Комплект оценочных средств, используемых для проведения олимпиады профессионального мастерства по укрупненной группе специальностей СПО 10.00.00 Информационная безопасность

Всероссийская олимпиада профессионального мастерства

Фонд оценочных средств
Всероссийской олимпиады профессионального мастерства
по укрупненной группе специальностей СПО
10.00.00 Информационная безопасность
(код и наименование)

Содержание

1. Спецификация Фонда оценочных средств.

2. Паспорт практического задания «Перевод профессионального текста».

3. Паспорт практического задания «Задание по организации работы коллектива».

4. Паспорт практического задания инвариантной части практического задания 2 уровня.

5. Паспорт практического задания вариативной части практического задания 2 уровня.

6. Оценочные средства (демоверсии, включающие инструкции по выполнению)

7. Индивидуальные ведомости оценок результатов выполнения участником практических заданий I уровня

8. Индивидуальная сводная ведомость оценок результатов выполнения участником заданий I уровня

9. Индивидуальные ведомости оценок результатов выполнения участником практических заданий 2 уровня

10. Индивидуальная сводная ведомость оценок результатов выполнения участником заданий 2 уровня

11. Сводная ведомость оценок результатов выполнения участниками заданий олимпиады

12. Методические материалы

Спецификация Фонда оценочных средств

1. Назначение Фонда оценочных средств

1.1.Фонд оценочных средств (далее – ФОС) - комплекс методических и оценочных средств, предназначенных для определения уровня сформированности компетенций участников Всероссийской олимпиады профессионального мастерства обучающихся по специальностям среднего профессионального образования (далее – Олимпиада).

ФОС является неотъемлемой частью методического обеспечения процедуры проведения Олимпиады, входит в состав комплекта документов организационно-методического обеспечения проведения Олимпиады.

Оценочные средства – это контрольные задания, а также описания форм и процедур, предназначенных для определения уровня сформированности компетенций участников олимпиады.

1.2. На основе результатов оценки конкурсных заданий проводятся следующие основные процедуры в рамках Всероссийской олимпиады профессионального мастерства:

процедура определения результатов участников, выявления победителя олимпиады (первое место) и призеров (второе и третье места);

процедура определения победителей в дополнительных номинациях.

2.Документы, определяющие содержание Фонда оценочных средств

2.1. Содержание Фонда оценочных средств определяется на основе и с учетом следующих документов:

Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

приказа Министерства образования и науки Российской Федерации от 14 июня 2013 г. № 464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;

приказа Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199 «Об утверждении перечня специальностей среднего профессионального образования»;

приказа Министерства образования и науки РФ от 18 ноября 2015 г. № 1350 «О внесении изменений в перечни профессий и специальностей среднего профессионального образования, утвержденные приказом Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199»;

регламента организации и проведения Всероссийской олимпиады профессионального мастерства обучающихся по специальностям среднего профессионального образования, утвержденного директором федерального государственного бюджетного учреждения «Федеральный институт оценки качества образования» С.Н. Пономаренко 22 декабря 2016 г.;

приказа Министерства образования и науки Российской Федерации от 13 августа 2014 г. № 1000 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.02 Информационная безопасность телекоммуникационных систем;

приказа Министерства образования и науки Российской Федерации от 28 июля 2014 г. № 806 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по

специальности 10.02.03 Информационная безопасность автоматизированных систем;

приказа Министерства труда и социальной защиты РФ от 3 ноября 2016 г. № 608н «Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях»;

приказа Министерства труда и социальной защиты РФ от 15.09.2016 № 522н «Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах";

Регламента Финала национального чемпионата «Молодые профессионалы» (WORLDSKILLS RUSSIA).

3. Подходы к отбору содержания, разработке структуры оценочных средств и процедуре применения

3.1. Программа конкурсных испытаний Олимпиады предусматривает для участников выполнение заданий двух уровней.

Задания I уровня формируются в соответствии с общими и профессиональными компетенциями специальностей среднего профессионального образования.

Задания II уровня формируются в соответствии с общими и профессиональными компетенциями специальностей укрупненной группы 10.00.00 специальностей СПО.

Для лиц с ограниченными возможностями здоровья формирование заданий осуществляется с учетом типа нарушения здоровья.

3.2. Содержание и уровень сложности предлагаемых участникам заданий соответствуют федеральным государственным образовательным стандартам СПО, учитывают основные положения соответствующих

профессиональных стандартов, требования работодателей к специалистам среднего звена.

3.3. Задания 1 уровня состоят из тестового задания и практических задач.

3.4. Задание «Тестирование» состоит из теоретических вопросов, сформированных по разделам и темам.

Предлагаемое для выполнения участнику тестовое задание включает 2 части - инвариантную и вариативную, всего 40 вопросов.

Инвариантная часть задания «Тестирование» содержит 20 вопросов по пяти тематическим направлениям, из них 4 – закрытой формы с выбором ответа, 4 – открытой формы с кратким ответом, 4 - на установление соответствия, 4 - на установление правильной последовательности. Тематика, количество и формат вопросов по темам инвариантной части тестового задания едины для всех специальностей СПО.

Вариативная часть задания «Тестирование» содержит 20 вопросов не менее, чем по двум тематическим направлениям. Тематика, количество и формат вопросов по темам вариативной части тестового задания формируются на основе знаний, общих для специальностей, входящих в УГС 10.00.00, по которой проводится Олимпиада.

Алгоритм формирования инвариантной части задания «Тестирование» для участника Олимпиады единый для всех специальностей СПО.

Таблица 1

Алгоритм формирования содержания задания «Тестирование»

№ п\п	**Наименование темы вопросов**	**Кол-во вопросов**	**Формат вопросов**				
			Выбор	**Открытая**	**Вопрос на соотве**	**Вопрос на устан**	**Макс.**

			ответа	форма	тствие	овление послед.	балл
	Инвариантная часть тестового задания						
1	Информационные технологии в профессиональной деятельности	4	1	1	1	1	1
2	Оборудование, материалы, инструменты	4	1	1	1	1	1
3	Системы качества, стандартизации и сертификации	4	1	1	1	1	1
4	Охрана труда, безопасность жизнедеятельности, безопасность окружающей среды	4	1	1	1	1	1
5	Экономика и правовое обеспечение профессиональной деятельности	4	1	1	1	1	1
	ИТОГО:	**20**					**5**
	*Вариативный раздел тестового задания (специфика УГС)**						
1	*Тема «Термины и определения в области информационной безопасности»*	10	3	5	1	1	2
2	Тема «*Методы и средства*	10	-	2	6	2	3

	обеспечения информационной безопасности»						
	ИТОГО:	**20**					**5**
	ИТОГО:	**40**					**10**

* Распределение заданий по вариативной части тестового задания является примерной, рекомендуемой для возможного использования

Вопрос закрытой формы с выбором одного варианта ответа состоит из неполного тестового утверждения с одним ключевым элементом и множеством допустимых заключений, одно из которых являются правильным.

Вопрос открытой формы имеет вид неполного утверждения, в котором отсутствует один или несколько ключевых элементов, в качестве которых могут быть: число, слово или словосочетание. На месте ключевого элемента в тексте задания ставится многоточие или знак подчеркивания.

Вопрос на установление правильной последовательности состоит из однородных элементов некоторой группы и четкой формулировки критерия упорядочения этих элементов.

Вопрос на установление соответствия. Состоит из двух групп элементов и четкой формулировки критерия выбора соответствия между ними. Соответствие устанавливается по принципу 1:1 (одному элементу первой группы соответствует только один элемент второй группы). Внутри каждой группы элементы должны быть однородными. Количество элементов во второй группе должно соответствовать количеству элементов первой группы. Количество элементов как в первой, так и во второй группе должно быть не менее 4.

Выполнение задания «Тестирование» реализуется посредством применения прикладных компьютерных программ, что обеспечивает возможность генерировать для каждого участника уникальную последовательность заданий, содержащую требуемое количество вопросов из каждого раздела и исключающую возможность повторения заданий. Для лиц с ограниченными возможностями здоровья предусматриваются особые условия проведения конкурсного испытания.

При выполнении задания «Тестирование» участнику Олимпиады предоставляется возможность в течение всего времени, отведенного на выполнение задания, вносить изменения в свои ответы, пропускать ряд вопросов с возможностью последующего возврата к пропущенным заданиям.

3.5. Практические задания 1 уровня включают два вида заданий: задание «Перевод профессионального текста (сообщения)» и «Задание по организации работы коллектива».

3.6. Задание «Перевод профессионального текста (сообщения)» позволяет оценить уровень сформированности:

умений применять лексику и грамматику иностранного языка для перевода текста на профессиональную тему;

умений общаться (устно и письменно) на иностранном языке на профессиональные темы;

способность использования информационно-коммуникационных технологий в профессиональной деятельности.

Задание по переводу текста с иностранного языка на русский включает 2 задачи:

перевод текста, содержание которого включает профессиональную лексику (возможен вариант аудирования);

ответы на вопросы по тексту (аудирование, выполнение действия).

Объем текста на иностранном языке составляет (1500-2000) знаков.

Задание по переводу иностранного текста разработано на языках, которые изучают участники Олимпиады.

3.7. «Задание по организации работы коллектива» позволяет оценить уровень сформированности:

умений организации производственной деятельности подразделения;

умения ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий;

способности работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями;

способность использования информационно-коммуникационных технологий в профессиональной деятельности.

Задание по организации работы коллектива включает 2 задачи:

1. Задача по расчету времени, необходимому коллективу исполнителей для реализации проекта системы информационной безопасности в организации.

2. Задача по определению состава исполнителей для реализации проекта системы информационной безопасности в организации.

3.8. Задания II уровня - это содержание работы, которую необходимо выполнить участнику для демонстрации определённого вида профессиональной деятельности в соответствии с требованиями ФГОС и профессиональных стандартов с применением практических навыков, заключающихся в проектировании, разработке, выполнении работ или изготовлении продукта (изделия и т.д.) по заданным параметрам с контролем соответствия результата существующим требованиям.

Количество заданий II уровня, составляющих общую или вариативную часть, одинаковое для специальностей или УГС профильного направления Олимпиады.

3.9. Задания II уровня подразделяются на инвариантную и вариативную части.

3.10. Инвариантная часть заданий II уровня формируется в соответствии с общими и профессиональными компетенциями специальностей УГС, умениями и практическим опытом, которые являются общими для всех специальностей, входящих в УГС.

Инвариантная часть заданий II уровня представляет собой практическое задание, которые содержит 2- 3 задачи.

Количество оцениваемых задач, составляющих то или иное практическое задание, одинаковое для всех специальностей СПО, входящих в УГС, по которой проводится Олимпиада.

3.11. Вариативная часть задания II уровня формируется в соответствии со специфическими для каждой специальности, входящей в УГС профессиональными компетенциями, умениями и практическим опытом с учетом трудовых функций профессиональных стандартов.

Практические задания разработаны в соответствии с объектами и видами профессиональной деятельности обучающихся по конкретным специальностям, или подгруппам специальностей, входящим в УГС.

Вариативная часть задания II уровня содержит 2-3 задачи различных уровней сложности.

3.12. Для лиц с ограниченными возможностями здоровья определение структуры и отбор содержания оценочных средств осуществляется с учетом типа нарушения здоровья.

4. Система оценивания выполнения заданий

4.1.Оценивание выполнения конкурсных заданий осуществляется на основе следующих принципов:

соответствия содержания конкурсных заданий ФГОС СПО по специальностям, входящим в укрупненную группу специальностей, учёта требований профессиональных стандартов и работодателей;

достоверности оценки – оценка выполнения конкурсных заданий должна базироваться на общих и профессиональных компетенциях участников Олимпиады, реально продемонстрированных в моделируемых профессиональных ситуациях в ходе выполнения профессионального комплексного задания;

адекватности оценки – оценка выполнения конкурсных заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания;

надежности оценки – система оценивания выполнения конкурсных заданий должна обладать высокой степенью устойчивости при неоднократных (в рамках различных этапов Олимпиады) оценках компетенций участников Олимпиады;

комплексности оценки – система оценивания выполнения конкурсных заданий должна позволять интегративно оценивать общие и профессиональные компетенции участников Олимпиады;

объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений членов жюри.

