

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
прикладной математики,
информатики, физики и
методики их преподавания



Е.А. Позднова
06.09.2017г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки: 44.03.01 Педагогическое образование

Профиль подготовки: Информатика и информационные технологии в образовании

Квалификация (степень) выпускника: бакалавр

**Паспорт
фонда оценочных средств
по учебной дисциплине
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

1. В результате изучения дисциплины «Информационная безопасность» обучающийся должен:

Знать:

- основные понятия теории информационной безопасности;
- направления разработки и применения средств защиты информации;
- методы и средства защиты информации;
- основные нормативные документы в сфере обеспечения информационной безопасности;

Уметь:

- уметь применять правовые, программные и технические средства для защиты информации в информационных системах;
- уметь пользоваться различными методами и средствами защиты информации в различных видах деятельности;

Владеть:

- навыками ориентироваться в законодательной базе РФ, обеспечивающей информационную безопасность на различных уровнях;
- способами осуществления выбора различных мер и средств обеспечения информационной безопасности в учебном процессе с учетом реального оснащения образовательного учреждения.

2. Программа оценивания контролируемой компетенции

Текущая аттестация	Контролируемые модули, разделы, (темы) дисциплины, их наименование	Код контролируемой компетенции (или её части)	Наименование оценочного средства
1	Угрозы информационной безопасности	ПК-4, ОПК-4, ОК-3;	
2	Информационные системы и их компоненты как объекты защиты	ПК-4, ОПК-4, ОК-3;	
3	Направления разработки и применения средств защиты информации	ПК-4, ОПК-4, ОК-3;	
4	Методика построения защищенных информационных систем	ПК-4, ОПК-4, ОК-3;	
5	Организационно-правовые меры и средства защиты информации	ПК-4, ОПК-4, ОК-3;	
6	Технические и программные средства защиты информации	ПК-4, ОПК-4, ОК-3;	
7	Технические средства контроля доступа к компонентам информационных систем	ПК-4, ОПК-4, ОК-3;	
8	Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.	ПК-4, ОПК-4, ОК-3;	
9	Методы и средства уничтожения информации	ПК-4, ОПК-4, ОК-3;	
10	Лабораторный практикум. Криптографические методы защиты информации	ПК-4, ОПК-4, ОК-3;	Контрольные вопросы к защите лабораторных работ
Промежуточная аттестация – зачет			Вопросы к зачету, итоговый тест

3. Типовые контрольные задания для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Материалы для проведения промежуточной аттестации

3.1.1. Форма КИМ [Приложение1](#)

3.1.2. Вопросы к зачету по дисциплине «Информационная_безопасность» [Приложение2](#)

3.1.3 Итоговый тест по дисциплине «Информационная безопасность» [Приложение 3](#)

3.2. Материалы для проведения текущей аттестации

3.2.1 Контрольные вопросы к защите лабораторных работ по дисциплине «Информационная безопасность» [Приложение 4](#)

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенции

Методические материалы, сопровождающие процедуры оценивания

	Процедура оценивания	Документальное сопровождение
	Определение технологии проведения промежуточной аттестации (в соответствии с действующими локальными актами).	Традиционная форма
		зачет
	Определение форм и оценочных средств текущего контроля для мониторинга показателей сформированности компетенций в процессе освоения учебной дисциплины.	Контрольные тесты / иное
	Доведение до сведения обучающихся методических рекомендаций по освоению дисциплины, форм и графика контрольно-оценочных мероприятий.	П ВГУ 2.1.07-2015 Положение о проведении промежуточной аттестации обучающихся по образовательным программам высшего образования / иное
	Систематический учет показателей сформированности компетенций у обучающихся в рамках балльно-рейтинговой системы и / или традиционных форм оценки и отражение результатов в соответствующих документах (балльно-рейтинговый лист / иное).	на основе текущей аттестации
	Оценивание показателей компетенций, сформированных в процессе изучения дисциплины / модуля в рамках промежуточной аттестации в соответствии с технологией проведения промежуточной аттестации на основе действующих локальных актов.	заполнение зачетной ведомости и представление в деканат

