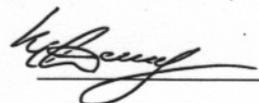


МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерных сетей

УТВЕРЖДАЮ

Декан факультета  
информатики и вычислительной техники

 Д.Ю. Чалый

« 31 » августа 2020 г.

**Рабочая программа дисциплины  
«Информатика, современные информационные технологии»**

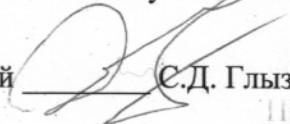
Направление подготовки  
06.03.01 Биология

Профиль «Биоэкология»

Квалификация выпускника  
Бакалавр

Форма обучения  
очная

Программа рассмотрена на заседании  
кафедры компьютерных сетей,  
протокол № 1 от 31 августа 2020 года

Зав. кафедрой  С.Д. Глызин

Программа одобрена НМК факультета  
информатики и вычислительной техники,  
протокол № 1 от 31 августа 2010 года

Председатель НМК  Г.В. Шабаршина

Ярославль  
2020

### 1. Цели освоения дисциплины

Целями освоения дисциплины «Информатика, современные информационные технологии» являются: приобретение знаний и умений в соответствии с ФГОС ВО, формирование и развитие способности применять информационные технологии в профессиональной и прикладной деятельности, проводить научные исследования с использованием современных информационных технологий.

Дисциплина должна давать представление о месте и роли информационных технологий в современном мире, мировой культуре и истории.

### 2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Информатика, современные информационные технологии» относится к вариативной части Блока 1.

Теоретической основой для изучения курса являются естественнонаучные дисциплины учебного плана средней общеобразовательной школы. Дисциплина является базовой для всех дисциплин, использующих компьютерную технику, информационные системы и технологии, автоматизированные методы анализа и статистической обработки данных. Такие личностные характеристики как общая образованность, организованность и трудолюбие, самостоятельность, настойчивость в достижении цели необходимы при освоении дисциплины.

### 3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП бакалавриата

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Код компетенции	Формулировка компетенции	Перечень планируемых результатов обучения
<b>Общепрофессиональные компетенции</b>		
ОПК-1	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<b>Знать:</b> <ul style="list-style-type: none"><li>– устройство персонального компьютера;</li><li>– принципы хранения и обработки информации в компьютере;</li><li>– классификацию программного обеспечения;</li><li>– основы алгоритмизации и программирования;</li><li>– основные понятия в области обработки и защиты информации и их определения;</li><li>последовательность выполнения работ по защите информации; классификацию нарушителей информационной безопасности; классификацию угроз информационной безопасности; виды и назначение средств защиты информации.</li></ul> <b>Уметь:</b> <ul style="list-style-type: none"><li>– пользоваться персональным компьютером для решения и оптимизации прикладных задач;</li><li>– настраивать аппаратное и программное обеспечения персонального компьютера для оптимальной работы;</li><li>– применять современные информационные</li></ul>

		<p>технологии при решении прикладных задач с учетом основных требований информационной безопасности;</p> <ul style="list-style-type: none"> <li>- устанавливать и осуществлять первичную настройку операционных систем, антивирусных средств и межсетевых экранов.</li> </ul> <p><b>Владеть навыками:</b></p> <ul style="list-style-type: none"> <li>– работы в текстовом процессоре Microsoft Word;</li> <li>– работы в табличном процессоре Microsoft Excel;</li> <li>– работы в программе для подготовки презентаций Microsoft PowerPoint.</li> <li>– работы с базами данных;</li> <li>– работы со средствами защиты информации.</li> </ul>
<b>Профессиональные компетенции</b>		
ПК-8	<p>способность использовать основные технические средства поиска научно-биологической информации, универсальные пакеты прикладных компьютерных программ, создавать базы экспериментальных биологических данных, работать с биологической информацией в глобальных компьютерных сетях</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>– устройство персонального компьютера;</li> <li>– принципы хранения и обработки информации в компьютере;</li> <li>– классификацию программного обеспечения;</li> <li>– основы алгоритмизации и программирования.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>– пользоваться персональным компьютером для решения и оптимизации прикладных задач;</li> <li>– настраивать аппаратное и программное обеспечения персонального компьютера для оптимальной работы;</li> <li>– применять современные информационные технологии при решении прикладных задач с учетом основных требований информационной безопасности.</li> </ul> <p><b>Владеть навыками:</b></p> <ul style="list-style-type: none"> <li>– работы в текстовом процессоре Microsoft Word;</li> <li>– работы в табличном процессоре Microsoft Excel;</li> <li>– работы в программе для подготовки презентаций Microsoft PowerPoint.</li> <li>– работы с базами данных.</li> </ul>

#### 4. Объем, форма реализации, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости  Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Введение	3	1						
2	Устройство персонального компьютера	3	2		2			2	Самостоятельная (лабораторная) работа
3	Программное обеспечение	3	2		2	1		3	Самостоятельная (лабораторная) работа
4	Основы баз данных и знаний	3	1		2	1		3	Самостоятельная (лабораторная) работа
5	Основы алгоритмизации и программирования	3	1		2	1		3	Самостоятельная (лабораторная) работа
6	Локальные и глобальные компьютерные сети	3	2		2	1		3	Самостоятельная (лабораторная) работа
7	Безопасность в современной информационной среде	3			8	1		23	Тест по каждой теме
							0,3	2,7	Зачет
	<b>Всего</b>		<b>9</b>		<b>18</b>	<b>5</b>	<b>0,3</b>	<b>39,7</b>	

#### Содержание разделов дисциплины:

##### 1. Введение

Информатика как наука. История развития информационных технологий и ЭВМ. Архитектура вычислительной системы. Принципы современной архитектуры компьютеров. Классификация компьютеров по назначению, уровню специализации, размеру.

##### 2. Устройство персонального компьютера

Базовая конфигурация персонального компьютера. Основные узлы системного блока. Назначение и основные характеристики материнской платы, процессора, оперативной памяти, жестких дисков, приводов для оптических дисков, монитора, видеоадаптера, клавиатуры, мышки. Внешние устройства.

##### 3. Программное обеспечение

Понятие программного обеспечения. Базовый и системный уровни программного обеспечения. Служебный уровень программного обеспечения. Классификация основных программ служебного уровня. Прикладной уровень программного обеспечения.

Классификация основных программ прикладного уровня. Текстовые и табличные процессоры, графические, аудио- и видео- редакторы, средства мультимедиа и коммуникации и др.

#### **4. Основы баз данных и знаний**

Понятия базы данных и знаний, системы управления базой данных. Реляционная модель. Понятие атрибута, сущности, записи, таблицы, первичного ключа. Язык запросов к базе данных SQL, основные команды SQL.

#### **5. Основы алгоритмизации и программирования**

Понятия и основные свойства алгоритма и программы. Понятие программирования, среды программирования, транслятора. Схема создания новых программ. Назначение и классификация языков программирования. Основные операторы языков программирования.

#### **6. Локальные и глобальные компьютерные сети**

Понятие локальной сети. Технологии построения и использования локальных сетей. Глобальная сеть Internet. Сетевые службы. Понятия сервера и клиента. Браузеры, средства работы с электронной почтой. Поиск информации в сети Internet. Современные информационные технологии, применяемые в компьютерных сетях.

#### **7. Безопасность в современной информационной среде**

##### **Тема 1. Правовые и организационные основы обеспечения информационной безопасности в Российской Федерации.**

Тема 1.1. Правовые основы обеспечения информационной безопасности.

Основные права граждан в сфере обработки и защиты информации. Основные принципы правового регулирования в области обработки и защиты информации. Информация. Основные свойства безопасности информации: конфиденциальность, целостность, доступность. Виды информации по порядку доступа и распространения. Ограничение доступа к информации. Виды тайн. Владелец информации. Информационные технологии. Информационные системы. Оператор информационной системы. Защита информации. Объекты защиты. Виды ответственности в сфере обработки и защиты информации.

Тема 1.2. Защита персональных данных.

Персональные данные и принципы их обработки. Виды персональных данных: специальные, биометрические и общедоступные. Условия обработки персональных данных. Согласие на обработку персональных данных. Трансграничная передача персональных данных. Права субъектов персональных данных. Оператор персональных данных и его обязанности. Меры обеспечения безопасности персональных данных. Контроль и надзор за выполнением мер по обеспечению безопасности. Уполномоченный орган по защите прав субъектов персональных данных.

Тема 1.3. Организационные основы обеспечения информационной безопасности.

Какие вопросы ставит информационная безопасность? Последовательность действий по защите информации. Выявление и анализ информационных активов. Формирование требований по защите информации. Подходы к моделированию нарушителей и угроз информационной безопасности. Выбор средств и методов защиты информации. Внедрение системы защиты информации. Эксплуатация системы защиты информации.

##### **Тема 2. Основы информационной безопасности в операционных системах.**

Тема 2.1. Введение в информационную безопасность операционных систем.

Общий способ хранения и обработки информации в компьютере. Понятия операционной и файловой систем. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Дискреционное управление доступом, мандатное управление доступом. Идентификация, аутентификация и авторизация. Аутентификация на основе паролей, на основе внешних носителей ключа, биометрическая аутентификация.

Тема 2.2. Информационная безопасность операционных систем семейства Windows. Управление доступом в операционных системах семейства Windows. Идентификация, аутентификация и авторизация в операционных системах семейства Windows. Реализация аудита в операционных системах семейства Windows.

Тема 2.3. Информационная безопасность операционных систем семейства Linux. Управление доступом в операционных системах семейства Linux. Идентификация, аутентификация и авторизация в операционных системах семейства Linux. Реализация аудита в операционных системах семейства Linux.

### **Тема 3. Основы информационной безопасности в локальных вычислительных сетях.**

Тема 3.1. Введение в архитектуру локальных вычислительных сетей.

Локальные вычислительные сети. Модель ISO/OSI. Архитектура и основные протоколы локальных вычислительных сетей.

Тема 3.2. Сетевые угрозы и методы противодействия им.

