивается функциональная эквивалентность программ до и после их обфускации?

20. Расскажите о возможности разработки такого дистрибутива операционной системы с открытыми исходными кодами, который обеспечил бы учет специфики объектов, потенциально уязвимых для кибератак. Перечислите основные компоненты такого дистрибутива.

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который правильно ответил на 5 случайно выбранных вопросов, показав достаточный уровень знаний. В случае если студент ответил на 4 вопроса правильно, но рассчитывает получить оценку «отлично» ему задаётся дополнительный вопрос ответить.

Оценка «хорошо» выставляется обучающемуся, который: правильно ответил на 4 случайно выбранных вопросов, показав достаточный уровень знаний. В случае если студент ответил на 3 вопроса правильно, но рассчитывает получить оценку «хорошо» ему задаётся дополнительный вопрос.

Оценка «удовлетворительно» выставляется обучающемуся, который: правильно ответил на 3 случайно выбранных вопросов, показав достаточный уровень знаний. В случае если студент ответил на 2 вопроса правильно, но рассчитывает получить оценку «удовлетворительно» ему задаётся дополнительный вопрос.

Оценка «неудовлетворительно» выставляется обучающемуся, который не ответил ни на один вопрос или ответил на 1 или 2 вопроса верно, но не ответил на дополнительный вопрос

Форма промежуточной аттестации по дисциплине *экзамен*.

Окончательные результаты обучения (формирования компетенций) определяются посредством перевода баллов, набранных студентом в процессе освоения дисциплины, в оценки:

– базовый уровень сформированности компетенции считается достигнутым если результат обучения соответствует оценке «удовлетворительно» (50 до 64 рейтинговых баллов);

– повышенный уровень сформированности компетенции считается достигнутым, если результат обучения соответствует оценкам «хорошо» (65-85 рейтинговых баллов) и «отлично» (86-100 рейтинговых баллов).

Дополнительные контрольные испытания

для студентов, набравших менее 50 баллов (в соответствии с Положением «О модульно-рейтинговой системе»), формируются из числа оценочных средств по темам, которые не освоены студентом.