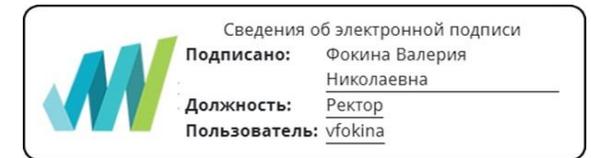


**Автономная некоммерческая организация высшего образования  
«Открытый университет экономики, управления и права»  
(АНО ВО ОУЭП)**

УТВЕРЖДАЮ

Ректор АНО ВО ОУЭП Фокина В.Н.



«25» июня 2024 г.

Решение Ученого Совета АНО ВО ОУЭП

Протокол № 11 от «25» июня 2024 г.

09.03.01 «Информатика и вычислительная техника»

Направленность (профиль): Информатика и вычислительная техника

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (МАТЕРИАЛОВ)**

Приложение 1  
по компетенциям

Оценочные материалы для проверки сформированности компетенции

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

## Оценочные материалы для проверки сформированности компетенции

**ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**

ОПК-3.1. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры, с применением информационно-коммуникационных технологий

ОПК-3.2. Самостоятельно проводит научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Компетенция формируется дисциплинами:

Основы теории передачи информации	4 семестр
Сети и телекоммуникации	6 семестр
Защита информации	6 семестр

## Вопросы и задания для проверки сформированности компетенции

### Дисциплина «Защита информации»

Разъясните основные понятия:

№	Понятие	Определение
1.	Методы и средства защиты информации	Методы и средства защиты информации – это организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и

		эксплуатации компьютерной системы для обеспечения защиты информации.
2.	Политика безопасности	Политика безопасности — это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.
3.	Угроза безопасности информации	Угроза безопасности информации в компьютерной системе – это событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.
4.	Утечка	Утечка – это неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками.
5.	Уязвимость информации	Уязвимость информации – это возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
6.	Целостность информации	Целостность информации – неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.
7.	Собственник информационных ресурсов, систем и технологий	Собственник информационных ресурсов, систем и технологий – это субъект с полномочиями владения, пользования и распоряжения указанными объектами.
8.	Разглашение	Разглашение – это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати).

9.	Непреднамеренное воздействие	Непреднамеренное воздействие на защищаемую информацию - воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий (например, уничтожение документов в результате отказа накопителя на жестком магнитном диске компьютера).
10.	Конфиденциальность информации	Конфиденциальность информации – это известность ее содержания только имеющим соответствующие полномочия субъектам.

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Что такое умышленная угроза информационной безопасности?	<p>К умышленным угрозам относятся:</p> <ul style="list-style-type: none"> <li>– несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);</li> <li>– несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.</li> </ul>
2.	Что относится к непреднамеренным угрозам компьютерных систем?	<p>К непреднамеренным угрозам относятся:</p> <ul style="list-style-type: none"> <li>– ошибки в проектировании КС;</li> <li>– ошибки в разработке программных средств КС;</li> <li>– случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;</li> <li>– ошибки пользователей КС;</li> <li>– воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной</li> </ul>

		совместимости) и др.
3.	Какие существуют непосредственные каналы утечки информации?	<p>Непосредственными каналами утечки информации являются:</p> <ul style="list-style-type: none"> <li>– хищение носителей информации;</li> <li>– сбор производственных отходов с информацией (бумажных и магнитных носителей);</li> <li>– копирование носителей информации;</li> <li>– намеренное использование для несанкционированного доступа к информации незаблокированных терминалов других пользователей КС;</li> <li>– маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т. п.);</li> <li>– обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.</li> </ul>
4.	Какие существуют косвенные каналы утечки информации?	<p>Косвенными каналами утечки называют каналы, не связанные с физическим доступом к элементам КС:</p> <ul style="list-style-type: none"> <li>– использование подслушивающих (радио закладных) устройств;</li> <li>– дистанционное видеонаблюдение;</li> <li>– перехват побочных электромагнитных излучений и наводок (ПЭМИН).</li> </ul>
5.	Что включают в себя организационные методы защиты информации?	<p>Методы и средства организационной защиты информации включают в себя:</p> <ul style="list-style-type: none"> <li>– ограничение физического доступа к объектам КС и реализация режимных мер;</li> <li>– ограничение возможности перехвата ПЭМИН (перехват побочных электромагнитных излучений и наводок);</li> <li>– разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при</li> </ul>