Классификации сетевых угроз, уязвимостей и атак. Сетевые атаки на различных уровнях модели ISO/OSI. Классификация вредоносного программного обеспечения. Признаки присутствия вредоносного программного обеспечения. Методы обнаружения.

Тема 3.3. Межсетевые экраны.

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Основные возможности МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации.

### **Тема 4. Криптографические методы защиты информации.**

Тема 4.1. Введение в криптографические методы защиты информации.

Исторический очерк развития криптографии. Симметричная и асимметричная криптография. Вычислительно сложные задачи математики. Криптосистема RSA. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Схемы цифровой подписи.

## **5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине**

«Информатика, современные информационные технологии» – современная инновационная дисциплина. Методика преподавания сочетает лекционное изложение с навыками практической работы на компьютере, в том числе самостоятельной.

*Лекции* включают в себя изложение современного аппаратного и программного обеспечения компьютеров, а также современных информационных технологий, с точки зрения практической работы и профессиональной деятельности.

*Лабораторные занятия* включают в себя работу на компьютере в ряде популярных современных программ. Обучающиеся выполняют лабораторные задания не только под руководством преподавателя, но и самостоятельно. При этом особое внимание уделяется возможным приложениям полученных профессиональных навыков в учебной и исследовательской работе. В индивидуальном порядке проводятся компьютерные симуляции, разбираются конкретные ситуации. Организованные таким образом лабораторные занятия являются важным способом контроля знаний учащихся и возможной площадкой для организации встреч с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классов экспертов и специалистов.

Раздел 7 «Безопасность в современной информационной среде» реализуется с использованием онлайн курса «Безопасность в современной информационной среде»,

предоставляемого образовательной платформой DemidOnline ЯрГУ  
(<https://demidonline.uniyar.ac.ru/courses/course-v1:DemidOnline+InfSec001x+2020/about>)

## **6. Перечень электронных ресурсов и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)**

В процессе осуществления образовательного процесса используются:

- операционные системы семейства Microsoft Windows;
- программы Microsoft Office;
- программа Adobe Acrobat Reader;
- браузеры Mozilla Firefox, Google Chrome;
- онлайн курс «Безопасность в современной информационной среде», URL:  
<https://demidonline.uniyar.ac.ru/courses/course-v1:DemidOnline+InfSec001x+2020/about>

## **7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

### **а) основная литература**

1. Информатика. Базовый курс : для бакалавров и специалистов : учеб. пособие для вузов / под ред. С. В. Симоновича. - 3-е изд., СПб., Питер, 2012. – 30 экз.
2. Информатика : задания для лабораторных работ [Электронный ресурс] : практикум / сост. М. В. Краснов ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2017, 72с  
<http://www.lib.uniyar.ac.ru/edocs/iuni/20170409.pdf>
3. Таненбаум Э. Современные операционные системы. / Э. Таненбаум, Х. Бос; [пер. с англ. А. Леонтьевой, М. Малышевой, Н. Вильчинского] - 4-е изд. - СПб.: Питер, 2019. - 1119 с.: ил.
4. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2005. 480 с.

### **б) дополнительная литература**

1. Могилев, А. В., Информатика : учеб. пособие для вузов / А. В. Могилев, Н. И. Пак, Е. К. Хеннер ; под ред. Е. К. Хеннер. - 2-е изд., стереотип., М., Академия, 2003. – 22 экз.
2. Таненбаум Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл; [пер. с англ. А. Гребенькова] - 5-е изд. - СПб.: Питер, 2019. - 955 с.
3. Конституция Российской Федерации: [принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020]. — Доступ из справочно-правовой системы «Консультант плюс». — Текст: электронный.
4. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 №63-ФЗ: [принят Государственной Думой 24.05.1996]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультант плюс». — Текст: электронный.

5. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.12.2001 №195-ФЗ: [принят Государственной Думой 20.12.2001]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультант плюс». —Текст: электронный.
6. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»: [принят Государственной Думой 08.07.2006]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультант плюс». —Текст: электронный.
7. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»: [принят Государственной Думой 08.07.2006]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультант плюс». —Текст: электронный.
8. Требования к защите персональных данных при их обработке в информационных системах персональных данных: [утверждены Постановлением Правительства Российской Федерации от 01.11.2012 №1119]. — Доступ из справочно-правовой системы «КонсультантПлюс». —Текст: электронный.
9. Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: [утвержден Постановлением Правительства Российской Федерации от 21.03.2012 №211]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «КонсультантПлюс». — Текст: электронный.

#### **в) ресурсы сети «Интернет»**

##### **1. Электронная библиотека учебных материалов ЯрГУ**

([http://www.lib.uniya.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniya.ac.ru/opac/bk_cat_find.php)).

##### **2. Электронно-библиотечная система «Университетская библиотека online»** ([www.biblioclub.ru](http://www.biblioclub.ru)).

**3. Научная библиотека ЯрГУ им. П.Г. Демидова** (доступ к лицензионным современным библиографическим, реферативным и полнотекстовым профессиональным базам данных и информационным справочным системам: реферативные базы данных Web of Science, Scopus; научная электронная библиотека eLIBRARY.RU; электронно-библиотечные системы IPRbooks, Юрайт, Проспект, издательства «ЛАНЬ»; базы данных Polpred.com, «Диссертации РГБ (авторефераты)», ProQuest Dissertations and Theses Global; электронные коллекции Springer; издательство Elsevier на платформе ScienceDirect; журналы Science (The American Association for the Advancement of Science (AAAS), Nature Publishing Group, и др.) [http://www.lib.uniya.ac.ru/content/resource/net\\_res.php](http://www.lib.uniya.ac.ru/content/resource/net_res.php)

##### **4. Справочно-правовая система «Консультант плюс»**

(<https://www.consultant.ru/>) справочно-правовая система по законодательству Российской Федерации.

##### **5. Справочно-правовая система «Гарант»**

(<http://www.garant.ru/>) справочно-правовая система по законодательству Российской Федерации.

#### **8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебная аудитория для проведения лабораторных работ;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории (персональный компьютер, мультимедийная установка, настенный проекционный экран).

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, хранящиеся на электронных носителях и обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплины.

Для проведения лабораторных работ используются: персональные компьютеры, подключенные к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ЯрГУ им. П.Г. Демидова.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации, а также доступом к образовательной онлайн-платформе ЯрГУ им. П.Г. Демидова (DemidOnline).

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для лабораторных работ – списочному составу подгруппы обучающихся (для проведения лабораторных работ группа обучающихся делится на две подгруппы).

Авторы :

Доцент кафедры компьютерных сетей, к.ф.-м.н.

\_\_\_\_\_ Е.В. Коновалов

**Приложение №1 к рабочей программе дисциплины  
«Информатика, современные информационные технологии»  
Фонд оценочных средств  
для проведения текущей и промежуточной аттестации студентов  
по дисциплине**

**1. Типовые контрольные задания или иные материалы,  
необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,  
характеризующих этапы формирования компетенций**

**1.1 Контрольные задания и иные материалы,  
используемые в процессе текущей аттестации**

**Примеры заданий для самостоятельных (лабораторных) работ**

**1. Microsoft Word: интерфейс и возможности программы, набор простого текста**

Набрать текст и отформатировать его по образцу

(1) ЭВМ — это машина для автоматической обработки информации.

Она состоит из процессора, памяти и внешних устройств. В памяти хранится разнообразная информация, закодированная в виде последовательности цифр 0 и 1, которые называют битами. Работа процессора происходит под управлением программы.

Программа находится в памяти ЭВМ и состоит из отдельных команд. Внешние устройства ЭВМ обеспечивают ввод и вывод информации, взаимодействие ЭВМ с человеком и с другими ЭВМ.

(2) ЭВМ – это машина для автоматической обработки информации. Она состоит из процессора, памяти и внешних устройств. В памяти хранится разнообразная информация, закодированная в виде последовательности цифр 0 и 1, которые называют битами. Работа процессора происходит под управлением программы. Программа находится в памяти ЭВМ и состоит из отдельных команд. Внешние устройства ЭВМ обеспечивают ввод и вывод информации, взаимодействие ЭВМ с человеком и с другими ЭВМ.

(3) *ЭВМ — это машина для автоматической обработки информации. Она состоит из процессора, памяти и внешних устройств. В памяти хранится разнообразная информация, закодированная в виде последовательности цифр 0 и 1, которые называют битами. Работа процессора происходит под управлением программы. Программа находится в памяти ЭВМ и состоит из отдельных команд. Внешние устройства ЭВМ обеспечивают ввод и вывод информации, взаимодействие ЭВМ с человеком и с другими ЭВМ.*

(4) ЭВМ — это машина для автоматической обработки информации. Она состоит из процессора, памяти и внешних устройств.

В памяти хранится разнообразная информация, закодированная в виде последовательности цифр 0 и 1, которые называют битами.

(5) Работа процессора происходит под управлением программы. Программа находится в памяти ЭВМ и состоит из отдельных команд.

Внешние устройства ЭВМ обеспечивают ввод и вывод информации, взаимодействие ЭВМ с человеком и с другими ЭВМ.

(6) ЭВМ — это машина для автоматической обработки информации. Она состоит из процессора, памяти и внешних устройств. В памяти хранится разнообразная информация, закодированная в виде последовательности цифр 0 и 1, которые называют битами. Работа процессора происходит под управлением программы. Программа находится в памяти ЭВМ и состоит из отдельных команд. Внешние устройства ЭВМ обеспечивают ввод и вывод информации, взаимодействие ЭВМ с человеком и с другими ЭВМ.

2. Microsoft Word: продвинутые возможности, набор сложного текста.

## Оглавление

<a href="#">В чем же состоит привлекательность Интернета?</a> .....	11
<a href="#">Коммуникационные возможности Сети</a> .....	12

**В** чем же состоит привлекательность Интернета? Сеть предоставляет массу возможностей человеку не только получить информацию, необходимую ему для профессиональной деятельности или в повседневной жизни, но и самореализоваться среди таких же пользователей, что не всегда возможно в реальном мире.<sup>1</sup>

❖ В последнее время Интернет все чаще используется не только для поиска информации или для профессиональной деятельности. Все больше пользователей начинают коммуницировать через Сеть, создавая так называемые «социальные сети» - «веб-сайты с возможностью указать какую-либо информацию о себе (школу, институт, дату рождения и другое), по которой вас смогут найти другие участники сети» («Википедия»®). Например, самая многочисленная социальная сеть российского

**odnoklassniki.ru**

сегмента Интернета

в настоящее время насчитывает более 10

млн. зарегистрированных участников.