4.2. При выполнении процедур оценки конкурсных заданий используются следующие основные методы:

метод экспертной оценки;

метод расчета первичных баллов;

метод расчета сводных баллов;

метод агрегирования результатов участников Олимпиады;

метод ранжирования результатов участников Олимпиады.

4.3. Результаты выполнения практических конкурсных заданий оцениваются с использованием следующих групп целевых индикаторов: основных и штрафных.

4.2. При оценке конкурсных заданий используются следующие основные процедуры:

процедура начисления основных баллов за выполнение заданий;

процедура начисления штрафных баллов за выполнение заданий;

процедура формирования сводных результатов участников Олимпиады;

процедура ранжирования результатов участников Олимпиады.

4.4. Результаты выполнения конкурсных заданий оцениваются по 100-балльной шкале:

за выполнение заданий I уровня максимальная оценка - 30 баллов: тестирование -10 баллов, практические задачи – 20 баллов (перевод текста) – 10 баллов, задание по организации работы коллектива – 10 баллов);

за выполнение заданий II уровня максимальная оценка - 70 баллов: общая часть задания – 35 баллов, вариативная часть задания – 35 баллов).

4.5. Оценка за задание «Тестирование» определяется простым суммированием баллов за правильные ответы на вопросы.

В зависимости от типа вопроса ответ считается правильным, если:

при ответе на вопрос закрытой формы с выбором ответа выбран правильный ответ;

при ответе на вопрос открытой формы дан правильный ответ;

при ответе на вопрос на установление правильной последовательности установлена правильная последовательность;

при ответе на вопрос на установление соответствия, если сопоставление произведено верно для всех пар.

Таблица 2

Структура оценки за тестовое задание

№ п\п	Наименование темы вопросов	Кол-во вопросов	Количество баллов				
			Вопрос на выбор ответа	Открытая форма вопроса	Вопрос на соответствие	Вопрос на установление послед.	Макс. балл
	Инвариантная часть тестового задания						
1	Информационные технологии в профессиональной деятельности	4	0,1	0,2	0,3	0,4	1

2	Оборудование, материалы, инструменты	4	0,1	0,2	0,3	0,4	1
3	Системы качества, стандартизации и сертификации	4	0,1	0,2	0,3	0,4	1
4	Охрана труда, безопасность жизнедеятельности, безопасность окружающей среды	4	0,1	0,2	0,3	0,4	1
5	Экономика и правовое обеспечение профессиональной деятельности	4	0,1	0,2	0,3	0,4	1
	ИТОГО:	**20**					**5**
	Вариативный раздел тестового задания (специфика УГС)						
1	*Тема «Термины и определения в области информационной безопасности»*	10	*0,3*	*1,0*	*0,3*	*0,4*	*2*
2	Тема «*Методы и средства обеспечения информационной безопасности»*	10	-	*0,4*	*1,8*	*0,8*	*3*
	ИТОГО:	**20**					**5**
	ИТОГО:	**40**					**10**

4.6. Оценивание выполнения практических конкурсных заданий I уровня осуществляется в соответствии со следующими целевыми индикаторами:

а) основные целевые индикаторы:

качество выполнения отдельных задач задания;

качество выполнения задания в целом.

б) штрафные целевые индикаторы, начисление (снятие) которых производится за нарушение условий выполнения задания (в том числе за нарушение правил выполнения работ).

Критерии оценки выполнения практических конкурсных заданий представлены в соответствующих паспортах конкурсного задания.

4.7. Максимальное количество баллов за практические конкурсные задания I уровня: «Перевод профессионального текста (сообщения)» составляет 10 баллов.

4.8. Оценивание конкурсного задания «Перевод профессионального текста» осуществляется следующим образом:

1 задача - перевод текста - 5 баллов;

2 задача – ответы на вопросы, выполнение действия, инструкция на выполнение которого задана в тексте или выполнение задания на аудирование – 5 баллов;

Критерии оценки являются едиными для всех УГС СПО.

При выполнении 2 задачи в содержание критериев могут быть внесены дополнения (изменения) касающиеся конкретной УГС, которые не влияют на удельный вес каждого критерия.

Таблица 3

Критерии оценки 1 задачи письменного перевода текста

№	Критерии оценки	Количество баллов
1.	Качество письменной речи	0-3
2.	Грамотность	0-2

По критерию «Качество письменной речи» ставится:

3 балла – текст перевода полностью соответствует содержанию оригинального текста; полностью соответствует профессиональной стилистике и направленности текста; удовлетворяет общепринятым нормам русского языка, не имеет синтаксических конструкций языка оригинала и несвойственных русскому языку выражений и оборотов. Все профессиональные термины переведены правильно. Сохранена структура оригинального текста. Перевод не требует редактирования.

2 балла - текст перевода практически полностью (более 90% от общего объема текста) – понятна направленность текста и его общее содержание соответствует содержанию оригинального текста; в переводе присутствуют 1-4 лексические ошибки; искажен перевод сложных слов, некоторых сложных устойчивых сочетаний, соответствует профессиональной стилистике и направленности текста; удовлетворяет общепринятым нормам русского языка, не имеет синтаксических конструкций языка оригинала и несвойственных русскому языку выражений и оборотов. Присутствуют 1-2 ошибки в переводе профессиональных терминов. Сохранена структура оригинального текста. Перевод не требует редактирования.

1 балл – текст перевода лишь на 50% соответствует его основному содержанию: понятна направленность текста и общее его содержание; имеет пропуски; в переводе присутствуют более 5 лексических ошибок; имеет недостатки в стиле изложения, но передает основное содержание оригинала,

перевод требует восполнения всех пропусков оригинала, устранения смысловых искажений, стилистической правки.

0 баллов – текст перевода не соответствует общепринятым нормам русского языка, имеет пропуски, грубые смысловые искажения, перевод требует восполнения всех пропусков оригинала и стилистической правки.

По критерию «Грамотность» ставится

2 балла – в тексте перевода отсутствуют грамматические ошибки (орфорграфические, пунктуационные и др.);

1 балл – в тексте перевода допущены 1-4 лексические, грамматические, стилистические ошибки (в совокупности);

0 баллов – в тексте перевода допущено более 4 лексических, грамматических, стилистических ошибок (в совокупности).

Таблица 4

Критерии оценки 2 задачи

«Перевод профессионального текста (сообщения)»

(ответы на вопросы, аудирование, выполнение действия)

№	Критерии оценки	Количество баллов
1.	Глубина понимания текста	0-4
2.	Независимость выполнения задания	0-1

По критерию «Глубина понимания текста» ставится:

4 балла – участник полностью понимает основное содержание текста, умеет выделить отдельную, значимую для себя информацию, догадывается о значении незнакомых слов по контексту;

3 балла – участник не полностью понимает основное содержание текста, умеет выделить отдельную, значимую для себя информацию, догадывается о значении более 80% незнакомых слов по контексту;

2 балла – участник не полностью понимает основное содержание текста, умеет выделить отдельную, значимую для себя информацию, догадывается о значении более 50% незнакомых слов по контексту;

1 балл - участник не полностью понимает основное содержание текста, с трудом выделяет отдельные факты из текста, догадывается о значении менее 50% незнакомых слов по контексту

0 баллов - участник не может выполнить поставленную задачу.

По критерию «Независимость выполнения задания» ставится:

1 балл – участник умеет использовать информацию для решения поставленной задачи самостоятельно без посторонней помощи;

0 баллов - полученную информацию для решения поставленной задачи участник может использовать только при посторонней помощи.

4.9. Максимальное количество баллов за выполнение задания «Задание по организации работы коллектива» - 10 баллов.

Оценивание выполнения задания 1 уровня **«Задание по организации работы коллектива»** осуществляется следующим образом:

Критерии оценки:

а) Задача выполнена полностью за отведенное время – 10 баллов;

б) штрафные баллы:

несущественные погрешности в расчетах – минус 2 балла;

существенные погрешности в расчетах – минус 8 баллов;

частичное правильное решение задачи – минус 5 баллов.

Полностью отсутствие решения задачи – минус 10 баллов.

4.10. Оценивание выполнения конкурсных заданий II уровня может осуществляться в соответствии со следующими целевыми индикаторами:

а) основные целевые индикаторы:

качество выполнения отдельных задач задания;

качество выполнения задания в целом;

скорость выполнения задания (в случае необходимости применения),

б) штрафные целевые индикаторы:

нарушение условий выполнения задания;

негрубые нарушения технологии выполнения работ;

негрубые нарушения санитарных норм.

Значение штрафных целевых индикаторов уточнено по каждому конкретному заданию.

Критерии оценки выполнения профессионального задания представлены в соответствующих паспортах конкурсных заданий.

4.11. Максимальное количество баллов за конкурсные задания II уровня 70 баллов.

4.12. Максимальное количество баллов за выполнение инвариантной части практического задания II уровня - 35 баллов.

Оценивание выполнения данного задания осуществляется следующим образом:

а) основные целевые индикаторы:

качество выполнения отдельных задач задания;

качество выполнения задания в целом;

скорость выполнения задания (в случае необходимости применения),

б) штрафные целевые индикаторы:

нарушение условий выполнения задания;

негрубые нарушения технологии выполнения работ;

негрубые нарушения санитарных норм.

4.13. Максимальное количество баллов за выполнение вариативной части практического задания II уровня - 35 баллов.

Оценивание выполнения данного задания осуществляется следующим образом:

а) основные целевые индикаторы:

качество выполнения отдельных задач задания;

качество выполнения задания в целом;

скорость выполнения задания (в случае необходимости применения),

б) штрафные целевые индикаторы:

нарушение условий выполнения задания;

негрубые нарушения технологии выполнения работ;

негрубые нарушения санитарных норм.

5. Продолжительность выполнения конкурсных заданий

Рекомендуемое максимальное время, отводимое на выполнения заданий в день – 8 часов (академических).

Рекомендуемое максимальное время для выполнения 1 уровня:

тестовое задание – 1 час (астрономический);

перевод профессионального текста, сообщения – 1 час (академический);

решение задачи по организации работы коллектива - 1 час (академический).

Рекомендуемое максимальное время для выполнения отдельных заданий 2 уровня- 2 часа.

6. Условия выполнения заданий. Оборудование

6.1.Для выполнения задания «Тестирование» необходимо соблюдение следующих условий:

наличие компьтерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть;

наличие специализированного программного обеспечения.

Должна быть обеспечена возможность единовременного выполнения задания всеми участниками Олимпиады.

6.2.Для выполнения заданий «Перевод профессионального текста» необходимо соблюдение следующих условий:

наличие компьютерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть;

Должна быть обеспечена возможность единовременного выполнения задания всеми участниками Олимпиады.

6.3. Для выполнения заданий «Задание по организации работы коллектива» необходимо соблюдение следующих условий:

наличие компьютерного класса (классов) или других помещений, в котором размещаются персональные компьютеры, объединенные в локальную вычислительную сеть;

6.4. Выполнение конкурсных заданий II уровня проводится на разных производственных площадках, используется специфическое оборудование. Требования к месту проведения, оборудованию и материалов указаны в паспорте задания.

6.5. Для лиц с ограниченными возможностями здоровья предусматриваются особые условия выполнения заданий.

7. Оценивание работы участника олимпиады в целом

7.1. Для осуществления учета полученных участниками олимпиады оценок заполняются индивидуальные сводные ведомости оценок результатов выполнения заданий I и II уровня.

7.2. На основе указанных в п.7.1.ведомостей формируется сводная ведомость, в которую заносятся суммарные оценки в баллах за выполнение заданий I и II уровня каждым участником Олимпиады и итоговая оценка выполнения профессионального комплексного задания каждого участника Олимпиады, получаемая при сложении суммарных оценок за выполнение заданий I и II уровня.