		<p>ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок);</p> <ul style="list-style-type: none"> <li>– резервное копирование наиболее важных с точки зрения утраты массивов документов;</li> <li>– профилактику заражения компьютерными вирусами.</li> </ul>
6.	Какие существуют уровни правового обеспечения информационной безопасности?	<p>Можно выделить четыре уровня правового обеспечения информационной безопасности.</p> <p>Первый уровень образуют международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России.</p> <p>Второй уровень составляют подзаконные акты, к которым относятся указы Президента РФ и постановления Правительства РФ, а также письма Высшего Арбитражного Суда РФ и постановления пленумов Верховного Суда РФ.</p> <p>Третий уровень составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами.</p> <p>Четвертый уровень образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации.</p>
7.	Какая информация является конфиденциальной?	<p>В соответствии с российским законодательством к конфиденциальной относится следующая информация:</p> <ul style="list-style-type: none"> <li>– служебная тайна (врачебная, адвокатская, тайна суда и следствия и т.п.);</li> <li>– коммерческая тайна;</li> <li>– персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность).</li> </ul>

8.	Что является опосредованной угрозой безопасности информации в КС?	Опосредованной угрозой безопасности информации в КС является угроза раскрытия параметров подсистемы защиты информации, входящей в состав КС. Реализация этой угрозы дает возможность реализации перечисленных ранее непосредственных угроз безопасности информации.
9.	Что представляет собой системно-концептуальный подход к решению задачи защиты информации в КС?	<p>При решении задачи защиты информации в КС необходимо применять так называемый системно-концептуальный подход. В соответствии с ним решение задачи должно подразумевать:</p> <ul style="list-style-type: none"> <li>– системность целевую, при которой защищенность информации рассматривается как составная неотъемлемая часть ее качества;</li> <li>– системность пространственную, предполагающую взаимосвязанность защиты информации во всех элементах КС;</li> <li>– системность временную, предполагающую непрерывность защиты информации;</li> <li>– системность организационную, предполагающую единство организации всех работ по защите информации в КС и управления ими.</li> </ul>
10.	Какие существуют методы и средства защиты информации?	<p>Существующие методы и средства защиты информации можно подразделить на четыре основные группы:</p> <ul style="list-style-type: none"> <li>– методы и средства организационно-правовой защиты информации;</li> <li>– методы и средства инженерно-технической защиты информации;</li> <li>– криптографические методы и средства защиты информации;</li> <li>– программно-аппаратные методы и средства защиты информации.</li> </ul>

Тестовые задания:

1	Упорядоченная совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы, называется:
---	---

	<ul style="list-style-type: none"> <li><b>a) информационной системой;</b></li> <li>b) политикой безопасности;</li> <li>c) информационной технологией;</li> <li>d) информационным процессором.</li> </ul>
2	<p>Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, называется</p> <p><b>Защитой информации</b></p>
3	<p>Получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней, называется</p> <p><b>Несанкционированным доступом</b></p>
4	<p>Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа, называется:</p> <ul style="list-style-type: none"> <li>a) защитой информации;</li> <li><b>b) политикой безопасности;</b></li> <li>c) стратегией защиты информации;</li> <li>d) правилами поведения.</li> </ul>
5	<p>Информация, содержание которой может быть понятно любому субъекту, называется:</p> <ul style="list-style-type: none"> <li>a) сказкой;</li> <li>b) инструкцией хакера;</li> <li>c) криптосистемой;</li> <li><b>d) открытым текстом.</b></li> </ul>
6	<p>Доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати):</p> <ul style="list-style-type: none"> <li>a) компьютерным шпионажем;</li> <li><b>b) разглашением;</b></li> </ul>

	<ul style="list-style-type: none"> <li>c) вредительством;</li> <li>d) предательством.</li> </ul>
7	<p>Субъект с полномочиями владения информационными ресурсами, их пользования и распоряжения, называется</p> <ul style="list-style-type: none"> <li>a) сетевым администратором;</li> <li><b>b) собственником информационных ресурсов;</b></li> <li>c) программистом;</li> <li>d) пользователем.</li> </ul>
8	<p>Неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками:</p> <ul style="list-style-type: none"> <li>a) расползанием информации;</li> <li>b) информационным предательством;</li> <li>c) вредительством;</li> <li><b>d) утечкой.</b></li> </ul>
9	<p>Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации, называется:</p> <ul style="list-style-type: none"> <li>a) устареванием политики безопасности;</li> <li>b) сбоем системы защиты информации;</li> <li><b>c) уязвимостью информации;</b></li> <li>d) обходом защиты информации.</li> </ul>
10	<p>Воздействие на защищаемую информацию из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий, называется:</p> <ul style="list-style-type: none"> <li><b>a) непреднамеренным воздействием;</b></li> <li>b) самоатакой;</li> <li>c) глюком.</li> </ul>