❖ Еще одним явлением, подтверждающим увеличение роли Интернета в межличностной коммуникации, явился



<sup>1</sup> В данном случае интересным представляется выделить основные описанные в психологии виды мотивационно-социально-коммуникативную, познавательную, развивающую

блог. Из статьи в «Википедии»®: «Блог (англ. blog, от weblog, «сетевой журнал или дневник событий») — это веб-сайт, основное содержимое которого — регулярно добавляемые записи, изображения или мультимедиа. Для блогов характерны не длинные записи временной значимости». Характерной чертой блога является то, что другие пользователи могут комментировать все выкладываемые автором материалы в личном дневнике. Получается, что пользователь, открывший блог, сознательно выкладывает на всеобщее обозрение свою жизнь, надеясь таким образом привлечь внимание окружающих к себе, найти собеседников со схожими интересами. Таким образом, все больше реальных людей оставляют след своей личности в виртуальном пространстве, обеспечивая информационную среду «очеловечиванием».

Коммуникационные возможности Сети, в общем, социальных сетей и блогов, в частности, очень обширны. Любой пользователь может найти такой круг собеседников, в котором ему наиболее комфортно общаться. Соответственно в период активной социализации молодой пользователь предпочтет виртуальное общение реальному, в котором гораздо легче найти психологически совместимую группу общения. С другой стороны, коммуникация посредством Интернета (за исключением видеочатов) предоставляет обоим собеседникам значительную анонимность, что обуславливает в процессе общения большую открытость и психологический комфорт. Это является важным фактором для людей, имеющих низкую самооценку.

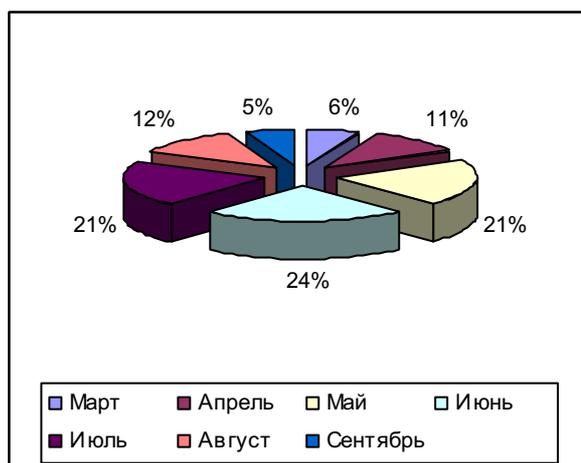
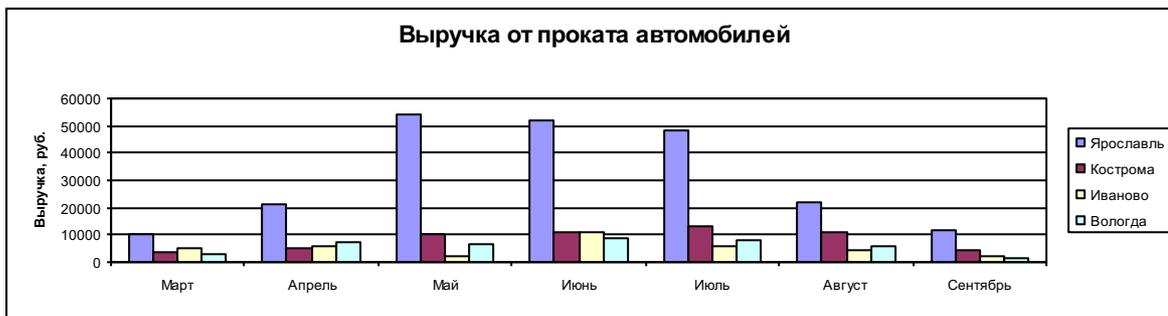
### 3. Microsoft Word: работа с диаграммами.

Построить диаграммы по набору данных

## Выручка от проката автомобилей

2003 г.

	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь
Ярославль	10500	21000	54000	52000	48200	22000	11900
Кострома	3400	5000	10000	11200	13100	10700	4050
Иваново	5000	6000	2400	11000	5700	4100	2150
Вологда	2900	7200	6400	9000	8100	6000	1100
Всего	21800	39200	72800	83200	75100	42800	19200



#### 4. Microsoft Word: работа с организационными диаграммами.

Примеры организационных диаграмм

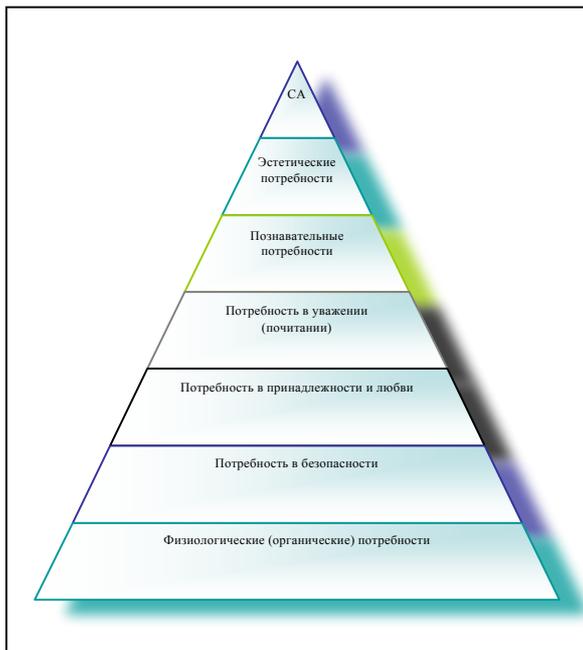


Рис.1. Пирамида потребностей по Маслоу

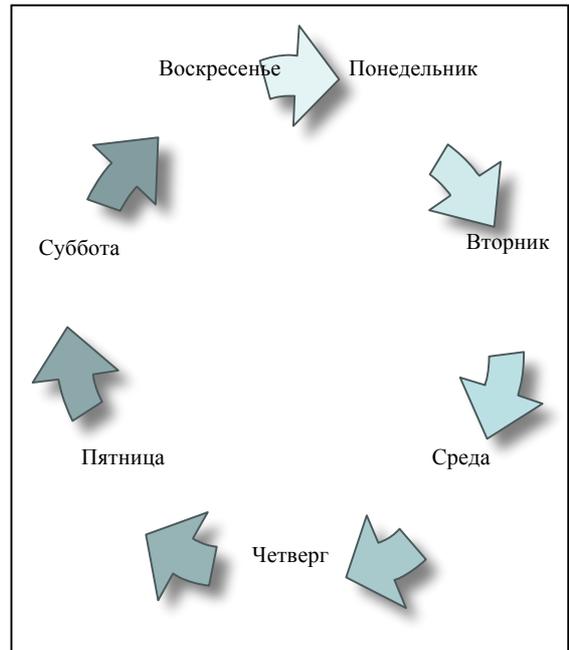


Рис.2. Чередование дней недели

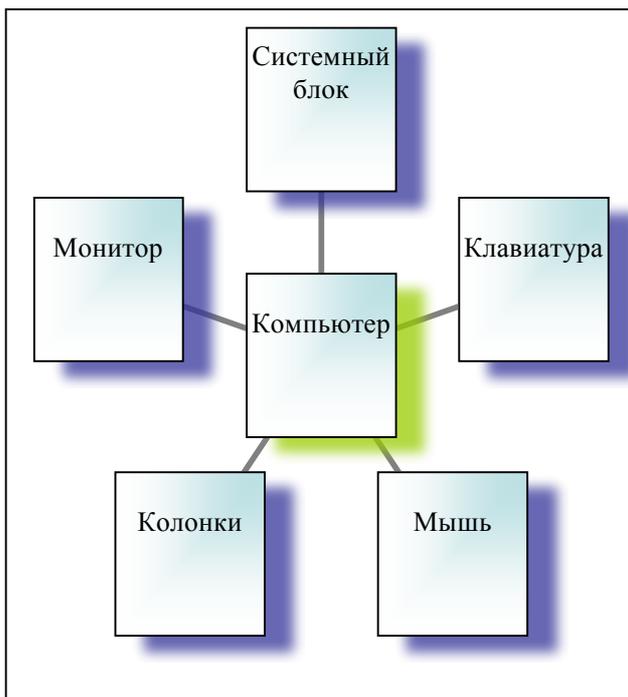


Рис.3. Конфигурация персонального компьютера

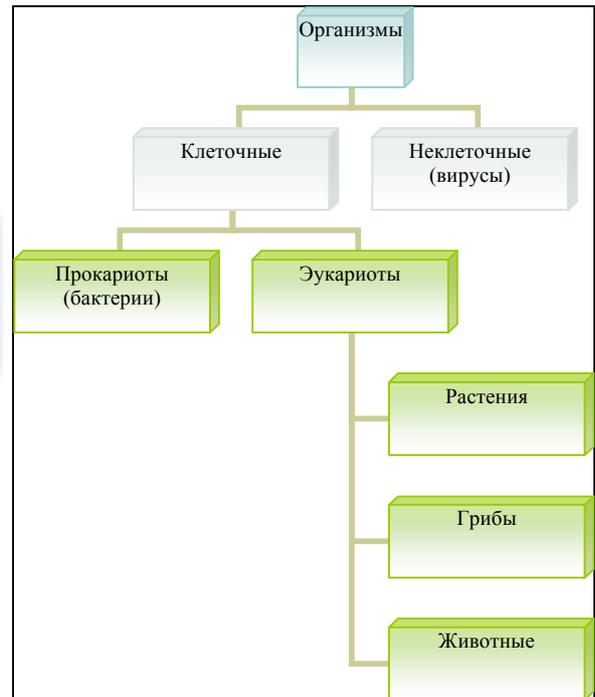


Рис.4. Современная биологическая система

**5. Microsoft Excel: интерфейс и возможности программы, работа с формулами.**

**Выручка от проката автомобилей**

**2013 г.**

	Март	Апрель	Май	Июнь	Август	Сентябрь	Октябрь
4 часа	10500	21000	23000	31000	28000	22000	11900
1 день	3400	5000	10000	11200	13100	10700	4050
1 неделя	5000	60000	70000	72000	58000	41000	20000
Всего	18900	86000	103000	114200	99100	73700	35950

Всего за период: 530850 руб.