7.3. Результаты участников заключительного этапа Всероссийской олимпиады ранжируются по убыванию суммарного количества баллов, после чего из ранжированного перечня результатов выделяют 3 наибольших результата, отличных друг от друга – первый, второй и третий результаты.

При равенстве баллов предпочтение отдается участнику, имеющему лучший результат за выполнение заданий II уровня.

Участник, имеющий первый результат, является победителем Всероссийской олимпиады. Участники, имеющие второй и третий результаты, являются призерами Всероссийской олимпиады.

Решение жюри оформляется протоколом.

7.4.Участникам, показавшим высокие результаты выполнения отдельного задания, при условии выполнения всех заданий, устанавливаются дополнительные поощрения.

Номинируются на дополнительные поощрения:

участники, показавшие высокие результаты выполнения заданий профессионального комплексного задания по специальности или подгруппам специальностей УГС;

участники, показавшие высокие результаты выполнения отдельных задач, входящих в профессиональное комплексное задание;

участники, проявившие высокую культуру труда, творчески подошедшие к решению заданий.

1. Введение

Всероссийская олимпиада профессионального мастерства обучающихся по специальности 10.02.03 «Информационная безопасность автоматизированных систем» среднего профессионального образования включает выполнение теоретического и профессионального конкурсных заданий. Содержание конкурсных заданий соответствует федеральному государственному образовательному стандарту среднего профессионального образования по специальности 10.02.03 «Информационная безопасность автоматизированных систем», конкурсные задания разработаны с учётом основных требований работодателей. Теоретическое задание представляется в виде тестов и выполняется на компьютере. Теоретическое задание включает в себя вопросы, охватывающие содержание общепрофессиональных дисциплин и профессиональных модулей по специальности 10.02.03 «Информационная безопасность автоматизированных систем»:

-основы информационной безопасности;
-технические средства информатизации;
-сети и системы передачи информации;
- операционные системы;
-электроника и схемотехника;
-основы алгоритмизации и программирования;
-базы данных;
- ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем;
- ПМ. 02 Применение программно-аппаратных средств обеспечения информационной
безопасности в автоматизированных системах.
Теоретическое задание насчитывает 270 вопросов.
Вопросы тестового задания могут быть нескольких типов:
- Множественный выбор с одним или несколькими вариантами ответов;
- Вопросы на соответствие;
- Открытые вопросы (требуется ввод ответа).
Содержание профессионального задания нацеливает участников Всероссийской
олимпиады на демонстрацию видов профессиональной деятельности, в соответствии с
профессиональными модулями по специальности 10.02.03 «Информационная безопасность автоматизированных систем»:
- ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем;
- ПМ. 02 Применение программно-аппаратных средств обеспечения информационной
безопасности в автоматизированных системах.
Профессиональное задание выполняется участниками Всероссийской олимпиады с
применением теоретических знаний и практических навыков, заключающихся в
проектировании, разработке решения по заданным параметрам с практическим
выполнением задания и контролем соответствия результата проектным показателям.

2. Теоретическое задание

Операционные системы

1. Безопасная информационная система – это система, которая …

а. проникает в компьютер под видом легального пользователя;
б. надежно хранит информацию и гарантирует неизменность данных;
в. использует чужие пароли, захватывает и анализирует сетевые сообщения.

2. Конфиденциальность – гарантия того, что …

а. обеспечивается запрет изменять, модифицировать, разрушать или создавать
данные;
б. авторизованные пользователи всегда получат доступ к данным;

в. секретные данные будут доступны только тем пользователям, которым этот
доступ разрешен.

**3. Как можно интерпретировать свойство конфиденциальности, примененное к
устройству печати?**

а. устройство готово к использованию всякий раз, когда в этом возникает необходимость;
б. неизменность параметров настройки данного устройства;
в. доступ к устройству имеют только те пользователи, которым этот доступ разрешен.

**4. Любое действие, которое направлено на нарушение конфиденциальности,
целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети, называется …**

5. Доступность – гарантия того, что …

а. авторизованные пользователи всегда получат доступ к данным;
б. секретные данные будут доступны только тем пользователям, которым этот
доступ разрешен;
в. обеспечивается запрет изменять, модифицировать, разрушать или создавать
данные.

**6. Вероятная оценка величины возможного ущерба, который может понести
владелец информационного ресурса в результате успешно проведенной атаки–
это …**

**7. Вставьте пропущенные слова в утверждении: «значение риска тем выше, чем
… уязвимой является существующая система безопасности и чем … вероятность реализации атаки».**

а. … менее … ниже;
б. …. более … выше;
в. … менее … выше.

8. Целостность – гарантия того, что …

а. авторизованные пользователи всегда получат доступ к данным;
б. обеспечивается запрет изменять, модифицировать, разрушать или создавать
данные;
в. секретные данные будут доступны только тем пользователям, которым этот
доступ разрешен.

9. Как можно интерпретировать свойство доступности, примененное к устройству печати?

а. устройство готово к использованию всякий раз, когда в этом возникает необходимость;
б. неизменность параметров настройки данного устройства;
в. доступ к устройству имеют только те пользователи, которым этот доступ разрешен.

10. Что из перечисленного можно отнести к типовым функциональным дефектам ОС, которые могут привести к созданию каналов утечки данных?

а. идентификация;
б. список паролей;
в. разрыв связей.

11. Угрозы могут быть разделены на …

а. законные и незаконные;
б. легальные и нелегальные;
в. умышленные и неумышленные.

12. Незаконное проникновение может быть реализовано …

а. следствием низкой квалификации лояльных сотрудников;
б. следствием отказа всего файлового сервера;
в. через уязвимые места в системе безопасности.

13. К какому роду угроз относятся последствия ненадежной работы программных и аппаратных средств системы?

а. неумышленные угрозы;
б. незаконное проникновение;
в. незаконное проникновение в один из компьютеров сети под видом легального пользователя.

14. Какие угрозы могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия?

а. незаконные;
б. легальные;
в. умышленные.

15. «Подслушивание» внутрисетевого трафика относится к …

а. нелегальным угрозам;
б. умышленным угрозам;
в. атаке.

16. Разрушение системы с помощью программ-вирусов относится к …

а. нелегальным угрозам;
б. умышленным угрозам;
в. атаке.

17. Использование специальных программ, которые работают путем перебора слов из некоторого файла, позволяет …

а. подобрать пароль;
б. «подслушать» внутрисетевой трафик;

в. получить доступ ко всем ресурсам системы.

18. Программа, работающая без ведома хозяина данного компьютера и выполняющая действия, заданные злоумышленником, называется …

19. Программа, которая маскируется под какую-нибудь полезную утилиту или
игру и производит действия, разрушающие систему, называется …

а. «троянский конь»;
б. системная программа;
в. утилита.

20. Вирусы могут привести к …

а. захвату и анализу сетевых сообщений;
б. повреждению или полной утрате информации;
в. незаконному проникновению в один из компьютеров сети под видом легального пользователя.

21. Нелегальные действия легального пользователя …

а. это незаконный мониторинг сети, захват и анализ сетевых сообщений;
б. вызываются ошибочными действиями лояльных сотрудников;
в. исходят от легальных пользователей сети, которые пытаются выполнять действия, выходящие за рамки их должностных обязанностей.

22. Что предотвращает доступ к сети нежелательных лиц и разрешает вход для
легальных пользователей?

а. авторизация;
б. аудит;
в. аутентификация.

23. Когда пользователь вводит свои идентификатор и пароль, которые автономно
обрабатываются операционной системой?

а. при авторизации доступа;
б. при локальной аутентификации;
в. при аудите.

24. Когда контролируется доступ легальных пользователей к ресурсам системы,
предоставляя каждому из них те права, которые ему были определены администратором?

а. при авторизации доступа;
б. при локальной аутентификации;
в. при аудите.

25. Фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам – это …

26. Аудит используется для того, чтобы …

а. вся информация делилась на уровни в зависимости от степени секретности;
б. засекать даже неудачные попытки «взлома» системы;
в. пользователи не имели возможности изменить уровень доступности информации.

27. Безопасная информационная система обладает следующими свойствами:

*а. конфиденциальности, б. доступности , в. целостности***.**

Каждому свойству поставьте в соответствие его определение:

А. … – это гарантия того, что авторизованные пользователи всегда получат доступ к данным

Б. … – это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные

В. … – это гарантия того, что секретные данные будут доступны только авторизованным пользователям

28. На каких двух компонентах базируется сетевая безопасность?

а. защита данных в момент их передачи по линиям связи ;

б. защита от несанкционированного удаленного доступа в сеть;

в. предотвращение доступа к сети нежелательных лиц;

г. разрешение входа для легальных пользователей.

29. С помощью каких биохарактеристик аутентифицируемый может доказать

свою идентичность?

а. электронная магнитная карта;

б. отпечатки пальцев;

в. рисунок радужной оболочки глаза;

30. Термин «аутентификация» в переводе с латинского означает …

Основы информационной безопасности

1. Установите соответствие между основными методами обеспечения информационной безопасности.

а. сервисы сетевой безопасности; б. теоретические методы; в. инженерно – технические методы; г. правовые методы.	А. защита авторских прав; Б. протоколирование и аудит; В. обоснование корректности и адекватности систем обеспечения ИБ; Г. защита информации от утечки по техническим каналам.

2. Установление полномочий субъектов для последующего контроля санкционированного использования ресурсов, доступных в системе это …

а. разграничение полномочий;

б. разграничение доступа;

в. аутентификация;

г. аудит.

3. Продолжите предложение

Принято выделять два основных метода разграничения доступа: …

4. Продолжите предложение

… выполняет функции разграничения информационных потоков на границе защищаемой автоматизированной системы.

5. Механизм подтверждения подлинности и целостности цифровых документов

а. пароль;

б. аутентификация пользователей;

в. цифровая подпись;

г. асимметричные криптосистемы.

6. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного

характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

а. информационная безопасность;

б. информационная война;

в. информационный ресурс;

г. конфиденциальность информации.

7. Ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

а. получение информации;

б. доступ к информации;

в. защита информации;

г. обработка информации.

8. Доступ к информации, не нарушающий установленные правила разграничения доступа

а. анонимный доступ к информации;

б. несанкционированный доступ к информации;

в. открытый доступ к информации;

г. санкционированный доступ к информации.

9. Продолжите фразу: «Статус, предоставленный данным и определяющий

требуемую степень их защиты – это …»

Запишите ответ: _____

10. Некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.

а. целостность системы;

б. конфиденциальность системы;

в. уязвимость системы;

г. защищенность системы.

11. Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или)

в
сопроводительной документации на него.
а. гриф секретности;
б. степень секретности;
в. цифровая подпись;
г. реквизиты секретности.
12. Продолжите фразу: «Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе
составляющая секреты производства «ноу-хау»), которая имеет действительную
или потенциальную коммерческую ценность в силу неизвестности ее третьим
лицам – это …»
Запишите ответ: _____
13. К формам защиты информации не относится…
а. аналитическая;
б. правовая;
в. организационно-техническая;
г. страховая.
14. Информация, составляющая государственную тайну, не может иметь гриф…
а. «для служебного пользования»;
б. «секретно»;
в. «совершенно секретно»;
г. «особой важности».
15. Элементы знака охраны авторского права:
а. буквы С в окружности или круглых скобках;
б. буквы Р в окружности или круглых скобках;
в. наименования (имени) правообладателя;
г. наименование охраняемого объекта.
16. Укажите соответствие для всех 4 вариантов ответа:

а. комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных	А. защита информации от утечки по акустическому каналу; Б. защита информации от утечки по визуально-оптическому каналу; В. защита информации от утечки по электромагнитным каналам; Г. защита информации от утечки по

полей побочного характера и наводок; б. комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов; в. комплекс мероприятий, исключающих или уменьшающих	материально-вещественному каналу.

возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей; г. комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

17. Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов
и объектов между собой - это..."
Запишите ответ: _____
18. Какие законы существуют в России в области компьютерного права? Выберите несколько из 4 вариантов ответа:
а. о государственной тайне;
б. об авторском праве и смежных правах;
в. о гражданском долге;
г. о правовой охране программ для ЭВМ и БД.
19. Укажите соответствие для всех 4 вариантов ответа:

а. наука о скрытой передаче информации путем сохранения в тайне самого факта передачи; б. наука скрывающая содержимое секретного сообщения; в. наука, занимающаяся методами шифрования и дешифрования; г. наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа.	А. стеганография; Б. криптоанализ; В. криптология; Г. криптография.

20. Расположите в порядке возрастания ущерб от атаки фирмы
а. фирма прекращает существование;
б. ущерб от атаки есть, но он незначителен, основные финансовые операции и
положение фирмы на рынке не затронуты;
в. значительные потери на рынке и в прибыли, от фирмы уходит ощутимая часть клиентов;
г. раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме.
21. Преднамеренно внесенные в ПО функциональные объекты, которые

при
определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации называются
а. вирус;
б. троян;
в. вредоносное ПО;
г. программная закладка.
22. Биометрические характеристики относятся к средствам…
а. аутентификации;
б. идентификации;
в. протоколирования ;
г. аудита.
23. Сбор и накопление информации о событиях, происходящих в информационной системе, называется…
а. экранированием;
б. аудитом;
в. протоколированием;
г. криптографией.
24. Укажите в правильном порядке этапы допуска в вычислительную систему
а. установление подлинности;
б. идентификация;
в. определение полномочий для последующего контроля и разграничения доступа.
25. Восстановите последовательность действий процедуры опознания с использованием простого пароля
а. система запрашивает пароль;
б. пользователь вводит пароль;
в. пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;
г. система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.
26. Основные угрозы доступности информации:
а. непреднамеренные ошибки пользователей;
б. хакерская атака;
в. разрушение или повреждение помещений;
г. перехват данных.
27. Разделы современной криптографии:
а. симметричные криптосистемы;
б. криптосистемы с открытым ключом;
в. управление паролями;

г. управление ключами;

28. Основные угрозы конфиденциальности информации:

а. маскарад;

б. переадресовка;

в. перехват данных;

г. злоупотребления полномочиями.

29. Преднамеренная угроза безопасности информации

а. кража;

б. наводнение;

в. повреждение кабеля, по которому идет передача, в связи с погодными условиями;

г. ошибка разработчика.

30. Вставьте пропущенное слово:

Информация может быть защищена без аппаратных и программных средств защиты с
помощью _____ преобразований.

Запишите ответ:

_____

Технические средства информатизации

**1. Сетевое устройство, объединяющее сети на существенно разных программных и
аппаратных платформах, называется**

а. шлюз;

б. мост;

в. концентратор.

2. Что может стать причиной сброса настроек в микросхеме BIOS?

а. действие вируса типа Kido;

б. разгон процессора;

в. переустановка ОС.

3. Единица измерения частоты дискретизации -

а. Мб;

б. Кб;

в. Гц;

г. Кц.

4. Качество кодирования непрерывного звукового сигнала зависит:

а. от частоты дискретизации и глубины кодирования;

б. от глубины цвета и разрешающей способности монитора;

в. от международного стандарта кодирования.

5. Совокупность условий и правил обмена информацией называется ...

а. выделенным каналом связи;

б. компьютерной сетью;

в. протоколом.

6. Укажите, где нельзя хранить резервные копии?

а. запись резервных данных на компактные диски;

б. запись резервных данных на жёсткий диск компьютера;

в. внутри локальной сети;
г. запись резервных данных на FTP-серверы;
д. запись резервных данных на любое USB-совместимое устройство (такое, как флэшкарта или внешний жёсткий диск).

7. Как называется процедура извлечения информации с запоминающего устройства в случае, когда она не может быть прочитана обычным способом.

а. восстановление данных;
б. образ;
в. резервное копирование.

8. Многопроводная шина информационного обмена внутри материнской платы называется:

а. портом;
б. магистралью;
в. адаптером;
г. линией внутренней связи.

9. Какие из накопителей информации применяемые в составе технических средств информации классифицированы верно?

а. по способу хранения информации выделяют: накопители прямого, последовательного и блочного доступа, а так же оптические;
б. по типу устройства хранения информации выделяют: встраиваемые (внутренние), внешние, автономные, мобильные (носимые) и др;
в. по виду носителя информации выделяют: магнитоэлектрические накопители, встраиваемые накопители, накопители блочного доступа.

10. Данное устройство выполняет основную работу по переработке информации, а также все арифметические действия, логические операции, сравнение данных и т. д.

а. арифметико - логическое устройство;
б. устройство управления;
в. регистр;
г. транзистор.

11. Данное устройство обеспечивает организацию выполнения программы обработки информации и согласованное взаимодействие всех узлов машин

а. арифметико - логическое устройство;
б. устройство управления;
в. регистр;
г. транзистор;

12. Технические средства информатизации - это ...

а. совокупность систем, машин, приборов, механизмов, устройств и прочих видов оборудования, предназначенных для автоматизации различных технологических процессов информатики, причем таких, выходным продуктом которых является информация, используемые для удовлетворения информационных потребностей в разных областях деятельности общества;
б. электронное устройство, выполненное в виде платы расширения (может быть интегрирован в системную плату) с разъемом для подключения к линии связи;
в. средство информации.

13. Сетевой адаптер - это:

а. специальная программа, через которую осуществляется связь нескольких компьютеров;
б. специальное аппаратное средство для эффективного взаимодействия персональных
компьютеров сети;
в. специальная система управления сетевыми ресурсами общего доступа;
г. система обмена информацией между компьютерами по локальным сетям.

**14. Для соединения компьютеров в сетях используются кабели различных типов. По
какому из них передаётся информация, закодированная в пучке света.**

а. витая пара;
б. телефонный;
в. коаксиальный;
г. оптико – волоконный.

15. Домен-это...

а. часть адреса, определяющая адрес компьютера пользователя в сети;
б. название программы, для осуществления связи между компьютерами;
в. название устройства, осуществляющего связь между компьютерами;
г. единица скорости информационного обмена.

16. Укажите верное(ые) высказывание(я):

а. внешняя память - это память высокого быстродействия и ограниченной емкости;
б. внешняя память предназначена для долговременного хранения информации
независимо от того, работает ЭВМ или нет;
в. внешняя память предназначена для долговременного хранения информации,
только когда работает ЭВМ.

**17. Как называется содержимое энергонезависимой памяти компьютера или любого
цифрового вычислительного устройства.**

а. прошивкой;
б. конфигурация устройства;
в. моддинг.

18. Отличительными особенностями компьютерного вируса являются:
а. значительный объем программного кода;
б. необходимость запуска со стороны пользователя;
в. способность к повышению помехоустойчивости операционной системы;
г. маленький объем; способность к самостоятельному запуску и многократному
копированию кода, к созданию помех корректной работе компьютера.
19. Загрузочные вирусы характеризуются тем, что:
а. поражают загрузочные сектора дисков;
б. поражают программы в начале их работы;
в. запускаются при загрузке компьютера;
г. изменяют весь код заражаемого файла;
д. всегда меняют начало и длину файла.
**20. Автоматизированное, отдельно поставляемое программное средство, используемое
для устранения проблем в программном обеспечении или изменения его функционала называется**
а. автоматическое программное обеспечение;
б. заплатка или патч;
в. деинсталляция программного обеспечения.
21. Назовите наиболее популярный формат для хранения несжатых аудио данных
а. MPEG;
б. MP 3;
в. JPEG;
г. WAV.
**22. Устройство, принимающее сигнал из одного порта и распределяющее его по всем
остальным портам, называется**
а. маршрутизатор;
б. коммутатор;
в. шлюз;
г. концентратор.
**23. Шина, предназначенная для обмена цифровой информацией между ПК и другими
электронными устройствами, особенно для подключения жёстких дисков и
устройств обработки аудио- и видеоинформации?**
а. шина VESA;
б. шина AGP;
в. шина SCSI;
г. шина IEEE 1394.
24. Что является характеристикой монитора? ...
а. цветовое разрешение
б. тактовая частота

в. дискретность
г. время доступа к информации

25. Что определяется произведением глубины адресного пространства на количество
линий ввода/вывода?

а. объём микросхемы памяти;
б. быстродействие микросхемы динамической памяти;
в. циклограмма;
г. разрядность шины ввода/вывода.

26. Что определяется суммой времени последовательного выполнения элементарных
действий между 2-мя операциями чтения либо записи данных?

а. быстродействие микросхемы динамической памяти;
б. циклограмма;
в. разрядность шины ввода/вывода;
г. объём микросхемы памяти.

27. Количество бит информации, которое хранится в ячейках памяти?

а. объём микросхемы памяти;
б. глубина адресного пространства;
в. банк памяти;
г. верного ответа нет.

28. Какое устройство обеспечивает наиболее полную защиту от перебоев в сети
электропитания?

а. сетевой фильтр;
б. линейный стабилизатор;
в. источник бесперебойного питания.

29. Как называется точная копия всего раздела или носителя (устройства),
хранящаяся в одном файле

а. образ;
б. записанный диск;
в. раздел жесткого диска;

30. Какое устройство предназначено для подключения к компьютерной сети?

а. центральный процессор;
б. блок питания;
в. видеокарта;
г. сетевая карта;
д. системная плата.

Сети и системы передачи информации

1. Аналоговый сигнал – это…

а. сигнал данных, у которого каждый из представляющих параметров описывается функцией дискретного времени и конечным множеством возможных значений;

б. сигнал данных, у которого каждый из представляющих параметров описывается функцией времени и непрерывным множеством возможных значений;
в. информационный сигнал, который может принимать лишь конечное число значений.

2. Амплитудная модуляция — …

а. вид модуляции, при которой изменяемым параметром несущего сигнала является его амплитуда;
б. вид аналоговой модуляции, при котором информационный сигнал управляет
частотой несущего колебания;
в. один из видов модуляции колебаний, при которой фаза несущего колебания
управляется информационным сигналом.

3. В каких единицах измеряется относительное напряжение?

а. в вольтах;
б. в милливольтах;
в. в децибелах.

4. Что определяет значение логической переменной при импульсном кодировании?

а. амплитуда сигнала;
б. фаза сигнала;
в. перепад напряжения.

5. Как называется информационный блок SDH?

а. кадр;
б. пакет;
в. блок;
г. сообщение.

6. Радиорелейная связь —….

а. один из видов спутниковой радиосвязи, основанный на многократной ретрансляции радиосигналов;
б. один из видов наземной радиосвязи, основанный на многократной ретрансляции радиосигналов;
в. один из видов наземной радиосвязи, основанный на сотовой связи.

7. Выберите утверждения, касающиеся глобальной сети:

а. соединяется с другими сетями, образуют одну всемирную сеть;
б. объединение множества локальных сетей и отдельных компьютеров;
в. охватывающая большие территории и включающая в себя большое число компьютеров;
г. все компьютеры выполняют одинаковые функции, нет преимущества ни у одного персонального компьютера.

8. Общий стандарт на представление и преобразование передаваемой информации по сети, название.

а. сервер-программа;
б. клиент-программа;

в. протокол;
г. интернет.

9. Комплекс аппаратных и программных средств, позволяющих компьютерам
обмениваться данными:

а. интерфейс;
б. магистраль;
в. компьютерная сеть;
г. адаптеры.

10. Укажите межсетевой протокол (протокол INTERNET) семейства протоколов
TCP/IP

а. ARP (Address Resolution Protocol);
б. IP (Internet Protocol);
в. ICMP (Internet Control Message Protocol).

11. Укажите уровень модели OSI, который не подписан на рисунке

а. информационный;
б. представительский;
в. коммутационный.

12. Цифровой сигнал — это…

а. сигнал данных, у которого каждый из представляющих параметров описывается функцией дискретного времени и конечным множеством возможных значений;
б. информационный сигнал, который может принимать лишь конечное число значений;
в. сигнал данных, у которого каждый из представляющих параметров описывается функцией времени и непрерывным множеством возможных значений.