Приложение 1

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

Форма контрольно-измерительного материала

УТВЕРЖДАЮ
заведующий кафедрой
прикладной математики, информатики, физики и
методики преподавания

подпись, расшифровка подписи

___.__.20__

Направление подготовки / специальность 44.03.01 Педагогическое образование
шифр, наименование

Дисциплина Информационная безопасность

Форма обучения заочное
очное, очно-заочное, заочное

Вид контроля зачет
экзамен, зачет;

Вид аттестации промежуточная
текущая, промежуточная

Контрольно-измерительный материал №__

1. _____

2. _____

.....

Преподаватель _____
подпись расшифровка подписи

Приложение 2

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

Кафедра прикладной математики,
информатики, физики и
методики преподавания

Вопросы к зачету по дисциплине «Информационная безопасность»

1. Понятие «Информационная безопасность». Основные компоненты информационной безопасности. Важность и комплексность проблемы информационной безопасности.
2. Понятие информационной угрозы. Классификация видов угроз информационной безопасности по различным признакам. Примеры реализации угроз информационной безопасности.
3. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации
4. Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы. Виды сервисов безопасности.
5. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
6. Организационно-правовые меры и средства защиты информации
7. Технические и программные средства защиты информации
8. Понятие «вредоносное программное обеспечение». Основная классификация вредоносного программного обеспечения согласно лаборатории Касперского.
9. Понятие компьютерный вирус. Основные механизмы развития и распространения.
10. Антивирусное обеспечение. Основные компоненты антивирусной программы.
11. Технические средства контроля доступа к компонентам информационных систем
12. Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.
13. Методы и средства уничтожения информации
14. Краткая история криптографии.
15. Основные понятия криптографии.
16. Симметричные криптосистемы. Перестановки. Метод Цезаря.
17. Симметричные криптосистемы. Перестановки. Метод Ришелье.
18. Метод моноалфавитной подстановки. Шифр Цезаря с использованием слова впереди алфавита.
19. Метод полиалфавитной подстановки. Шифр Вигнера.
20. Механические криптосистемы.
21. Асимметричные криптосистемы (с публичным ключом). Основные понятия. Необратимые функции.

22. Реализация асимметричной криптосистемы на основе задачи рюкзака. Секретная информация для криптосистем с публичным ключом.
23. Принципы построения криптосистемы с публичным ключом.
24. Электронная подпись. Общие понятия.
25. Электронные платежные системы. Основные свойства. Безопасность электронных платежей.

Критерии оценки:

- **оценка «отлично»** выставляется студенту, если студент отлично ориентируется в теоретическом материале; умеет изложить и корректно оценить различные подходы к излагаемому материалу, способен сформулировать и доказать собственную точку зрения; обнаруживает свободное владение понятийным аппаратом;

- **оценка «хорошо»** выставляется студенту, если студент хорошо ориентируется в теоретическом материале; имеет представление об основных подходах к излагаемому материалу; знает определения основных теоретических понятий излагаемой темы;

- **оценка «удовлетворительно»** выставляется студенту, если студент может ориентироваться в теоретическом материале; в целом имеет представление об основных понятиях излагаемой темы;

- **оценка «неудовлетворительно»** выставляется студенту, если студент не ориентируется в теоретическом материале; не сформировано представление об основных понятиях излагаемой темы.

Составители

_____ Е.А. Позднова

Приложение 3

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

Кафедра прикладной математики,
информатики, физики и
методики преподавания

Итоговый тест по дисциплине «Информационная безопасность»

Время, отводимое для выполнения теста - 40 мин. Проверка тестового задания осуществляется с помощью утверждённого ключа.

1. Информационная безопасность характеризует защищённость:

- А) Пользователя и информационной системы
- Б) Информации и поддерживающей её инфраструктуры
- В) Источника информации
- Г) Носителя информации

2. Что из перечисленного является составляющей информационной безопасности?