## СЧЕТ №275

Дата: 22.10.2018

Курс \$US: 35,58

Код товара	Цена	Колич.	Стоимость	НДС (20%)	Всего, \$	Всего, руб.
A21	31,2	2	62,4	12,48	74,88	2664,23
A42	10,5	2	21	4,2	25,2	896,62
A43	4,72	2	9,44	1,89	11,33	403,05
B5	100,2	3	300,6	60,12	360,72	12834,42
C71	34,2	6	205,2	41,04	246,24	8761,22
C4	13,1	12	157,2	31,44	188,64	6711,81
K9/71	6,45	10	64,5	12,9	77,4	2753,89
K16/24	78,43	5	392,15	78,43	470,58	16743,24
LA8	92,9	1	92,9	18,58	111,48	3966,46
<b>Итого</b>			1305,39	261,08	1566,47	55734,93

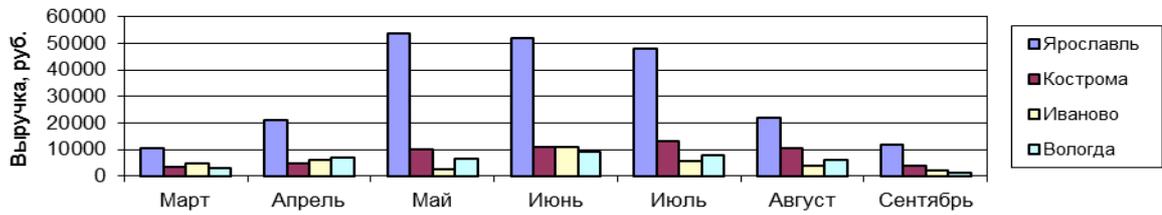
6. Microsoft Excel: работа с таблицами и диаграммами.

## Выручка от проката автомобилей 2003 г.

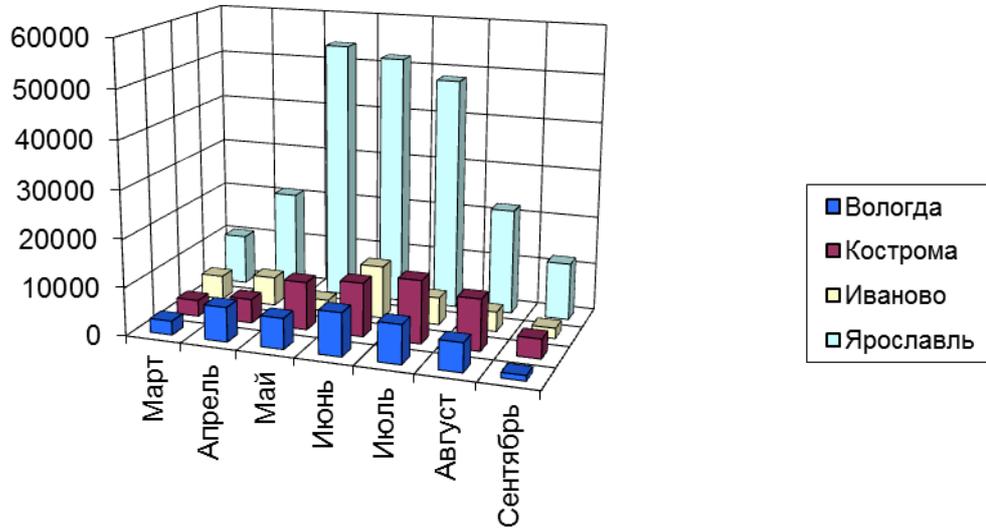
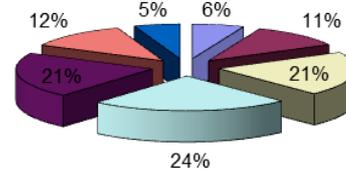
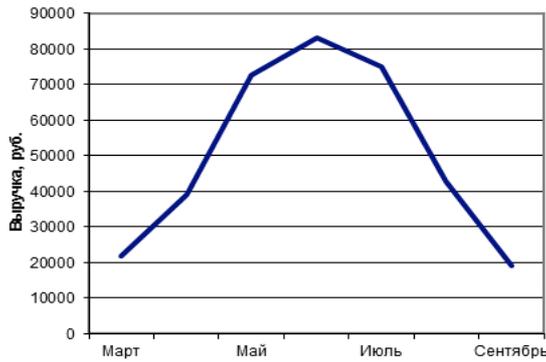
	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь
Ярославль	10500	21000	54000	52000	48200	22000	11900
Кострома	3400	5000	10000	11200	13100	10700	4050

Иваново	5000	6000	2400	11000	5700	4100	2150
Вологда	2900	7200	6400	9000	8100	6000	1100
Всего	21800	39200	72800	83200	75100	42800	19200

**Выручка от проката автомобилей**



**Выручка по месяцам**



## 7. Microsoft PowerPoint: интерфейс и возможности программы, создание презентации.

Задание: создать презентацию на любую тему со следующими условиями:

- не менее 10 слайдов
- использование различных шаблонов слайдов

- наличие выбранной цветовой схему
- наличие хотя бы одной картинке, таблицы, диаграммы, организационной диаграммы, аудио- или видеоклипа
- наличие эффектов анимации.

### **Правила выставления оценки за самостоятельную (лабораторную) работу:**

- Самостоятельная работа оценивается по 2-х балльной системе: «зачтено/незачтено». Для получения оценки «зачтено» студент должен выполнить все задания самостоятельной работы правильно. Если работа не выполнена или выполнена, но имеет грубые ошибки, то ставится оценка «незачтено».

### **Тест по теме «Безопасность в современной информационной среде»**

#### **по теме Правовые основы обеспечения информационной безопасности**

1. Какие положения, связанные с вопросами обработки информации, закреплены в Конституции Российской Федерации?
  - а) Право на неприкосновенность личной и семейной тайны.
  - б) Право на обработку любой информации любым возможным способом.
  - в) Запрет на обработку информации о частной жизни лица без его согласия.
  - г) Право на получение гражданами допуска к государственной тайне.
2. Какие виды информации обязательно требуется защищать в соответствии с законодательством Российской Федерации:
  - а) Информация для служебного пользования.
  - б) Персональные данные.
  - в) Государственная тайна.
  - г) Врачебная тайна.
  - д) Все перечисленные.
3. В соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» информация – это:
  - а) Любые данные, представленные на материальном носителе.
  - б) Сведения (сообщения, данные), независимо от формы их представления.
  - в) Не энергия и не материя.
  - г) Сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.
4. Что из перечисленного можно рассматривать как базу данных в соответствии с законодательством Российской Федерации:
  - а) EXCEL таблицу с упорядоченной и структурированной информацией.
  - б) Файл формата DOC, в котором создан список слушателей этой программы.
  - в) Картотеку регистратуры учреждения здравоохранения.
  - г) Все перечисленные.
5. Целостность информации – это:
  - а) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

- б) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.
  - в) Возможность получения информации и ее использования.
6. На территории Российской Федерации запрещено распространение:
- а) Информации, которая направлена на пропаганду войны.
  - б) Коммерческой тайны.
  - в) Информации, которая направлена на разжигание религиозной ненависти.
  - г) Персональных данных.
7. Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных – это:
- а) Владелец информации.
  - б) Оператор информационной системы.
8. Если не определено иного, оператором информационной системы является:
- а) Владелец информации.
  - б) Собственник используемых для обработки содержащейся в базах данных информации технических средств.
  - в) Лицо, определяющее цели обработки информации и осуществляющее обработку информации.
9. Не может быть ограничен доступ:
- а) К информации о состоянии окружающей среды.
  - б) К персональным данным государственных гражданских служащих.
  - в) К информации, хранящейся в открытых фондах библиотек.
  - г) К сведениям о золотовалютных запасах Российской Федерации.
10. Какую ответственность может повлечь нарушение требований Федеральных законов:
- а) Уголовную.
  - б) Дисциплинарную.
  - в) Административную.
  - г) Гражданско-правовую.
  - д) Все перечисленные.

### **Тест по теме Защита персональных данных**

1. Персональные данные – это:
- а) Сведения о субъекте персональных данных не зависимо от формы их представления.
  - б) Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
  - в) Любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных).
  - г) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
2. На какие отношения не распространяется действие федерального закона «О персональных данных»?