13. Частотная модуляция— …

а. вид модуляции, при которой изменяемым параметром несущего сигнала является его амплитуда;
б. вид аналоговой модуляции, при котором информационный сигнал управляет частотой несущего колебания;
в. один из видов модуляции колебаний, при которой фаза несущего колебания
управляется информационным сигналом.

14. Какой из перечисленных видов трафика наиболее чувствителен к задержкам
электрического сигнала?

а. речевой;
б. видео;
в. все выше перечисленные.

15. Как называется единица скорости передачи информации в телеграфных сетях?

а. бонд;

б. байт;
в. бод;
г. бод/с.

16. Какие устройства образуют канал связи?

а. источник сообщения; передатчик сообщения, приемник сообщения;
б. источник сообщения; преобразователь сигнал - сообщение, передатчик; линия
связи;
в. приемник сообщения;
г. передатчик сигнала; приемник сигнала; приемник сообщения;
д. передатчик сообщения, линия связи, приемник сообщения.

17. Канал связи это – …

а. совокупность линий передачи данных и блоков взаимодействия, предназначенных для передачи данных между станциями данных;
б. средства односторонней передачи данных;
в. устройство преобразования кодов и представляющих их электрических сигналов при взаимодействии аппаратуры окончания канала данных и линий связи;
г. система односторонней связи, при которой передаваемое сообщение поступает на пейджер пользователя, извещая его о необходимости предпринять то или действие или просто информируя его о тех или иных текущих событиях.

18. Технические средства, связывающие компьютеры в сетях, называются…

а. хост-машинами;
б. пропускной способностью;
в. скоростью передачи информации;
г. каналами связи.

19. Служба FTP в Интернете предназначена:

а. для создания, приёма и передачи Web-страниц;
б. для удалённого управления техническими системами;
в. для приёма и передачи файлов любого формата;
г. для обеспечения работы телеконференций.

20. Группа компьютеров, связанных каналами передачи информации и находящимися в пределах здания называется:

а. глобальной компьютерной сетью;
б. информационной системой с гиперсвязями;
в. локальной компьютерной сетью;
г. электронной почтой.

21. Укажите протокол пересылки файлов стека протоколов TCP/IP

а. FTP (File Transfer Protocol);
б. ICMP (Internet Control Message Protocol);
в. IP (Internet Protocol).

22. Укажите уровень модели OSI, который не подписан на рисунке

а. информационный;

б. коммутационный;
в. транспортный.
23. Параметры виртуальных локальных сетей определяются стандартом:
а. IEEE 802.1;
б. IEEE 802.2;
в. IEEE 802.1Q;
г. IEEE 802.2Q;
д. IEEE 802.3Q.
24. Маршрутизацию между виртуальными локальными сетями обеспечивает:
а. транковое соединение между коммутаторами;
б. транковое или обычное соединение между коммутаторами;
в. транковое или обычное соединение между коммутатором и маршрутизатором;
г. только транковое соединение между коммутатором и маршрутизатором.
25. По умолчанию управляющей сетью является:
а. первая сеть VLAN 1;
б. сеть, которой назначили IP-адрес;
в. сеть расширенного диапазона идентификаторов VLAN;
г. сеть, определенная стандартом 802.1.
26. Кабель, представляющий собой световод на кремниевой или пластмассовой
основе, который защищен материалом с низким коэффициентом преломления
а. Витая пара
б. Оптоволоконный кабель
в. Коаксиальный кабель
27. После удаления одной из виртуальных локальных сетей приписанные к ней
порты будут иметь следующий статус:
а. порты перейдут в пассивное состояние;
б. порты административно выключены;
в. порты будут связанными с удаленной сетью, пока не будут переназначены другой виртуальной сети;
г. порты удаленной сети будут автоматически переназначены сети VLAN1.
28. Сколько широковещательных доменов существует в сети (см. рис.)?
VLAN1 VLAN2 VLAN3
Switch Switch
Router
Ответ запишите цифрой:
29. Метрики пути из Сети 1 в Сеть 2 и из Сети 3 в Сеть 1 (см. рисунок) составляют:
A B C
Сеть 1

2048кбит/с 64 кбит/с
F0/1 F0/1 Сеть 2 E0/1 Сеть 3
а. 50 и 1621;
б. 48 и 1562;
в. 49 и 1563;
г. 1562 и 50;
д. 1562 и 10.

30. В строке таблицы маршрутизации

• 192.168.4.48 [110/2344] via 200.50.50.10, 00:00:10, Serial1/1

via 200.50.50.10 означает: (выбрать два ответа)
а. адрес сети назначения;
б. адрес выходного интерфейса маршрутизатора на пути к сети назначения;
в. адрес входного интерфейса соседнего маршрутизатора на пути к сети назначения;
г. адрес запасного пути (feasible succcessor) к сети назначения;
д. адрес преемника (succcessor).

Электроника и схемотехника

1. Какие диоды работают в режиме электрического пробоя?
а. варикапы;
б. туннельные;
в. стабилитроны.

2. Укажите маркировку интегральной микросхемы.
а. КП103Е;
б. К140УД1Б ;
в. КН102Г.

3. В каком случае коэффициент усиления по мощности биполярного транзистора меньше или равен 1?
а. во всех случаях он больше 1;
б. в схеме с общим эмиттером ;
в. во всех случаях он меньше 1.

4. Для отрицательной обратной связи, применяемой в усилителях, сдвиг фаз
между входным напряжением и напряжением обратной связи равен
а. 0 градусов;
б. 90 градусов;
в. 180 градусов.

5. Какими причинами можно объяснить завал амплитудно-частотной характеристики УНЧ в области низких частот
а. собственными шумами;
б. реактивными элементами в схеме;
в. влиянием температуры.

6. Длительность формируемых мультивибратором прямоугольных импульсов
определяется
а. элементами RC-цепей;

б. величиной напряжения питания;
в. выбором транзисторов.

7. Какое электронное устройство имеет два устойчивых состояния?

а. мультивибратор;
б. блокинг-генератор;
в. триггер.

8. С какой целью выпрямительные диоды включают последовательно?

а. для уменьшения габаритов и массы;
б. чтобы использовать диоды с меньшим Uобрмах;
в. чтобы использовать диоды с меньшим Iпрсред.

9. Какое свойство p-n переходов используют в варикапах?

а. односторонняя электропроводность;
б. частотные свойства;
в. емкостные свойства.

10. Какие значения параметров стабилизатора предпочтительнее?

а. Rвых = 0,5 Ом, Кст и = 300;
б. Rвых = 0,5 Ом, Кст и = 100;
в. Rвых = 50 Ом, Кст и = 300.

11. Какой пробой опасен для p-n-перехода?

а. тепловой;
б. электрический;
в. тот и другой.

12. У какого транзистора входное сопротивление максимально?

а. у биполярного;
б. у полевого с затвором в виде p-n-перехода;
в. у МДП-транзистора.

13. Как влияют примесные зоны на процесс образования пар свободных носителей заряда в полупроводниках?

а. не влияют;
б. облегчают;
в. затрудняют.

14. В каком случае разрешенный энергетический уровень в атоме расщепляется
на большее количество уровней?

а. если атом имеет несколько электронов;
б. если атом входит в состав молекул;
в. если атом находится в кристалле.

15. Как влияет дефекты кристаллической решетки на проводимость кристалла?

а. не влияют;
б. увеличивают;
в. уменьшают.

16. Выходные двухтактные каскады УНЧ обычно работают в экономичном
режиме класса

а. А;
б. АВ;
в. В.

17. Какое из указанных свойств характерно для схемы ОК – эмиттерного повторителя?

а. коэффициент усиления по напряжению ≈ 1;
б. малое значение Rвх;
в. большое значение Rвых.

18. Для самовозбуждения автогенератора гармонических колебаний необходимо
выполнение условия

а. = К;
б. βК < 1;
в. βК ≥ 1.

19. Какой атом называется возбужденным?

а. атом, поглотивший один квант энергии;
б. атом, поглотивший один или несколько квантов энергии;
в. атом, из которого вырван электрон.

20. Почему с увеличением температуры увеличивается проводимость полупроводникового кристалла?

а. увеличивается количество пар свободных носителей заряда;
б. увеличивается длина свободного пробега электрон;
в. увеличивается ширина запрещенной зоны.

21. Отрицательная обратная связь в усилителе

а. уменьшает динамический диапазон;
б. уменьшает нелинейные искажения;
в. повышает коэффициент усиления.

22. В каком направлении включается эмиттерный и коллекторный p-n-переходы
биполярного транзистора?

а. это зависит от типа транзистора (n-p-n или p-n-p);
б. эмиттерный – в обратном, коллекторный – в прямом;
в. эмиттерный – в прямом, коллекторный – в обратном.

23. Каково соотношение величины обратного тока p-n- перехода и прямого тока?

а. Iобр>> Iпр;
б. Iобр << Iпр;
в. Iобр = Iпр.

24. В каких режимах находятся транзисторы VT1 и VT2 в устойчивых состояниях
триггера на транзисторах

а. VT1 и VT2 закрыты;
б. VT1 и VT2 открыты;
в. VT1 открыт, VT2 закрыт; VT1 закрыт, VT2 открыт.

25. Как измениться скважность q если увеличить длительность паузы

между импульсами

а. q увеличится;

б. q уменьшится;

в. q не изменится.

26. Какие микросхемы могут быть изготовлены без навесных элементов?

а. тонкопленочные;

б. толстопленочные;

в. полупроводниковые.

27. Как включается емкостной фильтр Сф?

а. параллельно нагрузкеRн;

б. последовательно с нагрузкой Rн;

в. параллельно вторичной обмотке трансформатора.

28. Назовите главное достоинство схемы трехфазного выпрямителя

а. малое значение тока диодов;

б. малое обратное напряжение диодов;

в. малая пульсация выпрямленного тока.

29. Определить правильный ответ в логическом выражении $X + X =$

а. 0;

б. 1;

в. X .

30. Определите коэффициент усиления по мощности трехкаскадного усилителя в

децибелах, если каждый каскад обеспечивает десятикратное усиление по напряжению

а. 60 ;

б. 100;

в. 1000.

Основы алгоритмизации и программирования

1. Что изменяет операция присваивания?

а. Значение переменной

б. Имя переменной

в. Тип переменной

г. Тип алгоритма

2. Свойством алгоритма является…

а. Цикличность

б. Результативность

в. Возможность изменения последовательности выполнения команд

г. Возможность выполнения алгоритма в обратном порядке

3. Укажите, какие из перечисленных понятий не относятся к основным группам

алгоритмов?

а. Линейные

б. Разветвляющиеся

в. Структурные

г. Циклические

4. Чему равно число 2.731E07

а. 2731000

б. 0,0000002731

в. 273100000

г. 27310000

5. Поменять значения переменных x и y не используя дополнительных переменных:

а. x=2y, y=x/2, x=x/2

б. x=x-y, y=y-x, y=y+x

в. x=x+y, y=x-y, x=x-y

6. Высказывания A, B, C истинны для точек, принадлежащих кругу, треугольнику, прямоугольнику соответственно. Для всех точек выделенной на рисунке области истинно высказывание

а. (A или B) и B

б. (C и не A) и не B

в. (B или C) и не C

г. (B и C) и не A

д. (A и C) и не B

7. При графическом способе записи алгоритма блок означает

а. Проверку условия и выбор направления выполнения алгоритма*

б. Начало или конец обработки данных

в. Начало цикла

г. Конец цикла

8. Свойство алгоритма "Массовость" это:

а. Возможность применения алгоритма множеством пользователей

б. Возможность решения всего класса задач определенного типа без изменения алгоритма

в. Возможность применения алгоритма исполнителями с различной системой команд

г. Возможность одновременного выполнения нескольких копий алгоритма одним исполнителем

9. Чему равны значения переменных x и y после выполнения операторов присваивания x=2; y=5; x=y; y=x?