<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
a	защитой информации;	несанкционированным доступом;	b	d
<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>
b	b	d	c	a

### Дисциплина «Сети и телекоммуникации»

Разъясните основные понятия:

№	Понятие	Определение
1.	Телекоммуникации	Комплекс технических средств для передачи информации на расстояние. К техническим средствам относятся телефон, телеграф, радио, телевидение, компьютерные сети.
2.	Компьютерная сеть	Информационная система, объединяющая компьютеры, серверы и другое оборудование с помощью каналов связи. Различают виды компьютерных сетей: <ul style="list-style-type: none"> <li>– персональная;</li> <li>– локальная;</li> <li>– региональная;</li> <li>– глобальная;</li> <li>– глобальная (интернет);</li> <li>– виртуальная частная.</li> </ul>

3.	Архитектура клиент – сервер компьютерной сети	Это модель организации вычислительных систем, в которой задачи распределены между клиентами и серверами. Различают двухуровневую, трехуровневую и многоуровневую клиент-серверную архитектуру компьютерной сети.
4.	Топология компьютерных сетей	Топология сети характеризует свойства сетей, не зависящие от их размеров, отражает структуру, образуемую узлами сети и множеством связывающих их каналов.
5.	Провайдер	Организация, предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги. К основным услугам интернет-провайдеров относятся: широкополосный доступ в Интернет, коммутируемый доступ в Интернет, беспроводной доступ в Интернет.
6.	Беспроводное соединение	<p>При беспроводном соединении компьютеры соединяются с помощью радиосигналов, которые принимают и передают специальные приемники в компьютерах.</p> <p>Распространенный вид беспроводного соединения – Wi-Fi. Другими распространенными видами соединений являются Bluetooth-соединения и инфракрасное соединение.</p>
7.	Сетевые протоколы Интернет	<p>Наиболее известные протоколы, используемые в сети Интернет:</p> <ul style="list-style-type: none"> <li>– HTTP — это протокол передачи гипертекста.</li> <li>– FTP — это протокол передачи файлов со специального файлового сервера на компьютер пользователя.</li> <li>– POP и IMAP – это протоколы, которые используются для получения электронной почты с почтового сервера.</li> <li>– SMTP это протокол, который используется для отправки и доставки электронной почты.</li> </ul>

		<ul style="list-style-type: none"> <li>– DNS – это протокол, который используется для преобразования доменных имен (например, www.example.com) в IP-адреса.</li> <li>– VoIP – это протокол, который используется для передачи голосовой информации по сети интернет.</li> <li>– TELNET— это протокол удаленного доступа. TELNET дает возможность абоненту работать на любом компьютере находящейся с ним в одной сети.</li> </ul>
8.	Интернет	Глобальная компьютерная сеть, состоящая из многих сетей, работающих на основе протоколов TCP/IP, объединенных через шлюзы и использующих единое адресное пространство и пространство имен.

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Что такое двухуровневая архитектура клиент-серверной вычислительной сети	<p>Различают два подтипа двухуровневой архитектуры клиент-серверной вычислительной сети:</p> <ol style="list-style-type: none"> <li>1. Клиент-серверная архитектура с тонким клиентом. В ней большая часть задач приложения выполняется на сервере. С компьютеров-клиентов отправляется запрос на выполнение задач.</li> <li>2. Клиент-серверная архитектура с толстым клиентом. В ней на компьютерах клиентов обрабатывается большую часть задач приложений.</li> </ol>
2.	Что такое трехуровневая архитектура клиент-серверной вычислительной сети	Она состоит из трех компонентов: компьютеры клиентов, сервер и базу данных. Клиент формирует запрос, отправляет его на сервер. Сервер при обработке запроса обращается к базе данных для получения или сохранения данных. Затем отправляет результат клиенту.
3.	Что такое архитектура локальной сети Ethernet?	Ethernet – архитектура сетей с разделяемой средой и широковещательной передачей (все узлы получают пакет одновременно) и методом доступа