- а) На обработку персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.
  - б) На обработку персональных данных, необходимую для осуществления прав и законных интересов оператора или третьих лиц.
  - в) На обработку персональных данных, необходимую для исполнения судебного акта.
  - г) На обработку персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных.
  - д) На обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
  - е) На обработку персональных данных, необходимую для организации хранения, комплектования, учета и использования содержащих персональных данных архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.
3. Федеральный закон «О персональных данных» регулирует отношения, связанные:
- а) Исключительно с обработкой персональных данных с использованием средств автоматизации.
  - б) С обработкой персональных данных, независимо от того обрабатываются ли они с использованием средств автоматизации или нет.
  - в) С обработкой персональных данных с использованием средств автоматизации, а также с обработкой персональных данных без использования средств автоматизации, если такая обработка соответствует характеру действий, совершаемых с персональными данными с использованием средств автоматизации.
  - г) С обработкой персональных данных без использования средств автоматизации.
4. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных, – это:
- а) Блокирование персональных данных.
  - б) Уничтожение персональных данных.
  - в) Обезличивание персональных данных.
  - г) Перевод персональных данных на архивное хранение.
5. Действия, в результате которых временно прекращается обработка персональных данных, – это:
- а) Блокирование персональных данных.
  - б) Уничтожение персональных данных.
  - в) Обезличивание персональных данных.
  - г) Перевод персональных данных на архивное хранение.
6. Какие из перечисленных действий с персональными данными являются обработкой персональных данных:
- а) Хранение персональных данных.
  - б) Запись персональных данных.
  - в) Обезличивание персональных данных.
  - г) Удаление персональных данных.
7. С точки зрения федерального закона «О персональных данных» оператор – это:
- а) Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

- б) Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
8. Обработка персональных данных:
- а) Не допускается без согласия субъекта персональных данных.
  - б) Должна ограничиваться достижением конкретных, заранее определенных и законных целей.
  - в) Не допускается в случаях несовместимых с целями сбора персональных данных.
  - г) Должна осуществляться на законной и справедливой основе.
9. Обработка персональных данных допускается:
- а) С согласия субъекта персональных данных на обработку его персональных данных.
  - б) В случаях, если она необходима для исполнения судебного акта.
  - в) В случаях, если она необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации.
  - г) В случаях, если ведется обработка персональных данных, подлежащих опубликованию в соответствии с законодательством Российской Федерации.
10. Кто несет ответственность за действия юридического лица, которому поручена обработка персональных данных, перед субъектом персональных данных?
- а) Оператор.
  - б) Юридическое лицо, которому поручили обработку.
  - в) Никто.
  - г) Роскомнадзор.
11. В поручении обработки должны быть обязательно определены и указаны:
- а) Цели обработки персональных данных.
  - б) Субъекты персональных данных, чьи персональные данные будут обрабатываться по поручению.
  - в) Требования к защите обрабатываемых персональных данных.
  - г) Средства защиты информации, которые необходимо применять юридическому лицу, которому поручена обработка персональных данных.
12. На ком лежит обязанность по доказательству получения согласия от субъекта персональных данных?
- а) На Роскомнадзоре.
  - б) На юридическом лице, которому поручили обработку.
  - в) Ни на ком.
  - г) На операторе.
13. Согласие субъекта персональных данных должно включать:
- а) Паспортные данные субъекта персональных данных или его законного представителя.
  - б) Контактные данные лица, ответственного за организацию обработки персональных данных.
  - в) Адрес оператора.
  - г) Фамилии, имена и отчества физических лиц, которые осуществляют обработку персональных данных по поручению оператора.
14. В случае смерти субъекта персональных данных:
- а) Получать согласие на обработку его персональных данных требуется у наследников субъекта персональных данных.
  - б) Получать согласие на обработку его персональных данных требуется у Роскомнадзора.

- в) Получать согласие на обработку его персональных данных не требуется.
15. К специальным категориям персональных данных относятся:
- а) Сведения, касающиеся расовой принадлежности.
  - б) Сведения, касающиеся гражданства.
  - в) Сведения, касающиеся политических взглядов.
  - г) Сведения, касающиеся инвалидности.
16. С точки зрения федерального закона «О персональных данных» к биометрическим персональным данным относятся:
- а) Все сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.
  - б) Сведения, которые вносятся в базу биометрических данных граждан Российской Федерации.
  - в) Все сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются для установления его личности.
17. Кто обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных?
- а) Оператор.
  - б) Юридическое лицо, которому поручили обработку.
  - в) Никто.
  - г) Роскомнадзор.
18. Субъект персональных данных имеет право на получение следующей информации, касающейся обработки его персональных данных:
- а) Правовые основания и цели обработки персональных данных.
  - б) Поименный перечень сотрудников оператора, которые имеют доступ к его персональным данным.
  - в) Сведения об осуществленной или о предполагаемой трансграничной передаче данных.
  - г) Сведения о применяемых оператором средствах защиты информации.
19. Право гражданина на получение информации, касающейся обработки его персональных данных, может быть ограничено:
- а) На основании заявления другого субъекта персональных данных.
  - б) В случаях, если обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности.
  - в) В случаях, если обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка.
  - г) В случаях, если обработка персональных данных осуществляется в рамках законной деятельности средства массовой информации.
20. Контроль и надзор за выполнением мер по обеспечению безопасности персональных данных осуществляет (осуществляют):
- а) Минкомсвязи России.
  - б) Роскомнадзор.
  - в) ФСБ России.
  - г) ФСТЭК России.
21. Какой орган государственной власти имеет право ознакомления с персональными данными при осуществлении контрольных и проверочных мероприятий?
- а) ФСБ России.
  - б) Роскомнадзор.

- в) ФСТЭК России.
22. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, могут быть привлечены:
- а) К уголовной ответственности.
  - б) К дисциплинарной ответственности.
  - в) К административной ответственности.
  - г) К материальной ответственности.

### **Тест по теме Организационные основы обеспечения информационной безопасности**

1. Расположите в правильном порядке этапы работ по обеспечению безопасности информации.
- 1) Оценка соответствия объекта информатизации.
  - 2) Выявление и анализ информационных активов.
  - 3) Проектирование (разработка) системы защиты информации.
  - 4) Формирование требований к защите информации.
  - 5) Внедрение системы защиты информации.
  - 6) Эксплуатация системы защиты информации.
- а) 1) 2) 3) 4) 5) 6).
  - б) 4) 2) 3) 5) 1) 6).
  - в) 2) 4) 3) 5) 6) 1).
  - г) 2) 4) 3) 5) 1) 6).
2. Пусть не обезличенные персональные данные о состоянии здоровья всех граждан Ярославской области обрабатываются в информационной системе, для которой актуальны угрозы связанные с эксплуатацией уязвимостей в прикладном, но не в системном программном обеспечении. Какой уровень защищенности должен быть установлен для таких персональных данных?
- а) У31.
  - б) У32.
  - в) У33.
  - г) У34.
3. Пусть не обезличенные персональные данные в том числе фотография сотрудников небольшого (до 10 000 сотрудников) предприятия обрабатываются в системе контроля и управления доступом, для которой актуальны угрозы не связанные с эксплуатацией уязвимостей в прикладном и системном программном обеспечении. Какой уровень защищенности должен быть установлен для таких персональных данных?
- а) У31.
  - б) У32.
  - в) У33.
  - г) У34.
4. Внешние нарушители реализуют угрозы:
- а) Из внешних сетей связи общего пользования.
  - б) Непосредственно в информационных системах.
  - в) Из сетей международного информационного обмена.
  - г) Находясь в пределах контролируемой зоны.
5. Примерами внешних нарушителей могут являться:
- а) Пользователи информационной системы.

- б) Конкурирующие организации.
  - в) Недобросовестные партнеры.
  - г) Обслуживающий персонал организации.
6. Примерами внутренних нарушителей могут являться:
- а) Администраторы безопасности информационных систем.
  - б) Сторонние физические лица.
  - в) Лица, обеспечивающие сопровождение программного обеспечения.
  - г) Криминальные структуры.
7. К объективным угрозам относятся:
- а) Ошибки обслуживающего персонала.
  - б) Дефекты, сбои и отказы, аварии технических средств и систем объектов информатизации, а так же систем обеспечения объектов информатизации.
  - в) Природные явления, стихийные бедствия.
  - г) Факторы социально-политического характера.
8. Угрозы утечки информации возможны посредством:
- а) Воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.
  - б) Передачи информации по открытым каналам связи.
  - в) Подключения к техническим средствам и системам объекта информатизации.
  - г) Обработки информации на незащищенных технических средствах обработки информации.
9. Угрозы несанкционированного доступа к информации, реализуются путем:
- а) Копирования информации на незарегистрированный носитель информации.
  - б) Хищения носителя защищаемой информации.
  - в) Использования программного обеспечения технических средств информационной системы, через применение вредоносного программного кода.
  - г) Силового электромагнитного воздействия по проводным линиям связи на порты ввода-вывода сигналов и порты связи.
10. Какие средства защиты информации обычно применяются для обеспечения безопасности информации, обрабатываемой на автономных компьютерах:
- а) Средства защиты информации от несанкционированного доступа.
  - б) Межсетевые экраны.
  - в) Средства криптографической защиты информации.
  - г) Средства антивирусной защиты.
  - д) Системы обнаружения вторжений.
11. Какие средства защиты информации позволяют обеспечить безопасность информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны:
- а) Средства защиты информации от несанкционированного доступа.
  - б) Межсетевые экраны.
  - в) Средства криптографической защиты информации.
  - г) Системы обнаружения вторжений.
12. Какой вид средств защиты информации позволяет контролировать различные каналы передачи информации: электронную почту, месенджеры, съемные носители информации?
- а) IPS.
  - б) DLP.
  - в) IDS.
  - г) CSP.
13. Аттестация объектов информатизации – это:

- а) Документальное удостоверение соответствия продукции или иных объектов, процессов проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.
  - б) Прямое или косвенное определение соблюдения требований, предъявляемых к объекту защиты.
  - в) Официальное признание компетентности физического или юридического лица выполнять работы в определенной области.
  - г) Комплекс организационно-технических мероприятий, в результате которых посредством специального документа подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.
14. Какой документ дает право обработки информации с указанным в нем уровнем конфиденциальности?
- 1) Лицензия.
  - 2) Аттестат аккредитации.
  - 3) Сертификат.
  - 4) Аттестат соответствия.
15. На настоящий момент срок действия аттестата соответствия информационной системы, в которой обрабатывается конфиденциальная информация, в случае, если в ходе ее эксплуатации, в нее не вносятся существенные изменения, составляет:
- а) 3 года.
  - б) 5 лет.
  - в) Весь срок эксплуатации информационной системы.
16. Тестирование на проникновение – это скорее:
- а) Анализ уязвимостей информационной системы.
  - б) Испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе.