а. 5; 2

б. 2; 5

в. 5; 5

г. 2; 2

10. Если элементы массива F[1..6] равны соответственно 6, 5, 4, 3, 2, 1, то значение выражения F[F[F[3]]] – F[F[2]-F[4]] равно:

а. – 1;

б. 6;

в. 0;
г. 4;
д. – 3.

11. Укажите последовательность команд, в результате выполнения которых
значения переменных X и Y поменяются местами:

а. B=X; X=Y; Y=X;
б. X=Y; Y=X;
в. Y=X; B=X; X=Y;
г. C=X; X=Y; Y=C.

12. Величины в языках программирования характеризуются:

а. элементами, размером, значением;
б. однородностью, предназначением, полезностью;
в. местоположением, принадлежностью, значением;
г. типом, именем, значением*

13. Переменная в программировании считается полностью заданной, если известны ее…

а. Тип, имя
б. Имя, значение
в. Тип, значение
г. Тип, имя, значение

14. Каждое выражение (каждый оператор) в программе отделяется друг от друга ...

а. ;*
б. -
в. .
г. ,
д. :

15. Правильная строковая запись выражения

а. x-x***3/absx + sin(x)
б. x-x*x*x/abs(x) +sin(x)
в. (x-x*x*x)/abs(x) +sin(x)
г. x-x*x*x/absx +sinx

16. До каких пор будут выполняться	**операторы в**
теле цикла while (x < 100)?	
а. Пока x строго меньше ста	
б. Пока x равен ста	
в. Пока x меньше или равен ста	
г. Пока x больше ста	

17. Укажите объектно-ориентированный язык программирования

а. Java
б. Все варианты ответов
в. C++

г. C#

18. Тело оператора выбора if, будет выполняться. если его условие:

а. истинно (true)

б. ложно (false)

19. Массив - это ...

а. Массив - это упорядоченные в памяти элементы одного и того же типа, имеющие
имя. Доступ к отдельным элементам массива осуществляется по имени массива и
индексу

б. Массив - это упорядоченные в памяти элементы одного и того же типа, имеющие
имя. Доступ к отдельным элементам массива осуществляется по имени массива и
адресу

x

x x

x sin

3

– +

в. Массив - это упорядоченные в памяти элементы одного и того же типа, имеющие
общий адрес. Доступ к отдельным элементам массива осуществляется по адресу и
индексу

20. Графическое представление алгоритма?

а. Блок - схема;

б. Схема;

в. График;

г. Структура;

21. Что такое условный оператор?

а. Конструкция языка программирования, обеспечивающее выполнение действий только при выполнении некоторого логического выражения*

б. Некоторая часть исходного кода обеспечивающее повторение определенного действия

в. Стандартная библиотека во многих языках программирования

22. Что такое цикл?

а. Имя переменной

б. Оператор присваивания

в. Оператор, предназначенный для многократного использования определенных
инструкций

23. Зачем нужен тип данных?

а. Для обеспечения целостности данных

б. Для создания переменных с неизвестным типом

в. Для указания переменной типа ее содержимого

24. Что такое функция?

а. Некоторая часть программы, имеющая собственное имя и которая может вызываться столько раз, сколько это нужно

б. Некоторая часть программы, содержащая вредоносный код, и блокирующая
определенные действия системы

в. Некоторая часть программы, в которой происходит начальная инициализация всех
полей структур, массивов, переменных и т д.

25. Какие операции допустимы с логическими переменными?

а. логическое сложение

б. логическое умножение

в. отрицание

г. логическое вычитание

26. Данные, значения которых не меняются в процессе выполнения алгоритма.

а. Переменные

б. Константы

в. Исходные данные

**27. Тело цикла для вычисления значений функций f(x)=x*4, на отрезке [-5,5] с
шагом 0.1 будет иметь вид:**

а. f:= x*x*x*x; x:=x+0.5; cout<<f<<x;

б. f:= x*4; x:=0.1; cout<<f<<x;

в. f:= x*4; cout<<f<<x; x:=x+0.1;

г. f:= x*4; x:=x+0.1; cout<<f<<x;

28. Рекурсия – это:

а. Повторение выполнения функции или процедуры внутри себя;

б. Оператор;

в. Цикл;

г. Возвращаемое функцией или процедурой значение.

29. Указать выражение, соответствующее указанному условию: ни одно

из
чисел x, y и z не является положительным.
а. (x>0) или (y>0) или (z>0)
б. (x<0) и (y<0) и (z<0)
в. (x<0) или (y<0) или (z<0)
г. (x>0) и (y>0) и (z>0)
30. Какой из документов является алгоритмом?
а. Правила техники безопасности
б. Инструкция по получению денег в банкомате
в. Расписание уроков
Базы данных
1. **В базе данных хранятся:**
а. Только данные
б. Данные и описание данных — метаданные
в. Данные, метаданные и программы СУБД
г. Данные, метаданные и пользовательские программы
д. Все ответы неверны
2. Система управления базами данных — это:
а. Программы работы с данными и метаданными
б. Программы работы с данными и метаданными и программы пользовательского
интерфейса
в. Программы работы с данными и метаданными и программы решения задач предметной области
г. Данные, метаданные и пользовательские программы
д. Все ответы неверны
3. По отношению к метаданным СУБД выполняет функции:
а. Создания новых объектов
б. Создание и изменение объектов
в. Создание, изменение и удаление объектов
г. Создание, изменение, удаление и выборка объектов
4. По отношению к данным СУБД выполняет функции:
а. Добавление новых данных
б. Добавление и изменение данных
в. Добавление, изменение и удаление данных
г. Добавление, изменение, удаление и выборка данных
5. Произвольные структуры данных позволяют поддерживать модели данных:
а. Только иерархические

б. Сетевые и реляционные
в. Только реляционные
г. Только сетевые
д. Ни одна из перечисленных

6. Метаданные представляют собой:

а. Описание данных, хранящихся в базе данных
б. Данные, хранящиеся в базе данных
в. Ничего из указанного

7. Произвольные запросы к базе данных лучше всего реализуются:

а. В последовательных файлах
б. В иерархических системах
в. В сетевых системах
г. В реляционных системах
д. В сетевых и реляционных базах данных
е. Во всех базах данных

8. Безопасность данных лучше всего может быть реализована:

а. В последовательных файлах
б. В иерархических системах
в. В сетевых системах
г. В реляционных системах
д. В сетевых и реляционных базах данных
е. Во всех базах данных

9. Целостность данных лучше всего может быть реализована:

а. В последовательных файлах
б. В иерархических системах
в. В сетевых системах
г. В реляционных системах
д. В сетевых и реляционных базах данных
е. Во всех базах данных

10. В реляционной базе данных данные хранятся в виде однородных таблиц:

а. Верно
б. Неверно

11. Диаграммы Бахмана позволяют описать:

а. Структуру программы
б. Отношения внутри записи (структуру записи)
в. Отношения в базе данных (отношения между данными в базе данных)
г. Ни одно из указанных

12. Администратор базы данных:

а. Создает базу данных
б. Разрабатывает программы для работы с базой данных
в. Отвечает за обеспечение целостности и безопасности базы данных
г. Работает с программами, использующими базу данных

13. Разработчик базы данных:

а. Создает базу данных
б. Разрабатывает программы для работы с базой данных
в. Отвечает за обеспечение целостности и безопасности базы данных
г. Работает с программами, использующими базу данных

14. Прикладной программист:

а. Создает базу данных
б. Разрабатывает программы для работы с базой данных
в. Отвечает за обеспечение целостности и безопасности базы данных
г. Работает с программами, использующими базу данных

15. Для добавления в базу данных нового объекта используется оператор (набор
текста)

16. Для добавления в таблицу базы данных новой строки используется оператор
(набор текста)

17. Для удаления из базы данных объекта используется оператор (набор текста)

18. Для удаления строк из таблицы базы данных используется оператор (набор
текста)

19. Для изменения характеристик объекта базы данных используется оператор
(набор текста)

20. Для изменения данных в базе данных используется оператор (набор текста)

21. Для выборки данных из таблиц базы данных используется оператор (набор
текста)

22. Индексы в реляционной базе данных используются:

а. Для ускорения выборки данных
б. Для ускорения упорядочения выбранных данных
в. Для ускорения выборки и упорядочения данных
г. Ни для чего из перечисленного

23. Таблица может иметь несколько первичных ключей:

а. Верно
б. Неверно

24. Таблица может иметь несколько внешних ключей:

а. Верно
б. Неверно

25. Первичный ключ в таблице может быть использован:

а. Для однозначной идентификации строки таблицы
б. В реализации отношения один ко многим
в. Во всех перечисленных случаях
г. Ни в одном из перечисленных случаев

26. Внешний ключ в таблице может быть использован:

а. Для однозначной идентификации строки таблицы
б. В реализации отношения один ко многим
в. Во всех перечисленных случаях
г. Ни в одном из перечисленных случаев

27. Предложение CHECK в таблице задает:

а. Ограничение первичного ключа
б. Ограничение внешнего ключа
в. Ограничение уникального ключа
г. Проверку значения столбца или группы столбцов
д. Значение по умолчанию

28. Предложение DEFAULT в таблице задает:

а. Ограничение первичного ключа
б. Ограничение внешнего ключа
в. Ограничение уникального ключа
г. Проверку значения столбца или группы столбцов
д. Значение по умолчанию

29. К хранимым процедурам в базе данных могут обращаться:

а. Только хранимые процедуры
б. Хранимые процедуры и триггеры
в. Хранимые процедуры, триггеры, программы
г. Ничто из указанного неверно

30. К триггерам в базе данных могут обращаться:

а. Только хранимые процедуры
б. Хранимые процедуры и триггеры
в. Хранимые процедуры, триггеры, программы
г. Ничто из указанного неверно

ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем

1. Что относятся к активным методам защиты речевой информации?

а. создание маскирующих акустических и вибрационных помех;

б. выявление факта несанкционированного подключения к линии;

в. создание прицельных электромагнитных помех акустическим закладным устройствам;

г. выявление излучений акустических закладных устройств;

д. уничтожение средств несанкционированного подключения к телефонной линии.

2. К мероприятиям по выявлению технических каналов утечки информации
относятся:

а. специальная проверка автоматизированной системы;

б. специальные обследования выделенных помещений;

в. специальные исследования с использованием контрольно-измерительной аппаратуры;

г. специальный анализ потенциального злоумышленника.

3. Закончите фразу: «Период создания и использования АИС, охватывающий ее
различные состояния, начиная с момента возникновения необходимости в данной
автоматизированной системе и заканчивая моментом ее полного выхода из
употребления у пользователей – это ...»

4. Восстановите в правильном порядке основные стадии жизненного цикла АИС

а. проектная;

б. функционирование;

в. внедрение;

г. предпроектная.

5. Какая из приведенных моделей не является моделью жизненного цикла АИС

а. поэтапная модель с промежуточным контролем;

б. каскадная;

в. спиральная;

г. классическая.

6. Периодичность проведения контроля эффективности средств защиты:

а. раз в 6 месяцев;

б. раз в год;

в. раз в 4 месяца;

г. раз в месяц.

7. В результате реализации атаки доступа (прослушивания) по технических каналов
утечки информации, возможно возникновение -

а. угрозы утечки акустической информации;
б. угрозы утечки видовой информации;
в. угроза утечки информации по каналам побочных электромагнитных излучений и
наводок.

8. Закончите фразу: «Любой объект содержит информацию о самом себе или о
другом объекте»

9. Продолжите фразу: «…- продукт абстрактного мышления человека. Она отображает
объекты, явления, как материального мира, так и создаваемые им образы и модели с
помощью символов на языках общения людей».

10. К источникам функциональных сигналов относятся:

а. передатчики систем связи;
б. передатчики радиотехнических систем;
в. излучатели акустических сигналов гидролокаторов;
г. условные сигналы;
д. ничего не относится.

11. Признаки, позволяющие отличить один объект от другого, называются

а. демаскирующими;
б. отличительными;
в. опознавательные;
г. признаки деятельности.