- А) Нарушение целостности информации
- Б) Проверка прав доступа к информации
- В) Доступность информации
- Г) Выявление нарушителей

3. Получение требуемой информации информационной услуги пользователем за определённое время, это:

- А) Целостность информации
- Б) Конфиденциальность информации
- В) Доступность информации
- Г) Защищённость информации

4. Конфиденциальность информации гарантирует:

- А) Доступность информации кругу лиц, для кого она предназначена
- Б) Защищённость информации от потери
- В) Защищённость информации от фальсификации
- Г) Доступность информации только автору

5. Сколько уровней формирования режима информационной безопасности?

- А) Три
- Б) Четыре
- В) Два
- Г) Пять

6. Год издания закона Российской Федерации «О государственной тайне»:

- А) 2000 год
- Б) 1993 год
- В) 1995 год
- Г) 1996 год

7. Номер статьи Уголовного кодекса предусматривающей наказание за разглашение государственной тайны?

- А) 138

- Б) 283
- В) 273
- Г) 237

8. *Неправомерный доступ к компьютерной информации наказывается лишением свободы*

- А) До пяти лет
- Б) До трех лет
- В) До года
- Г) До двух лет

9. *Основной источник внутренних отказов?*

А) Невозможность пользователя работать с системой в силу отсутствия соответствующей подготовки

Б) Нежелание пользователя работать с информационной системой

В) Отступление от установленных правил эксплуатации

Г) Нарушение работы систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования

10. *Уровни не относящиеся к уровням формирования режима информационной безопасности?*

- А) Законодательно-правовой
- Б) Информационный
- В) Административный (организационный)
- Г) Программно-технический

11. *На сколько классов подразделяют угрозы информационной безопасности?*

- А) 4
- Б) 3
- В) 2
- Г) 5

12. *Что является самым эффективным при борьбе с непреднамеренными случайными ошибками?*

- А) Резервирование аппаратуры
- Б) Определение степени ответственности за ошибки
- В) Максимальная автоматизация и строгий контроль
- Г) Контроль действий пользователя

13. *Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией*

- А) Законодательно-правовой
- Б) Информационный
- В) Административный (организационный)
- Г) Программно-технический

14. *Основополагающим документом по информационной безопасности в РФ является:*

- А) Конституция РФ
- Б) Уголовный кодекс
- В) Закон о средствах массовой информации
- Г) Закон об информационной безопасности

15. *Целостность информации гарантирует:*

- А) Существование информации в исходном виде
- Б) Принадлежность информации автору
- В) Доступ информации определенному кругу пользователей
- Г) Защищенность информации от несанкционированного доступа

16. *Сколько категорий государственных информационных ресурсов определяет закон «Об информации, информатизации и защите информации»?*

- А) Три
- Б) Четыре
- В) Два
- Г) Пять

17. *Неправомерный доступ к компьютерной информации наказывается штрафом:*

- А) От 5 до 20 минимальных размеров оплаты труда
- Б) От 200 до 500 минимальных размеров оплаты труда
- В) От 150 до 200 минимальных размеров оплаты труда
- Г) До 300 минимальных размеров оплаты труда

18. *Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок:*

- А) До года
- Б) До двух лет
- В) До пяти лет
- Г) До трех месяцев

19. *Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации – это:*

- А) Компьютерная безопасность
- Б) Информационная безопасность
- В) Защита информации
- Г) Защита государственной тайны

20. *Что из перечисленного является задачей информационной безопасности?*

- А) Устранение неисправностей аппаратных средств
- Б) Устранение последствий стихийных бедствий
- В) Защита технических и программных средств информатизации от ошибочных действий персонала
- Г) Восстановление линий связи

21. *Выберите правильную иерархию пространства требований в «Общих критериях»:*

- А) Класс – семейство – компонент – элемент
- Б) Элемент – класс – семейство – компонент
- В) Компонент – семейство – класс – элемент
- Г) Семейство – компонент – класс – элемент

22. *Сколько классов СВТ по уровню защищенности от НСД к информации определено в руководящем документе Гостехкомиссии «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?*