### **Тест по теме Введение в информационную безопасность операционных систем**

1. Пусть в ОС реализовано дискреционное управление доступом со следующими правами: чтение(r), запись(w) и исполнение(x). Присутствует файл приложения «Калькулятор.exe» со следующим списком доступа: (Алиса: rwx), (Борис: rx). Выберите правильные утверждения:
- а) Алиса может запустить приложение «Калькулятор.exe».
  - б) Борис не может запустить приложение «Калькулятор.exe».
  - в) Алиса не может изменить содержимое файла «Калькулятор.exe».
  - г) Борис может изменить содержимое файла «Калькулятор.exe».
2. Пусть в ОС реализовано групповое управление доступом со следующими правами: чтение(r), запись(w) и исполнение(x). Присутствует файл «Накладная.docx» со следующим списком доступа: (Бухгалтеры: rw), (Курьеры: r), (Алиса: rw). В системе заданы роли, в которые включены соответствующие пользователи: (Бухгалтеры: Борис, Галина), (Курьеры: Виктор). Выберите правильные утверждения:
- а) Борис не может изменить содержимое файла «Накладная.docx».
  - б) Галина может читать содержимое файла «Накладная.docx».
  - в) Виктор может изменить содержимое файла «Накладная.docx».

- г) Виктор может читать содержимое файла «Накладная.docx».
- д) Алиса может изменить содержимое файла «Накладная.docx».
3. Пусть в ОС реализовано мандатное управление доступом. Присутствует файл «log.txt» с уровнем секретности 1. Присутствуют пользователи Алиса с уровнем допуска 1, Борис с уровнем допуска 2 и Виктор с уровнем допуска 0. Выберите правильные утверждения:
- а) Виктор может изменить содержимое файла «log.txt».
- б) Виктор может читать содержимое файла «log.txt».
- в) Алиса может изменить содержимое файла «log.txt».
- г) Алиса может читать содержимое файла «log.txt».
- д) Борис может изменить содержимое файла «log.txt».
- е) Борис может читать содержимое файла «log.txt».
4. Пусть в ОС реализована модель целостности Биба. Присутствует файл «log.txt» с уровнем целостности 1. Присутствуют пользователи Алиса с уровнем целостности 1, Борис с уровнем целостности 2 и Виктор с уровнем целостности 0. Выберите правильные утверждения:
- а) Виктор может изменить содержимое файла «log.txt».
- б) Алиса может изменить содержимое файла «log.txt».
- в) Борис может изменить содержимое файла «log.txt».
- г) Все трое могут читать содержимое файла «log.txt».
5. Выберите правильные утверждения о аутентификации в современных ОС:
- а) Пароли пользователя хранятся на диске, на котором установлена система, в первоначальном виде.
- б) Эталонные значения, необходимые для прохождения биометрической аутентификации, хранятся в системе в недостаточном для восстановления изначальных биометрических данных объеме.
- в) Токен физически изготовлен таким образом, что считывание с него закрытого ключа является невозможной или дорогостоящей операцией.
- г) Для аутентификации с помощью токена в системе должен присутствовать открытый ключ пользователя, соответствующий закрытому ключу на его токене.
6. Что не входит в метаданные файла (выберите один вариант)?
- а) Время создания файла.
- б) Адрес корневой директории.
- в) Время модификации файла.
- г) Адреса кластеров содержимого файлов.
- д) Информация о владельце файла.
7. Выберите верные утверждения о управлении памятью в современных ОС:
- а) Современные ОС используют виртуальную память.
- б) Современные ОС не защищают память одних процессов от чтения другими процессами.
- в) Современные ОС разделяют общую память между процессами, часто в такой памяти находятся библиотеки.
- г) Современные ОС никогда не выгружают части оперативной памяти на диск во время работы.
- д) В современных ОС память разбита на маленькие фрагменты, называемые страницами.
8. Выберите верные утверждения о планировщике:
- а) Планировщик выделяет процессорное время короткими интервалами, называемыми квантами.

- б) В случае исполнения процессом инструкции, для завершения которой требуется длительное ожидание, планировщик переводит процесс в состояние «заблокирован» и не будет выделять ему процессорное время, пока состояние не сменится на «готов».
- в) Для работы планировщика процессы должны сами передавать на него управление, так как компьютеры не предоставляют ОС механизма для периодического прерывания выполнения пользовательского процесса.
- г) В планировании по приоритетам все процессы с разными приоритетами получают примерно одинаковое количество времени.
9. Выберите верное утверждение (выберите один вариант):
- а) ОС реализована аппаратно в процессоре.
- б) ОС реализована аппаратно в материнской плате.
- в) ОС – программное обеспечение, которое предоставляет приложениям ресурсы аппаратного обеспечения компьютера в виде удобных абстракций, но не управляет этим аппаратным обеспечением.
- г) ОС – программное обеспечение, которое предоставляет приложениям ресурсы аппаратного обеспечения компьютера в виде удобных абстракций и управляет этим аппаратным обеспечением.
10. Выберите верное утверждение (выберите один вариант):
- а) В ОС компьютера с одноядерным процессором в каждый момент времени может работать только один процесс.
- б) В ОС компьютера с одноядерным процессором у процессов всегда присутствует только один поток.
- в) В ОС компьютера с многоядерным процессором в конкретный момент времени могут выполняться несколько потоков одного процесса.
- г) В ОС компьютера с многоядерным процессором конкретный процесс может использовать только одно ядро процессора.

### **Тест по теме Информационная безопасность операционных систем семейства Windows**

1. На основе каких данных субъекта ОС Windows принимает решение о доступе?
- а) Хеш значение пароля пользователя, запустившего процесс.
- б) Токен перевоплощения.
- в) Идентификатор процесса.
- г) Токен доступа.
- д) Базовый приоритет процесса.
2. На основе каких данных объекта ОС Windows принимает решение о доступе?
- а) Привилегии.
- б) Токен доступа.
- в) Deskriptor безопасности.
- г) Системный список управления доступом.
- д) Способ аутентификации пользователя.
3. Какие примитивные права объединяет в себе право чтения ОС Windows?
- а) «Чтение атрибутов безопасности».
- б) «Чтение системных атрибутов», «чтение атрибутов безопасности».
- в) «Чтение данных».
- г) «Чтение системных атрибутов», «чтение атрибутов безопасности», «чтение данных».

- д) «Чтение системных атрибутов», «чтение атрибутов безопасности», «чтение данных», «выполнение файлов» и «переход в директорию».
4. Выберите правильные утверждения о мандатной политике «Не-Записывать-Вверх» ОС Windows:
- а) Обеспечивает свойство целостности данных.
  - б) Обеспечивает свойство конфиденциальности данных.
  - в) Используется в системе только для объектов сетевых сокетов.
  - г) Неявно используется для всех NTFS-файлов.
  - д) Разрешает доступ на запись только субъектам с уровнем целостности равным или большим по отношению к уровню целостности объекта доступа.
5. Какие из перечисленных прав ОС Windows предоставляет по умолчанию владельцу файла?
- а) Читать ССУД.
  - б) Читать ДСУД.
  - в) Читать содержимое файла.
  - г) Изменять ДСУД.
  - д) Изменять ССУД.
  - е) Изменять содержимое файла.
6. Выберите правильные утверждения относительно алгоритма определения правомерности доступа ОС Windows:
- а) Первым действием является проверка соответствия доступа мандатной политике.
  - б) Проверка соответствия доступа мандатной политике осуществляется после анализа записей ДСУД.
  - в) Если при последовательном анализе записей ДСУД оказывается, что одно из запрашиваемых прав запрещается в текущей записи, то доступ запрещается.
  - г) Если при последовательном анализе записей ДСУД разрешающие права текущей записи в сумме с разрешающими правами предыдущих записей перекрыли все запрашиваемые права, то доступ разрешается.
  - д) Если в списках ДСУД не было запрещающих запрашиваемые права записей, и в то же время все разрешающие записи не перекрыли запрашиваемые права, то доступ запрещается.
7. Какая привилегия ОС Windows позволяет читать любой файл вне зависимости от заданных прав?
- а) Привилегия создания резервных копий.
  - б) Привилегия изменения системного времени.
  - в) Привилегия завершения работы системы.
  - г) Привилегия увеличения рабочего набора.
  - д) Привилегия создания файла подкачки.
8. Выберите сущности, не входящие в токен доступа в ОС Windows:
- а) SID пользователя.
  - б) ДСУД всех объектов системы.
  - в) SID-ы групп.
  - г) ССУД всех объектов системы.
  - д) Привилегии.
9. Выберите сущности, входящие в дескриптор безопасности объекта в ОС Windows:
- а) SID владельца объекта.
  - б) Дискреционный список управления доступом.
  - в) Системный список управления доступом.
  - г) Список токенов доступа процессов, осуществляющих доступ к объекту.
  - д) Уровень целостности.

10. Какие из пунктов правильно описывают фильтрованный токен доступа администратора в ОС Windows?
- а) Уровень целостности устанавливается средним.
  - б) Уровень целостности устанавливается высоким.
  - в) Список привилегий, которые могут попасть в фильтрованный токен, сильно ограничен.
  - г) При определении правомерности доступа среди записей ДСУД с SID административных групп будут учтены только запрещающие.
  - д) Списки привилегий одинаковы в обычном и фильтрованном токене доступа администратора.