12. Наиболее характерные уязвимости АС предприятия, на которые следует особо
обратить внимание при составлении плана защиты, это:

а. точки доступа;
б. наличие в АС часто используемых сетевых служб;
в. неправильно сконфигурированные системы;
г. программные ошибки;
д. внутренние враги.

13. Комплексные системы защиты информации в сетях могут включать в себя такие

подсистемы, как:

а. подсистема виртуальных частных сетей (VPN);

б. подсистема защиты удалённых и мобильных пользователей;

в. подсистема контроля и разграничения доступа;

г. подсистема аутентификации.

14. Совокупность компонент, которая реализует основные принципы функционирования и управления подсистемой защиты информации, правила
взаимодействия ее компонент, позволяет конфигурировать состав средств
обеспечения защиты в зависимости от динамично изменяющихся условий
эксплуатации и модели угроз в системе это -

а. центр;

б. ядро;

в. главный компонент;

г. ключ.

15. Особенностью этих вирусов является умение изменять собственный код

а. файловые вирусы;

б. трояны;

в. резидентные вирусы;

г. полиморфные вирусы.

16. Активный перехват информации это перехват, который:

а. заключается в установке подслушивающего устройства в аппаратуру средств
обработки информации;

б. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

в. неправомерно использует технологические отходы информационного процесса;

г. осуществляется путем использования оптической техники;

д. осуществляется с помощью подключения к телекоммуникационному оборудованию
компьютера.

17. Как называется способ несанкционированного доступа к информации, который
заключается в отыскании участков программ, имеющих ошибку или неудачную

логику построения?

а. “За дураком”;

б. “Брешь”;

в. “Компьютерный абордаж”;

г. “За хвост”;

д. “Неспешный выбор”.

18. Способ несанкционированного доступа к информации “Компьютерный абордаж” заключается в:

а. отыскании участков программ, имеющих ошибку или неудачную логику построения;

б. подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;

в. подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;

г. нахождении злоумышленником уязвимых мест в ее защите;

д. несанкционированном доступе в компьютер или компьютерную сеть без права на то.

19. Кого называют «Фишер»?

а. это лицо, которое взламывает интрасеть в познавательных целях;

б. это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;

в. это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

г. так в XIX веке называли плохих игроков в гольф, дилетантов;

д. это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

20. Искусственные угрозы безопасности информации вызваны:

а. деятельностью человека;

б. ошибками при проектировании АСОИ, ее элементов или разработке программного
обеспечения;
в. воздействиями объективных физических процессов или стихийных природных
явлений, независящих от человека;
г. корыстными устремлениями злоумышленников;
д. ошибками при действиях персонала.

**21. По уровню эталонной модели взаимосвязи открытых систем OSI Международной
организации стандартизации (ISO) удаленные атаки делятся на:**

а. условные и безусловные;
б. атаки с обратной связью и без обратной связи;
в. внутрисегментные и межсегментные;
г. пассивные и активные;
д. атаки, которые могут реализовываться на всех семи уровнях.

**22. Атака, которая заключается в запуске на атакуемом компьютере программы
"сетевого шпиона":**

а. подмена доверенного объекта или субъекта распределенной вычислительной сети;
б. ложный объект распределенной вычислительной сети;
в. анализ сетевого трафика;
г. отказ в обслуживании;
д. удаленный контроль над станцией в сети.

23. По среде обитания классические вирусы разделяются на:

а. паразитические;
б. компаньоны;
в. файловые;
г. ссылки;
д. перезаписывающие.

**24. Защищаемая по закону информация, довереная или ставшая известной лицу
(держателю) исключительно в силу исполнения им своих профессиональных
обязанностей, не связанных с государственной и муниципальной службой,
распространение которой может нанести ущерб правам и законным интересам**

другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

а. Профессиональная тайна;

б. Коммерческая тайна;

в. Банковская тайна;

г. Врачебная тайна.

25. Метод защиты информации идентификация и установление подлинности

заключается в:

а. контроле доступа к внутреннему монтажу, линиям связи и технологическим
органам управления;

б. создании физической замкнутой преграды с организацией доступа лиц, связанных с
объектом функциональными обязанностями;

в. разделении информации, на части и организации доступа к ней должностных лиц в
соответствии с их функциональными обязанностями и полномочиями;

г. том, что из числа допущенных к ней должностных лиц выделяется группа, которой
предоставляется доступ только при одновременном предъявлении полномочий всех
членов группы;

д. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

26. Замкнутая программная среда — предотвращает запуск программного обеспечения (ПО)

а. доступного;

б. неразрешённого;

в. разрешенного;

г. базового.

27. Совместно с ОС Windows модуль входа в систему обеспечивает:

а. обработку выхода пользователя в систему (проверка возможности входа, оповещение остальных модулей о начале или завершении работы пользователя);

б. блокировку работы пользователя;

в. функциональный контроль работоспособности системы;

г. загрузку данных с персональных идентификаторов пользователя;

д. усиленную аутентификацию пользователя при входе в систему.

28. Подсистема обеспечивает взаимодействие с устройствами аппаратной поддержки
системы Secret Net и состоит из следующих компонентов:
а. модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам;
б. модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
в. драйверы устройств аппаратной поддержки (если они необходимы);
г. программные модули.

29. Временное нарушение работоспособности какого – либо элемента АСОД,
следствием чего может быть неправильное выполнение им в этот момент своих
функций.
а. сбой;
б. отказ;
в. ошибка;
г. стихийное бедствие;
д. побочное явление.

30. DNS (Domain Name System) – это…
а. сетевая служба, производящая преобразование доменных (символьных) имен в IP
адреса и обратно;
б. параметр, обозначающий скорость передачи информации по сети;
в. главный компьютер (сервер) в сети;
г. программа на сервере, назначающая каждому компьютеру уникальный IP адрес.

ПМ. 02 Применение программно-аппаратных средств обеспечения информационной
безопасности в автоматизированных системах

1. Шифры замены бывают:
а. простые одноалфавитные;
б. одноконтурные полиалфавитные;
в. многоконтурные полиалфавитные;
г. монофонические полиалфавитные;
д. усложненные по маршрутам.

2. Криптосистемы с секретным ключом называют:
а. симметричными криптосистемами;
б. асимметричными криптосистемами;

в. одноключевыми криптосистемами;

г. двуключевыми криптосистемами.

3. Хэш-функция должна обладать следующими функциями:

а. устойчивость к коллизиям;

б. симметричность;

в. однонаправленность;

г. линейность.

4. Алгоритм RSA основан на использовании

а. односторонней функции;

б. односторонней функции с лазейкой;

в. надежного простого числа;

г. составного числа, образованного двумя простыми числами.

5. Коды аутентичности сообщений позволяют

а. шифровать сообщения;

б. дешифровывать сообщения;

в. подтверждать целостность сообщения;

г. подтверждать подлинность отправителя.

6. К симметричным криптосистемам относятся алгоритмы

а. DES

б. 3DES

в. AES

г. RSA

д. TWOFISH

7. Устройство «Сцитало» является примером шифрования:

а. методом подстановки;

б. методом перестановки;

в. методом гаммирования.

8. Шифры делятся на

а. блоковые и последовательные;

б. блочные и поточные;

в. потоковые и дискретные.

9. К достоинствам блочных шифров относят

а. высокую скорость шифрования;

б. дешевизну реализации;

в. похожесть процедур шифрования и расшифрования.

10. Стандарт шифрования ГОСТ 28147-89 предусматривает шифрование и

расшифровку данных в следующих режимах работа:

а. простая замена;

б. маршрутная перестановка;
в. гаммирование;
г. гаммирование с обратной связью;
д. выработка имитовставки.

11. Режим выработка имитовставки в стандарте шифрования ГОСТ 28147-89
гарантирует:

а. конфиденциальность сообщения;
б. целостность сообщения;
в. аутентификацию сообщения;

12. К методам защиты от НСД относятся:

а. разделение доступа;
б. разграничение доступа;
в. увеличение доступа;
г. ограничение доступа;
д. аутентификация и идентификация.

13. Выделите группы, на которые делятся средства защиты информации:

а. физические, аппаратные, программные, криптографические, комбинированные;
б. химические, аппаратные, программные, криптографические, комбинированные;
в. физические, аппаратные, программные, этнографические, комбинированные.

14. Что такое целостность информации?

а. свойство информации, заключающееся в возможности ее изменения любым
субъектом;
б. свойство информации, заключающееся в возможности изменения только единственным пользователем;
в. свойство информации, заключающееся в ее существовании в виде единого набора файлов;
г. свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

15. К аспектам ИБ относятся

а. дискретность;
б. целостность;
в. конфиденциальность;

г. актуальность;

д. доступность.

16. Что такое несанкционированный доступ (нсд)?

а. доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

б. создание резервных копий в организации;

в. правила и положения, выработанные в организации для обхода парольной защиты;

г. вход в систему без согласования с руководителем организации;

д. удаление не нужной информации.

17. К видам защиты информации относятся:

а. правовые и законодательные;

б. морально-этические;

в. юридические;

г. административно-организационные;

18. Какие атаки предпринимают хакеры на программном уровне?

а. атаки на уровне ОС;

б. атаки на уровне сетевого ПО;

в. атаки на уровне пакетов прикладных программ;

г. атаки на уровне СУБД.

19. ГПСЧ Fortuna состоит из трех частей:

а. генератора;

б. аккумулятора;

в. трансформатора;

г. системы управления файлом начального числа;

д. файла загрузки.

20. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

а. операционной системы, сетевого программного обеспечения;

б. операционной системы, сетевого программного обеспечения и системы управления базами данных;

в. операционной системы, системы управления базами данных;

г. сетевого программного обеспечения и системы управления базами данных.

21. Верификация –

а. это проверка принадлежности субъекту доступа предъявленного им идентификатора;

б. проверка целостности и подлинности информации, программы, документа;

в. это присвоение имени субъекту или объекту.

22. Утечка информации

а. несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу;
б. ознакомление постороннего лица с содержанием секретной информации;
в. потеря, хищение, разрушение или неполучение переданных данных.

23. К основным аппаратным средствам защиты информации относятся:

а. устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.);
б. устройства для шифрования информации;
в. устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы);
г. нет правильного ответа.

24. Продолжите фразу: «В модели программная закладка внедряется в ПЗУ, системное или программное обеспечение и сохраняет вводимую информацию с внешних устройств или выводимую на эти устройства в скрытой области памяти локальной или удаленной компьютерной системы».

25. Закончите фразу: «Уникальная характеристика компьютера или других
устройств системы, которая может быть использована для защиты и проверена программным способом – это...»

26. Укажите исходные данные, по которым производится классификация АС:

а. наличие сети передачи данных АС;
б. перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
в. условий размещения СВТ АС;
г. исходя из принятой схемы обработки информации в АС.

27. При разработке АС, предназначенной для обработки или хранения конфиденциальной информации, необходимо ориентироваться на классы
защищенности АС не ниже:

а. 3А
б. 3Б
в. 2А
г. 2Б
д. 1Г

28. Отметьте соответствующие требованию угрозы. Должна осуществляться
физическая охрана СВТ (устройств и носителей информации),

предусматривающая постоянное наличие охраны территории и здания, где
размещается АС, с помощью технических средств охраны и специального
персонала, использование строгого пропускного режима, специальное оборудование помещений АС.

а. возможны действие террористических групп или отдельных лиц с целью завладения секретной информации;
б. возможны хищения СВТ;
в. возможен доступ к СВТ посторонних лиц (посетителей, гостей.);
г. возможны действия диверсионных групп;
д. возможны умышленные действия персонала АС нарушающие установленные
правила доступа к объектам доступа.

29. Отметьте правильные варианты ответа. К основным способам НСД относятся:

а. непосредственное обращение к объектам доступа;
б. просмотр информации с экранов мониторов посторонними лицами;
в. создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
г. разглашение защищаемых сведений сотрудниками организации;
д. применение портативных устройств съема информации.