- А) Три
- Б) Семь
- В) Пять
- Г) Четыре

23. *Комплекс предупредительных мер по обеспечению информационной безопасности организации – это:*

- А) Информационная политика
- Б) Политика безопасности
- В) Информационная безопасность
- Г) Защита информации

24. *Аутентичность связана:*

- А) С доказательством авторства документа
- Б) С проверкой прав доступа

В) С изменением авторства документа

Г) С контролем целостности данных

25. *Что не рассматривается в политике безопасности?*

А) Требуемый уровень защиты данных

Б) Роли субъектов информационных отношений

В) Анализ рисков

Г) Защищенность механизмов безопасности

26. *Исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или коммуникационных сетях с целью изменить или уничтожить программное обеспечение и /или данные, хранящиеся в автоматизированных системах – это:*

А) Троянская программа

Б) Компьютерный вирус

В) Программный вирус

Г) Вирус

27. *Какие вирусы заражают файлы-документы и электронные таблицы офисных приложений?*

А) Файловый вирус

Б) Сетевой вирус

В) Макро-вирус

Г) Загрузочный вирус

28. *Основная особенность компьютерных вирусов заключается:*

А) В возможности их самопроизвольного внедрения в различные объекты операционной системы

Б) В возможности нарушения информационной безопасности

В) В возможности заражения окружающих

Г) В их постоянном существовании

29. *Первый сетевой вирус появился:*

А) В начале 60-х гг.

Б) В начале 80-х гг.

В) В начале 70-х гг.

Г) В середине 60-х гг.

30. *По особенностям алгоритма работы вируса бывают*

А) Резидентные и стелс-вирусы

Б) Полиморфик-генераторы и загрузочные вирусы

В) Макро-вирусы и логические бомбы

Г) Утилиты скрытого администрирования

31. *«Маски» вирусов используются:*

А) Для поиска известных вирусов

Б) Для создания известных вирусов

В) Для уничтожения известных вирусов

Г) Для размножения вирусов

32. *Какой вирус самостоятельно выходил в сеть через модем и сохранял свою копию на удаленной машине?*

А) Elk Kloner

Б) Pervading Animal

В) Creeper

Г) Brain

33. *Евгений Касперский переориентировался на создание антивирусных программ после обнаружения на своем компьютере вируса:*

А) Chameleon

- Б) Cascade
- В) Eddie
- Г) Virdem

34. *Первый вирус, противодействовавший антивирусному программному обеспечению:*

- А) Eddie
- Б) DiskKiller
- В) Dir_II
- Г) Virdem

35. *Первый макровирус, поражающий документы MSWord:*

- А) GreenStripe
- Б) Wazzu
- В) Concept
- Г) DiskKiller

36. *Первый полиморфный вирус:*

- А) DiskKiller
- Б) Chameleon
- В) MtE
- Г) Brain

37. *Вирус 1987 года, заражающий только системные файлы Command.com, и уничтожающий всю информацию на текущем диске, - это:*

- А) Suriv
- Б) Jerusalem
- В) Lehigh
- Г) MtE

38. *\$189 – такую сумму предлагалось прислать тем пользователям, чей компьютер был заражен вирусом...*

- А) Aids Information Diskette
- Б) Cascade
- В) Eddie
- Г) MtE

39. *Первый сетевой вирус-червь, использующий протокол передачи данных FTP (1997 г.)*

- А) Homer
- Б) ShareFar
- В) BackOrifice
- Г) Червь Морриса

40. *Достаточно труднообнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода – это:*

- А) Полиморфик-вирусы
- Б) Стелс-вирусы
- В) Макро-вирусы
- Г) Конструкторы вирусов

41. *Угроза перехвата данных может привести:*

- А) К нарушению доступности данных
- Б) К нарушению доступности и целостности данных
- В) К нарушению целостности данных
- Г) К нарушению конфиденциальности данных

42. *Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным – это:*

- А) Аутентификация
- Б) Идентификация

- В) Аутентичность
- Г) Конфиденциальность

43. Черви, использующие для распространения системы мгновенного обмена сообщениями:

- А) IM-черви
- Б) P2P-черви
- В) Почтовые черви
- Г) IRC-черви

44. Что из перечисленного не является идентификатором при аутентификации?