### **Тест по теме Информационная безопасность операционных систем семейства Linux**

1. На основе каких данных субъекта ОС Linux принимает решение о доступе?
  - а) SUID-бит.
  - б) Sticky-бит.
  - в) Учетные данные.
  - г) UID процесса.
  - д) Электронная подпись программы.
2. Какие права присутствуют в ОС Linux:
  - а) Исполнение.
  - б) Чтение i-node.
  - в) Чтение.
  - г) Удаление.
  - д) Запись.
3. Для чего служит SUID-бит в ОС Linux?
  - а) Позволяет запустить приложение от имени владельца файла приложения.
  - б) Позволяет запустить приложение от имени суперпользователя.
  - в) Позволяет запустить приложение с привилегией CAP\_SYS\_ADMIN.
  - г) Позволяет запустить приложение с UID равным нулю.
  - д) Запрещает запуск приложения всем пользователям, кроме суперпользователя.
4. Что делает маска в списке управления доступом файла в ОС Linux?
  - а) Задаёт максимальные права, которые можно получить из записей для групп.
  - б) Задаёт максимальные права, которые можно получить из записи остальных.
  - в) Задаёт максимальные права, которые можно получить из записи владельца файла.
  - г) Задаёт максимальные права, которые можно получить из записей для пользователей и групп.
  - д) Задаёт максимальные права, которые можно получить из записей для пользователей.
5. Что такое соль хеш-значения пароля в ОС Linux?
  - а) Строка, которая выбирается при каждой аутентификации случайно для обеспечения безопасности пароля.
  - б) Случайно выбранная при создании пароля строка, которая склеивается с хеш-значением после вычисления хеш-функции.
  - в) Случайно выбранная при создании пароля строка, которая склеивается с паролем перед вычислением хеш-функции.
  - г) Длина, до которой урезается пароль пользователя для компактного хранения в системе.
6. Выберите сущности, входящие в учетные данные процесса в ОС Linux:

- а) UID пользователя, запустившего процесс.
  - б) Группы пользователя, запустившего процесс.
  - в) Привилегии.
  - г) Права исполняемого файла, из которого был запущен процесс.
  - д) Флаг эффективности привилегий.
7. Выберите сущности, входящие в атрибуты безопасности файла в ОС Linux:
- а) Тройка прав для каждой группы в системе.
  - б) Привилегии.
  - в) Тройка прав владельца файла.
  - г) Тройка прав пользователей, не являющихся владельцами файла и не входящих в группу владельца файла по умолчанию.
  - д) Владелец файла.
8. Выберите сущности, входящие в атрибуты безопасности файла в ОС Linux:
- а) Тройка прав для каждой группы в системе.
  - б) Привилегии.
  - в) Тройка прав владельца файла.
  - г) Тройка прав пользователей, не являющихся владельцами файла и не входящих в группу владельца файла по умолчанию.
  - д) Владелец файла.
9. Какие наборы привилегий есть у файла в ОС Linux:
- а) Наследуемые.
  - б) Эффективные.
  - в) Внешние.
  - г) Ограничивающие.
  - д) Разрешенные.
10. Какую хеш-функцию использует ОС Linux для вычисления хеш-значения пароля в ОС Linux?
- а) MD-5.
  - б) SHA-256.
  - в) SHA-512.
  - г) SHA-3.
  - д) Функций несколько, около хеш-значения пароля хранится номер использованной хеш-функции.
11. Что делает конвейер в ОС Linux?
- а) Фильтрует вывод команды.
  - б) Перенаправляет стандартный вывод команды с консоли стандартный на вход другой команде.
  - в) Поднимает права до прав суперпользователя.
  - г) Откладывает выполнение команды на указанный срок.

### **Тест по теме Введение в архитектуру локальных вычислительных сетей**

1. Какой порядок уровней модели OSI верный?
- а) Физический, канальный, транспортный, сетевой, сеансовый, представления, прикладной.
  - б) Физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной.
  - в) Физический, канальный, сетевой, транспортный, сеансовый, прикладной, представления.

- г) Физический, канальный, транспортный, сетевой, сеансовый, прикладной, представления.
2. Какие протоколы относятся к транспортному уровню модели OSI?
    - а) UDP.
    - б) ARP.
    - в) IPv4.
    - г) GSM.
    - д) TCP.
    - е) DNS.
    - ж) PPTP.
  3. Какой уровень предназначен для определения пути передачи данных?
    - а) Физический.
    - б) Сеансовый.
    - в) Транспортный.
    - г) Представления.
    - д) Канальный.
    - е) Прикладной.
    - ж) Сетевой.
  4. Какие флаги используются в протоколе TCP для установления соединения?
    - а) RST.
    - б) SYN.
    - в) FIN.
    - г) URG.
    - д) ACK.
    - е) PSH.
  5. Какие преимущества есть у FTTB?
    - а) Высокая скорость работы Интернет.
    - б) Равная скорость приема и передачи информации.
    - в) Независимость скорости доступа от числа абонентов, подключенных к коммутатору.
    - г) Отсутствие необходимости размещения коммутатора провайдера в здании.
  6. Какие недостатки есть у FTTB?
    - а) Низкая скорость работы Интернет.
    - б) Разная скорость приема и передачи информации.
    - в) Зависимость скорости доступа от числа абонентов, подключенных к коммутатору.
    - г) Необходимость размещения коммутатора провайдера в здании.
  7. Выберите верные утверждения
    - а) TCP не гарантирует доставку датаграмм.
    - б) UDP не гарантирует доставку датаграмм.
    - в) UDP гарантирует доставку датаграмм.
    - г) TCP гарантирует доставку датаграмм.
  8. Какой адрес относится к адресному пространству IPv4?
    - а) 192.168.0.17
    - б) 129.256.0.0
    - в) 301.169.107.0.0.3
    - г) 127.0.1000.0
  9. Как работает концентратор (хаб)?
    - а) При получении пакета данных хаб пересылает этот пакет на все остальные свои порты.

- б) При получении пакета данных хаб пересылает этот пакет на порт в соответствии с таблицей MAC-адресов. Если соответствия нет, пакет отбрасывается.
  - в) При получении пакета данных хаб пересылает этот пакет на порт в соответствии с таблицей MAC-адресов. Если соответствия нет, в сеть отправляется ARP-запрос.
10. Как работает коммутатор?
- а) В случае, если для отправляемого MAC-адреса нет соответствия, коммутатор рассылает пакеты на все порты, кроме порта-получателя.
  - б) При получении пакета данных коммутатор пересылает этот пакет на все остальные свои порты.
  - в) Коммутатор хранит в памяти таблицу коммутации, в которой указано сопоставление MAC-адреса и номера порта коммутатора.
  - г) Со временем коммутатор строит таблицу для всех активных MAC-адресов.
  - д) Таблица MAC-адресов коммутатора статична и настраивается вручную.

### Тест по теме Сетевые угрозы и методы противодействия им

1. Какие бывают источники возникновения уязвимостей?
  - а) Ошибки реализации.
  - б) Ошибки обслуживания.
  - в) Ошибки проектирования.
  - г) Ошибки HR-отдела.
2. Что не входит в базовую группу метрик CVSS?
  - а) Способ получения доступа.
  - б) Влияние на конфиденциальность.
  - в) Влияние на пользователя.
  - г) Показатель аутентификации.
  - д) Сложность получения доступа.
3. Какой группы метрик CVSS не существует?
  - а) Комплексная.
  - б) Временная.
  - в) Базовая.
  - г) Контекстная.
4. Кем разработана CVSS?
  - а) ISO.
  - б) FIRST.
  - в) WWW.
  - г) UCLA.
5. Что не является метрикой в CVSS?
  - а) Сложность атаки.
  - б) Влияние на доступность.
  - в) Длительность атаки.
  - г) Способ получения доступа.
  - д) Показатель аутентификации.
6. Что является пассивной атакой?
  - а) Прослушивание трафика.
  - б) Отказ в обслуживании.
  - в) Физическое нападение на объект.
  - г) Эксплуатация уязвимости.
7. Что такое эвристический анализ?
  - а) Метод, предназначенный для обнаружения новых, еще не выявленных вирусов.

- б) Механизм, необходимый для отслеживания неизменности файлов, документов, реестра, конфигурации оборудования.
  - в) Метод, основанный на последовательном просмотре памяти устройства, загрузочных секторов, файлов в поиске сигнатур известных вирусов.
8. Что такое бэкдор?
- а) Часть вредоносного программного обеспечения, реализованного для сокрытия присутствия этого вредоносного кода и его действий.
  - б) Приложение, используемое для дальнейшей загрузки и запуска полноценного вредоносного программного обеспечения.
  - в) Вредоносное программное обеспечение, которое, помимо получения контроля над зараженным устройством, пытается захватить под свой контроль другие узлы сети.
  - г) Приложение, позволяющее управлять компьютером удаленно.
9. Что такое руткит?
- а) Часть вредоносного программного обеспечения, реализованного для сокрытия присутствия этого вредоносного кода и его действий.
  - б) Приложение, используемое для дальнейшей загрузки и запуска полноценного вредоносного программного обеспечения.
  - в) Вредоносное программное обеспечение, которое, помимо получения контроля над зараженным устройством, пытается захватить под свой контроль другие узлы сети.
  - г) Приложение, позволяющее управлять компьютером удаленно.
10. Что следует делать, чтобы защитить себя от вирусов?
- а) Не запускать приложения из недоверенных источников.
  - б) Следить за цифровыми подписями устанавливаемого программного обеспечения.
  - в) Отключить межсетевой экран.
  - г) Всегда открывать вложения электронной почты с темой «Важно» и «Срочно».
  - д) Своевременно обновлять операционную систему и программное обеспечение.
  - е) Использовать антивирусное программное обеспечение.