30. Каким из перечисленных способов не реализуется Распределение ключей
между пользователями компьютерной сети:

а. документирование алгоритмов обеспечения защиты информации;
б. использование одного или несколько центров распределения ключей;
в. прямым обменом сеансовыми ключами между пользователями сети;
г. использование одного центра распределения ключей.

Прочитать предложенный текст, выбрать:
- этапы построения системы защиты информации
- перечень должностей, которые должны быть вовлечены в создание и подготовку документов по политике безопасности.

Выполнить их перевод на русский язык.

Network Working Group B. Fraser
Request for Comments: 2196 Editor
FYI: 8 SEI/CMU
Obsoletes: 1244 September 1997
Category: Informational

...

1.5 Basic Approach

This guide is written to provide basic guidance in developing a security plan for your site. One generally accepted approach to follow is suggested by Fites, et. al. [Fites 1989] and includes the following steps:Identify what you are trying to protect. Determine what you are trying to protect it from. Determine how likely the threats are. Implement measures which will protect your assets in a cost-effective manner. Review the process continuously and make improvements each time a weakness is found.
Most of this document is focused on item 4 above, but the other steps cannot be avoided if an effective plan is to be established at your site. One old truism in security is that the cost of protecting yourself against a threat should be less than the cost of recovering if the threat were to strike you. Cost in this context should be remembered to include losses expressed in real currency, reputation, trustworthiness, and other less obvious measures. Without reasonable knowledge of what you are protecting and what the likely threats are, following this rule could be difficult.

1.6 Risk Assessment

1.6.1 General Discussion

One of the most important reasons for creating a computer security policy is to ensure that efforts spent on security yield cost effective benefits. Although this may seem obvious, it is possible to be mislead about where the effort is needed. As an example, there is a great deal of publicity about intruders on computers systems; yet most surveys of computer security show that, for most organizations, the actual loss from "insiders" is much greater.
Risk analysis involves determining what you need to protect, what you

need to protect it from, and how to protect it. It is the process of examining all of your risks, then ranking those risks by level of severity. This process involves making cost-effective decisions on what you want to protect. As mentioned above, you should probably not spend more to protect something than it is actually worth.
A full treatment of risk analysis is outside the scope of this document. [Fites 1989] and [Pfleeger 1989] provide introductions to this topic. However, there are two elements of a risk analysis that will be briefly covered in the next two sections.
Identifying the assets
Identifying the threats
For each asset, the basic goals of security are availability, confidentiality, and integrity. Each threat should be examined with an eye to how the threat could affect these areas.

1.6.2 Identifying the Assets

One step in a risk analysis is to identify all the things that need to be protected. Some things are obvious, like valuable proprietary information, intellectual property, and all the various pieces of hardware; but, some are overlooked, such as the people who actually use the systems. The essential point is to list all things that could be affected by a security problem.
One list of categories is suggested by Pfleeger [Pfleeger 1989]; this list is adapted from that source: Hardware: CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers. Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs. Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media. People: users, administrators, hardware maintainers. Documentation: on programs, hardware, systems, local administrative procedures. Supplies: paper, forms, ribbons, magnetic media.

1.6.3 Identifying the Threats

Once the assets requiring protection are identified, it is necessary to identify threats to those assets. The threats can then be

examined to determine what potential for loss exists. It helps to consider from what threats you are trying to protect your assets. The following are classic threats that should be considered. Depending on your site, there will be more specific threats that should be identified and addressed.
Unauthorized access to resources and/or information
Unintented and/or unauthorized Disclosure of information
Denial of service

2.1.3 Who Should be Involved When Forming Policy?

In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. It is especially important that corporate management fully support the security policy process otherwise there is little chance that they will have the intended impact. The following is a list of individuals who should be involved in the creation and review of security policy documents.
Site security administrator. Information technology technical staff (e.g., staff from computing center). Administrators of large user groups within the organization (e.g., business divisions, computer science department within a university, etc.). Security incident response team Representatives of the user groups affected by the security policy. Responsible management. Legal counsel (if appropriate).
The list above is representative of many organizations, but is not necessarily comprehensive. The idea is to bring in representation from key stakeholders, management who have budget and policy authority, technical staff who know what can and cannot be supported, and legal counsel who know the legal ramifications of various policy choices. In some organizations, it may be appropriate to include EDP audit personnel. Involving this group is important if resulting policy statements are to reach the broadest possible acceptance. It is also relevant to mention that the role of legal counsel will also vary from country to country.
...

2. Профессиональное задание.

2.1 **Задания Cisco Packet Tracer**

Для всех устройств локальный пользователь: cisco пароль: cisco

Пароль enable: cisco

Для настройки Router0 используйте Laptop0.

Используйте сеть 172.18.0.0/16 для разделения на подсети с длиной префикса /24:

LAN-0 должен использовать нулевую подсеть.

LAN-1 должен использовать первую подсеть.

LAN-2 должен использовать вторую подсеть.

На Router0 создайте 4 псевдоинтерфейса с инкапсуляцией dot1q на интерфейсе FastEthernet0/0. Используйте VID 100(LAN-0), VID 101(LAN-1), VID 102 (LAN-2) и укажите им первый свободный IP адрес в соответствующих подсетях. Создайте последний псевдоинтерфейс с VID 252 для управления сетевым оборудованием, назначьте ему IP адрес из подсети 10.10.0.0/16 см. таблица 1.

Первому псевдоинтерфейсу дайте описание "Servers".

Второму псевдоинтерфейсу дайте описание "IT".

Третьему псевдоинтерфейсу дайте описание "Manager".

Псевдоинтерфейсу для управления сетевым оборудованием дайте описание "Management".

Настройте 3 DHCP пула, дайте им имена в соответствии с описание псевдоинтерфейсов.

Назначьте для всех пулов выдачу IP адресов, шлюза и dns в соответствии подсетям.

Сделайте резервирование первых IP адресов каждой подсети.

Настройку Switch0 производите с Router0 при помощи telnet, для подключения см. таблица 1.

Создайте три VLAN в соответствии подсетям и VID. Используйте названия VLAN

такие же как и для псевдоинтерфейсов.

Настройте порты FastEthernet0/1-0/3 в VLAN - Servers.

Настройте порты FastEthernet0/11-0/12 в VLAN - IT.

Сделайте порт FastEthernet0/22 транковым, разрешите доступ только для всех ранее созданных VLAN.

На PC6 назначьте первый свободный IP адрес из подсети 10.10.0.0/16 см. таблица 1

Настройку Switch1 производите с PC6 при помощи telnet, для подключения см. таблица 1.

Сделайте агрегирование каналов между Switch0 и Switch1 (FastEthernet0/23-0/24). Используйте первую группу и протокол LACP. Сделайте группу каналов транковой, разрешите все ранее созданные VLAN.

На Switch1 сделайте порты Gi0/1-0/2 транковыми, разрешите все ранее созданные VLAN.

Назначьте Server1 IP адрес: 172.18.0.253/24

Оставьте включенной только роль WEB сервера.

Назначьте Server2 IP адрес: 172.18.0.254/24

Оставьте включенной только роль DNS сервера.

Создайте A записи см. таблица 1.

Назначьте Server3 IP адрес: 172.18.0.252/24

Оставьте включенной роль FTP сервера.

На всех коммутаторах назначьте шлюз по умолчанию IP адрес Management интерфейса Router0.

На всем сетевом оборудование установите имя хоста в соответствии с таблицей 1.

На всех коммутаторах настройте VTP в соответствии с таблицей:

Device	Mode	Version	Domain	Password
Switch0	Server	2	YktSkills	ykt2015
Switch1	Client	2	YktSkills	ykt2015
Switch2	Client	2	YktSkills	ykt2015
Switch3	Client	2	YktSkills	ykt2015

На всех коммутаторах включите быстрый Spanning-tree.

На всех сетевых устройствах назначьте DNS сервер.

PC0-PC6 должны получать IP адрес автоматический, в соответствующих подсетях.

Таблица 1.

Device	Hostname	IP адрес
Router0	R0	10.10.0.1
Switch0	SW0	10.10.0.2
Switch1	SW1	10.10.0.3
Switch2	SW2	10.10.0.4
Switch3	SW3	10.10.0.5
Server1	WEB	172.18.0.253
Server2	DNS	172.18.0.254
Server3	FTP	172.18.0.252

2.2. Настройка ОС Windows 10

а. Настроить сетевые параметры следующим образом

Сетевое имя: IBCLI-X

IP адрес, маска: 172.16.1.6X/24

DNS сервер 172.16.1.1

IPv6: отключен

б. Создать пользователей и группы следующим образом

Имя: ib_admin

Пароль: Pa$$w0rd

Группа: Администраторы, ib_admins

Имя: ib_user

Пароль: 12345

Группа: Пользователи, ib_users

в. Настройте политику паролей для локального компьютера

Максимальный срок действия пароля: 30 дней

Минимальная длина пароля: 5 символов

Пароль НЕ должен отвечать требованиям сложности

б. Настройте брандмауэр следующим образом

Брандмауэр включен для всех сетей

Обеспечена рработоспосноть протокла ICMP

г. Настройте политику Chrome для группы ib_users

Файлы шаблонов находятся в C:/policy_templates/

д. Настройте подключение к VPN следующим образом

Дистрибутив клиентской программы в C:/VPN/

г. Подключите сетевой диск

Адрес: \\192.168.66.2\Recovery\

Буква диска: R

Восстанавливать при входе в систему

Имя пользователя: net_smb

Пароль: smbPa$$w0rd

д. Восстановление данных на usb накопителе

Дистрибутив программы находится на диске R

2.3. Подключение ПКП «Гранит-3,4,5,8».

Перед началом работы внимательно изучите руководство по эксплуатации, ознакомьтесь с принципом работы прибора, а также со схемами внешних соединений (Приложение).

Внимание! Особое внимание обратите на меры безопасности. Проведите внешний осмотр. Убедитесь в отсутствии внешних повреждений и в соответствии заводского номера прибора, номеру, указанному в руководстве по эксплуатации.

Убедитесь внешним осмотром в соответствии комплекта поставки прибора, комплектности, указанной в руководства.

Подключите к прибору сетевой кабель 220 В (не комплектуется) и жгуты для подключения АБ: синий – к «-», красный – к «+» контакту клеммника «АКБ».

Проведите проверку технического состояния согласно табл.13.

Произведите монтаж всех линий, соединяющих прибор с охранными и пожарными извещателями, световыми и звуковыми оповещателями и т.д., соблюдая полярность в соответствии со схемами соединений.

Внимание! Допускается одновременное включение в ШС пожарных извещателей, только увеличивающих потребляемый ток при срабатывании (токопотребляющие, типа ИП101-1А, ИП212-63, ИП535-8-А и т.п.), либо только извещателей, размыкающих цепь шлейфа (электроконтактные, типа ИП103, ИП105 и т.п.).

Установите в прибор аккумуляторную батарею. Перед установкой АБ подсоедините синюю клемму жгута к «-», а красную – к «+» контакту АБ. При этом индикатор «АБ» должен светиться зелёным.

Задайте нужную тактику применения прибора: установите необходимым образом перемычки J1…J3, J5, J6 и нажмите кнопку SB2. Запрограммируйте электронные ключи. Либо замкните J1…J3, нажмите SB2, подключите с помощью microUSB-кабеля прибор к компьютеру и с помощью Конфигуратора настройте прибор.

Закройте крышку прибора и включите питание 220 В. Индикатор «Сеть» должен светиться зелёным.

Проверьте правильность выполнения монтажа и проведите проверку работоспособности прибора с питанием от сети переменного тока и АБ в следующей последовательности (в зависимости от конфигурации прибора методика проверки может быть различной):

Проверьте режим «Неисправность ШП» - при поставленном на охрану пожарном ШС сделайте короткое замыкание и обрыв в шлейфе. - Путем отключения прибора от сети 220 В убедитесь в работоспособности прибора при питании от аккумуляторной батареи.