		CSMA/CD. Согласно данной архитектуре, компьютер выдает в сеть сообщение без предварительных запросов на передачу.
4.	Что такое архитектура локальной сети Arcnet?	В сети Arcnet компьютер может передать свое сообщение в сеть только после получения специального служебного маркера. Маркер представляет собой специальную последовательность битов. Он перемещается по сети от компьютера к компьютеру в порядке возрастания их системных номеров.
5.	Что такое линии связи и каналы передачи данных?	Линии связи и каналы передачи данных обеспечивают физическую среду для передачи информации. Они могут быть проводными (медные кабели, волоконно-оптические кабели) или беспроводными (радиоволны).
6.	В чем состоят особенности технологий LTE?	LTE является стандартом беспроводной коммуникации, который обеспечивает высокую скорость передачи данных, низкую задержку и более эффективное использование спектра.
7.	Что такое стек протоколов TCP/IP?	TCP/IP – набор правил, которые описывают, как компьютеры соединяются и передают информацию друг другу. Наименование модели состоит из названий двух главных протоколов: <ul style="list-style-type: none"> <li>– TCP – протокол, который описывает, как передается информация внутри сети;</li> <li>– IP – протокол, который описывает связь компьютеров друг с другом.</li> </ul>
8.	Что такое IP-адрес?	IP-адрес представляет собой строку чисел, разделенных точками. IP-адреса выражаются в виде набора из четырех цифр. Каждое число в наборе может находиться в диапазоне от 0 до 255.
9.	Что такое динамические IP-адреса?	Динамические IP-адреса меняются автоматически и регулярно интернет-провайдерами. Интернет-провайдеры покупают большой пул IP-адресов и автоматически назначают их своим клиентам. Периодически они

		переназначают их и помещают старые IP-адреса обратно в пул для использования другими клиентами.
10.	Что такое статические IP-адреса?	Для статического IP-адреса характерно то, что только сеть присваивает IP-адрес, он уже не меняется. Большинству частных лиц и компаний не нужен статический IP-адрес, но для компаний, которые планируют разместить собственный сервер, его наличие крайне важно.

Тестовые задания:

1	Компьютерная сеть, охватывающая небольшую территорию (этаж, здание, несколько соседних зданий) внутри компании, называется <ul style="list-style-type: none"> <li>a) <b>локальной компьютерной сетью</b></li> <li>b) региональной компьютерной сетью</li> <li>c) серверной сетью</li> <li>d) рабочей станцией</li> </ul>
2	Модель организации вычислительных систем, в которой задачи распределены между клиентами и сервером, называется <ul style="list-style-type: none"> <li>a) иерархической архитектурой</li> <li>b) <b>клиент-серверной архитектурой</b></li> <li>c) сетевой архитектурой</li> <li>d) сотовой архитектурой</li> </ul>
3	Технология обмена информацией между такими устройствами, как персональные компьютеры, мобильные телефоны, планшеты, мыши, наушники и акустические системы на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи, называется <ul style="list-style-type: none"> <li>a) <b>Bluetooth</b></li> <li>b) Wi-Fi</li> </ul>

	<p>c) C-CMOS d) LANCE</p>
4	<p>Технология беспроводного подключения по локальной сети для домашних устройств с помощью роутера, называется:</p> <p>a) провайдером b) Ethernet c) <b>Wi-Fi</b> d) LANCE</p>
5	<p>Топология локальной компьютерной сети, при которой к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует свою отдельную линию связи, называется</p> <p><b>Звезда</b></p>
6	<p>Топология локальной компьютерной сети, при которой каждый компьютер передает информацию всегда только одному компьютеру, следующему в цепочке, а получает информацию только от предыдущего в цепочке компьютера, и эта цепочка замкнута, называется</p> <p><b>Кольцо</b></p>
7	<p>Организация, предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги, называется</p> <p>a) сервисной компанией b) блогером c) <b>провайдером</b> d) сервером</p>
8	<p>Базовым протоколом Интернета является</p> <p>a) HTTP; b) <b>TCP/IP;</b> c) HTML;</p>

	d) FTP.
9	Компьютер, подключенный к Интернету, обязательно имеет <b>a) IP-адрес;</b> b) Доменное имя; c) Домашнюю web-страницу; d) Модем.
10	Укажите IP-адрес компьютера a) <a href="http://dialup.mtam;">http://dialup.mtam;</a> b) <a href="http://referat.kulichki.het/author.html">http://referat.kulichki.het/author.html;</a> <b>c) 192.168.10.11;</b> d) <a href="http://www.gov.ru">http://www.gov.ru.</a>

Ключ к тестовым заданиям

1	2	3	4	5
a	b	a	c	звезда
6	7	8	9	10
КОЛЬЦО	c	b	a	c

## Дисциплина «Основы теории передачи информации»

Разъясните основные понятия:

№	Понятие	Определение
1	Информация	Данные или факты, которые передаются и обрабатываются для получения смысла или пользы.
2	Кодирование	Процесс преобразования информации из одной формы в другую, чтобы было возможно передать или хранить ее.
3	Канал связи	Среда или система, по которой передается информация от отправителя к получателю.
4	Шум	Нежелательные искажения или интерференции, возникающие во время передачи информации по каналу связи.
5	Пропускная способность	Максимальное количество информации, которое может быть передано через канал связи за единицу времени.
6	Код	Набор правил и систематических способов преобразования информации для ее передачи или хранения.
7	Цифровая передача	Форма передачи информации, где она преобразуется в цифровой (бинарный) вид, состоящий из двух состояний: "1" и "0".
9	Протоколы связи	Совокупность правил и стандартов, определяющих способ организации и передачи информации по каналу связи.
10	Модуляция	Процесс изменения носителя или несущего сигнала для передачи информации.

Вопросы открытого типа:

№	Вопрос	Ответ
1	Какой процесс называется частотной модуляцией?	Это процесс изменения частоты несущего сигнала, пропорционально амплитуде модулирующего (исходного) сигнала.
2	Что из себя представляет дискретная двоичная модуляция?	Это метод модуляции, при котором информационный сигнал преобразуется в последовательность дискретных уровней, как правило, двух уровней, обычно обозначаемых как "0" и "1".
3	Что представляет собой импульсная модуляция.	Это метод модуляции, при котором информационный сигнал кодируется в виде последовательности импульсов, которые управляют формой, амплитудой и временем появления несущего сигнала.
5	Что называется шириной спектра сигнала?	Это диапазон частот, занимаемых данным сигналом в спектре частот.
6	Какие характеристики канала связи можно отнести к основным, существенно влияющим на качество передачи сигнала?	<ol style="list-style-type: none"> <li>1. Пропускная способность.</li> <li>2. Затухание.</li> <li>3. Задержка.</li> <li>4. Шум.</li> <li>5. Искажение сигнала.</li> </ol>
7	Что называется полосой пропускания канала связи?	Это диапазон частот, в пределах которого канал способен передавать сигнал без искажений или значительной потери информации.
8	Какой процесс называется помехоустойчивым кодированием?	Это процесс добавления дополнительных информационных символов, называемых проверяющими символами, к передаваемым данным с целью обнаружения и/или исправления ошибок, возникающих в процессе передачи.

9	Сформулируйте основные достоинства цифровой передачи информации.	1. Высокая помехоустойчивость. 2. Высокая скорость передачи информации. 3. Совместимость с вычислительной техникой и создание цифровых сетей. 4. Обеспечение высокой информационной безопасности.
10	Какой принцип лежит в основе оптимального кодирования по методу Шеннона –Фано?	Принцип: наиболее вероятным сообщениям должны присваиваться короткие кодовые комбинации, а сообщениям с малой вероятностью – более длинные комбинации.

Тестовые задания:

1.	Технические средства, обеспечивающие передачу и прием информации между удаленными друг от друга людьми или устройствами - это система
А)	<b>Связи</b>
Б)	Взаимодействия
В)	переговоров
Г)	Общения

2.	Дискретизация передаваемой информации используется для
А)	<b>формирования цифрового представления аналогового сигнала</b>
Б)	ограничения полосы входных сигналов
В)	преобразования цифрового представления сигнала в аналоговое
Г)	определения частотного спектра сигнала

3.	Современные средства коммуникации в подавляющем большинстве используют _____ сигналы.
А)	<b>Электрические</b>

Б)	Звуковые
В)	Световые
Г)	Импульсные

4.	Преобразование Фурье используется для
А)	<b>преобразование периодического сигнала из временной области в частотную и обратно</b>
Б)	фильтрации нежелательных частот
В)	сжатия дискретных сигналов
Г)	сжатия аналоговых сигналов

5.	С увеличением статистических связей символов на выходе источника информации избыточность его сообщений _____
А)	<b>Уменьшается</b>
Б)	Увеличивается
В)	не изменяется

6.	Свойства сложных сигналов характеризуются
А)	<b>энергетическим спектром, близким к равномерному</b>
Б)	<b>функцией корреляции с узким пиком</b>
В)	энергетическим спектром с узким пиком
Г)	равномерной функцией корреляции

7.	_____ сигналы — это зависящие от времени напряжения или токи, которые непрерывно изменяются по определенному закону.
<b>Аналоговые</b>	

8.	_____ сигналы — это сигналы, формируемые на основе использования дискретных отсчетов и уровней квантования аналоговых сигналов.
<b>Цифровые</b>	

Ключ к тестовым заданиям

1	2	3	4	5
a	a	электрические	a	a
6	7	8	9	10
ab	аналоговые	цифровые		