### **Тест по теме Межсетевые экраны**

1. Что такое межсетевой экран?
- а) Программное или программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков.
  - б) Устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.
  - в) Устройство, которое позволяет организовать локальную сеть с возможностью выхода в интернет для других устройств.
2. Межсетевые экраны для веб-приложений располагают:
- а) Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу).
  - б) После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану).
  - в) Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен.
  - г) Вместо защищаемого веб-сервера.
3. Персональные межсетевые экраны для настольных компьютеров и ноутбуков:

- а) Обеспечивают дополнительный уровень защиты от сетевых атак.
  - б) Полностью заменяют все остальные инструментальные средства обеспечения безопасности.
  - в) Полностью заменяют маршрутизаторы, являясь шлюзом по умолчанию для защищаемого компьютера или ноутбука.
  - г) Предоставляют все необходимые сетевые сервисы для защищаемого компьютера или ноутбука.
4. Персональные межсетевые экраны для настольных компьютеров и ноутбуков являются:
- а) Аппаратно-программными средствами защиты.
  - б) Всегда встроенными в ОС, которую они защищают; не могут быть реализованы внешними производителями.
  - в) Исключительно программными.
  - г) Исключительно внешними, не встроенными в ОС, которую они защищают; всегда реализованы внешними производителями.
5. Персональные межсетевые экраны для настольных компьютеров и ноутбуков устанавливаются:
- а) На хостах, которые они защищают.
  - б) На маршрутизаторах, которые указаны на хосте в качестве шлюза по умолчанию.
  - в) На отдельных компьютерах.
  - г) На конечных точках VPN.
6. Выберите несуществующий вид трансляции сетевых адресов.
- а) Динамическая.
  - б) Статическая.
  - в) С использованием портов.
  - г) С использованием мостов.
7. Шлюзы уровня приложений позволяют:
- а) Исключить прямое взаимодействие двух узлов путем реализации роли посредника.
  - б) Выполнять функции шлюза сеансового уровня.
  - в) Анализировать все существующие в мире протоколы.
  - г) Анализировать только поддерживаемые этим межсетевым экраном протоколы.
8. Управляемые коммутаторы могут:
- а) Осуществлять фильтрацию на основе IP-адресов.
  - б) Осуществлять фильтрацию по используемому протоколу.
  - в) Осуществлять фильтрацию на основе MAC-адреса.
  - г) Осуществлять фильтрацию на основе VLAN ID.
9. Выберите возможности межсетевого экрана.
- а) Регистрация событий и генерация отчетов.
  - б) Фильтрация трафика.
  - в) Трансляция сетевых адресов.
  - г) Аутентификация пользователей.
  - д) Администрирование.
10. Какие утверждения о программном межсетевом экране верны?
- а) Подходит в случаях, когда устройство пользователя помещается в недоверенную среду.
  - б) При его работе используются ресурсы устройства, на котором он функционирует.
  - в) Подходит для задач сегментирования сетей.

- г) Подходит для отделения доверенной части сети от внешних угроз.
- д) Считается более отказоустойчивым, чем аппаратный межсетевой экран.

**Тест по теме Введение в криптографические методы защиты информации**

1. Каждый шифротекст может быть получен как результат следующего преобразования:
  - а)  $E_k(D_k(p))$ .
  - б)  $D_k(p)$ .
  - в)  $E_k(p)$ .
  - г.  $D_k(E_k(p))$ .
2. Зашифруйте с помощью шифра «Атбаш» слово «World».

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

- а) Dlrow.
  - б) Svood.
  - в) Woild.
  - г) Dliow.
3. Рассшифруйте слово «Xjхов», зашифрованное с помощью шифра Гая Юлия Цезаря:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

- а) Tgtly.
  - б) Amare.
  - в) Crupt.
  - г) Vivna.
4. Зашифруйте слово «Жизнь» с помощью перестановки

1	2	3	4	5
2	5	3	1	4

- а) Нжзы.
  - б) Ёнзиж.
  - в) Нзьжи.
  - г) Иьзжн.
5. Расшифруйте слово «1216312611» с помощью таблицы Полибия:

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	Ы	Е	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	*	*	*

- а) Белка.
  - б) Ёэвюа.
  - в) Стрелка.
  - г) Белок.
6. Впервые метод частотного криптоанализа впервые изложил:
    - а) Леон Баттиста Альберти.

- б) Франческо Симонетта.  
 в) Абу Юсуф Якуб аль-Кинди.  
 г) Джироламо Кардано.
7. Диск Альберти позволяет автоматизировать:  
 а) Шифр простой замены (одноалфавитный шифр).  
 б) Многоалфавитный шифр.  
 в) Шифр перестановки.  
 г) Поточный шифр.
8. Использование пароля для мнемонического запоминания перестановки символов алфавита предложил:  
 а) Матео Ардженти.  
 б) Блез де Виженер.  
 в) Джованни Баттиста Беллазо.  
 г) Джамбаттиста (Джованни) делла Порта.
9. Помещение для перлюстрации переписки в XVII – XX веках называлось:  
 а) Белый кабинет.  
 б) Тайная комната.  
 в) Янтарная комната.  
 г) Черный кабинет.  
 д) Красный кабинет.
10. Шифры, в которых каждый символ открытого текста преобразуется в символ шифротекста, в зависимости от своего расположения в открытом тексте и ключа называются:  
 а) Многоалфавитными шифрами.  
 б) Блочными шифрами.  
 в) Поточными шифрами.  
 г) Роторными шифрами.
11. Зашифруйте слово «СЛОН» биграммным шифром Плейфера.

У	Ч	О	Ь	В
Ж	Т	Э	Н	Ф
Ш	Г	Л	Б	П
М	Я	Ц	З	Р
С	Е	А	Ы	К
Ю	Д	Щ	И	Х

- а) ВАБИ.  
 б) ШАЭЬ.  
 в) ЭЦУЫ.  
 г) ЫЦЦЗ.
12. Пусть перестановка  $T$  представлена следующей таблицей:

1	2	3	...	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	$n$
5	6	7	...	$n-1$	$n$	1	2	3	4

13. Какой вид имеет перестановка обратная перестановке  $T$ ?

а.

1	2	3	...	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	$n$
1	2	3	...	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	$n$

б.

1	2	3	...	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	$n$
4	3	2	...	10	9	8	7	6	5

в.

1	2	3	...	$n-4$	$n-3$	$n-2$	$n-1$	$n$
4	5	6	...	$n-1$	$n$	1	2	3

г.

1	2	3	4	5	...	$n-3$	$n-2$	$n-1$	$n$
$n-3$	$n-2$	$n-1$	$n$	1	...	$n-7$	$n-6$	$n-5$	$n-4$

14. Зашифруйте с помощью открытого ключа (8051, 5) криптосистемы RSA сообщение  $m = 10$ .
- 8051.
  - 3388.
  - 1949.
  - 12.
15. Какое свойство безопасности гарантирует, что участнику криптографического протокола целостности полученного сообщения и его создание до момента получения, но не гарантирует защиту от повторной отправки сообщения?
- Свойство «аутентификация сторон».
  - Свойство «аутентификация источника».
  - Свойство «инвариантность отправителя».
  - Свойство «аутентификация сообщения».
16. Какое свойство безопасности гарантирует, что участнику криптографического протокола, что участники, начавшие исполнение протокола, не изменились с течением времени?
- Свойство «аутентификация сторон».
  - Свойство «аутентификация источника».
  - Свойство «инвариантность отправителя».
  - Свойство «аутентификация сообщения».

## 1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

### Список вопросов к зачету

- Определение вычислительной техники, вычислительной системы, ЭВМ.
- История появления и развития ЭВМ.
- Различные классификации ЭВМ.
- Архитектура вычислительной системы.
- Классификация компьютеров (по назначению, уровню специализации, размеру).
- Определение и базовая конфигурация персонального компьютера. Основные узлы системного блока.
- Назначение и строение материнской платы. Основные устройства, расположенные на материнской плате.
- Назначение и основные характеристики центрального процессора.
- Назначение и основные характеристики оперативной памяти.
- Назначение и основные характеристики жестких дисков.
- Назначение, классификация и основные характеристики приводов для оптических дисков.

12. Назначение, классификация и основные характеристики мониторов.
13. Назначение, классификация и основные характеристики видеоадаптеров.
14. Назначение и основные характеристики клавиатуры, опциональная классификация клавиш. Назначение и типы манипуляторов.
15. Назначение, классификация и основные характеристики принтеров.
16. Назначение, классификация и основные характеристики модемов.
17. Понятие информации. Общий способ хранения и обработки информации в компьютере. Понятия двоичного кода, бита, байта.
18. Понятия файла, каталога, диска, файловой системы.
19. Имя и расширение файлов. Типы файлов. Поиск файлов.
20. Понятия и основные свойства алгоритма и программы.
21. Базовый и системный уровни программного обеспечения. Примеры программ.
22. Служебный уровень программного обеспечения. Примеры программ.
23. Прикладной уровень программного обеспечения. Примеры программ.
24. Понятие, назначение и классификация баз данных. Понятия предметной области, сущности, атрибута, записи, поля записи.
25. Программное обеспечение для работы с базами данных. Ключевые поля, связь между таблицами. Понятия запроса и языка SQL.
26. Алгоритмизация и программирование. Понятие языка программирования. Классификация и примеры языков программирования.
27. Понятие среды программирования. Структура программы. Понятия блок-схемы и оператора. Операторы присваивания, условия, цикла.
28. Понятие и различные классификации компьютерных сетей. Понятия пакета, сетевого протокола. Понятия сетевых служб, сервера и клиента. Примеры.
29. Технологии локальных сетей. Проводные и беспроводные сети.
30. Технологии глобальных сетей. IP-адреса и доменные имена. Структура глобальной сети Internet. Поиск информации в сети Internet.

### **Правила выставления оценки на зачете:**

Допуском к зачету является:

- выполненных всех самостоятельных работ по темам №№ 1-6;
- успешное прохождение онлайн курса «Безопасность в современной информационной среде» на площадке MOOK ЯрГУ им. П.Г. Демидова (DemidOnline) (зачет по итогам изучения темы № 7).

Ответ студента на зачете оценивается по 2-х балльной системе.

Отметка «зачтено» ставится, если:

- знания отличаются глубиной и содержательностью, дается полный исчерпывающий ответ, как на основные вопросы к зачету, так и на дополнительные;
- студент свободно владеет научной терминологией;
- ответ студента структурирован, содержит анализ существующих теорий, научных школ, направлений и их авторов;
- ответ студента логично и доказательно раскрывает проблему, предложенную для решения;
- ответ студента характеризуется глубиной, полнотой и не содержит фактических ошибок;
- ответ студента иллюстрируется примерами, в том числе из собственной научно-исследовательской деятельности;

- студент демонстрирует умение аргументировано вести диалог и научную дискуссию;

- студент демонстрирует навыки поиска и обработки научной информации и экспериментальных данных.

Отметка «незачтено» ставится, если:

- ответ студента обнаружил незнание или непонимание сущностной части дисциплины;

- содержание вопросов не раскрыто, допускаются существенные фактические ошибки, которые студент не может исправить самостоятельно;

- на большую часть дополнительных вопросов по содержанию зачета студент затрудняется дать ответ или не дает верных ответов;

- студент не демонстрирует навыки поиска и обработки научной информации и экспериментальных данных.