- А) Пароль
- Б) Особенности поведения пользователя
- В) Персональный идентификатор
- Г) Секретный ключ

45. Постоянные пароли относятся к:

- А) Статической аутентификации
- Б) Временной аутентификации
- В) Устойчивой аутентификации
- Г) Постоянной аутентификации

46. Относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом – это:

- А) Закрытый ключ шифрования
- Б) Вирусная маска
- В) Электронная цифровая подпись
- Г) Открытый ключ шифрования

47. Какое управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах, и официального разрешения субъекта к информации соответствующего уровня конфиденциальности?

- А) Мандатное управление доступом
- Б) Принудительное управление доступом
- В) Дискретное управление доступом
- Г) Статистическое управление доступом

48. Резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об этом пользователю, это:

- А) Иммунизаторы
- Б) Блокировщики
- В) Сканеры
- Г) CRC-сканеры

49. Технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов, это:

- А) Эвристический анализ
- Б) Поведенческий анализ
- В) Анализ контрольных сумм
- Г) Поиск вирусов по запросу пользователя

50. Какое управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах, и официального разрешения субъекта к информации соответствующего уровня конфиденциальности?

- А) Мандатное управление доступом
- Б) Принудительное управление доступом

В) Дискретное управление доступом
Г) Статистическое управление доступом
ЭТАЛОН ДЛЯ ПРОВЕРКИ

1. Б	26. В
2. В	27. В
3. В	28. А
4. А	29. В
5. А	30. А
6. Б	31. А
7. Б	32. В
8. Г	33. Б
9. В	34. А
10. Б	35. В
11. А	36. Б
12. В	37. В
13. Г	38. А
14. А	39. А
15. А	40. А
16. Г	41. Г
17. Б	42. Б
18. Б	43. А
19. Б	44. Б
20. В	45. А
21. А	46. В
22. Б	47. А
23. Б	48. Б
24. А	49. А
25. Г	50. А

Критерии оценки:

- **оценка «отлично»** выставляется студенту, если правильно выполнено более 90% заданий;
- **оценка «хорошо»** выставляется студенту, если правильно выполнено более 70% заданий;
- **оценка «удовлетворительно»** выставляется студенту, если правильно выполнено более 50% заданий;
- **оценка «неудовлетворительно»** выставляется студенту, если правильно выполнено менее 50% заданий.

Составители

_____ Е.А. Позднова

Приложение 4

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

Кафедра прикладной математики,
информатики, физики и
методики преподавания

Контрольные вопросы к защите лабораторных работ по дисциплине «Информационная безопасность»

Контрольные вопросы к лабораторной работе №1

1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки одноалфавитных методов?
3. Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод из рассмотренных вы выберете? Обоснуйте свой выбор.
4. Целесообразно ли повторно применять для уже зашифрованного текста: метод многоалфавитного шифрования, метод Цезаря?

Контрольные вопросы к лабораторной работе №2

1. Чем отличается «псевдооткрытый» текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста?
2. Как зависит время вскрытия описанным способом подбора ключей от длины вероятного слова?
3. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?
4. В чем недостатки метода дешифрования с использованием протяжки вероятного слова?

Контрольные вопросы к лабораторной работе №5

1. Сравните основные алгоритмы описанные в работе?
2. Сравните эквивалентность прямого и обратного преобразований в алгоритмах?

Составители

_____ Е.А. Позднова

Приложение 4

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3	4
1	Вопросы к экзамену	Средство контроля, рассчитанное на выяснение объема знаний обучающегося по разделам, темам и т.п. дисциплины.	Вопросы по всем темам/разделам дисциплины
2	Итоговый тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
3	Контрольные вопросы к защите лабораторных работ	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных вопросов к каждой лабораторной работе