РАЗДЕЛ 3. ЗАДАНИЯ ДЛЯ ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ

3.1 Теоретическое задание.

Вариант 1.

1. Какова сфера действия и цель №152-ФЗ? Как в соответствии с законом о персональных данных (ПД) должна организовываться адресная рассылка информации потребителям услуг в целях маркетинга и рекламы? Как должен поступить человек в ситуации, когда он получает навязчивую адресную рассылку от банка с предложениями о кредитах, а банк отказывается исключить его из рассылки?

2.Что обязан делать работодатель в целях охраны конфиденциальности информации, составляющей коммерческую тайну?

Вариант 2.

1. Что понимается под коммерческой тайной? Приведите примеры информации, относящейся к системе управления организацией, которая может / не может составлять коммерческую тайну.

2. При каких условиях меры по охране конфиденциальности информации признаются разумно достаточными?

Вариант 3.

1. Каковы принципы обработки персональных данных (ПД)? Приведите примеры реализации этих требований на примере своей организации.

2. Когда режим коммерческой тайны считается установленным?

Вариант 4.

1. Каковы условия обработки персональных данных (ПД)? Опишите ситуации, когда кредитно-финансовая организация на законном основании может обрабатывать персональные данные клиентов без их согласия? (такие ситуации точно есть).

2. Что должны включать в себя меры по охране конфиденциальности информации?

Вариант 5.

1. Конфиденциальность персональных данных (ПД) и общедоступные источники ПД. Каковы основания для включения ПД в общедоступные источники ПД. Приведите примеры таких источников в Вашей организации.

2. Какие права имеет обладатель информации, составляющей коммерческую тайну?

Вариант 6.

1. Что представляет собой согласие субъекта персональных данных (ПД) на обработку его ПД? Составьте пример согласия для обработки ПД клиента, открывающего вклад в некотором банке.

2. Как предоставлять информацию, составляющую коммерческую тайну?

Вариант 7.

1. Какие существуют специальные категории персональных данных (ПД)? Приведите пример документов, содержащих такие ПД. Какие требования должен соблюдать оператор при обработке специальных категорий ПД?

2. Какие сведения не могут составлять коммерческую тайну?

Вариант 8.

1. Что такое биометрические персональные данные (ПД)? Приведите примеры биометрических ПД. Опишите основные требования по их обработке. Как выполнить эти требования при внедрении внутренней системы видеонаблюдения в организации?

2. Какие существуют способы получения информации, составляющей коммерческую тайну?

Вариант 9.

1. Как осуществить трансграничную передачу персональных данных (ПД) с соблюдением требований закона о персональных данных? Ответ поясните на примере. В качестве примера можно рассмотреть ситуацию, когда студент обучается по программе «двойной диплом», в которой партнёром российской образовательной организации является зарубежный вуз.

2. Определите основные понятия, используемые в №98-ФЗ

Вариант 10.

1. Какова ответственность за нарушение требований №152-ФЗ. Используя официальную информацию Уполномоченного органа по защите прав субъектов персональных данных (ПД), приведите примеры привлечения операторов к такой ответственности.

2. Каковы цели и сфера действия №98-ФЗ?

Вариант 11.

1. Что такое Уполномоченный орган по защите прав субъектов персональных данных (ПД), каковы его функции, на кого возложена реализация этих функций? Используя официальный интернет-ресурс данного органа, определите адрес его территориального представительства. Определите, включена ли Ваша организация в План проверок исполнения требований по обработке ПД на текущий календарный год.

2. Какие обязательства берет на себя работник в целях охраны конфиденциальности информации, составляющей коммерческую тайну? Как это оформляется?

Вариант 12.

1. Кто может являться оператором персональных данных (ПД)? Кто является оператором в ситуации, когда компания «Орг» передаёт на аутсорсинг в специализированную фирму «Бухгалтерия» функции бухгалтерского учёта и начисления заработной платы? Ответ обосновать.

2. Какие минимально необходимые требования должны быть выполнены в рамках режима коммерческой тайны? Как обеспечить требование конфиденциальности при передаче коммерческой тайны организации-партнёру по бизнесу?

Вариант 13.

1. Какая ответственность существует за нарушение №98-ФЗ**?** Как распределяется ответственность в случае инцидентов, связанных с обработкой персональных данных между оператором и лицом, осуществляющим обработку персональных данных (ПД) по поручению оператора? Поясните ответ на примере модельной ситуации, когда компания «Орг» передаёт на аутсорсинг в специализированную фирму «Бухгалтерия» функции бухгалтерского учёта и начисления заработной платы для своих сотрудников?

2. В каких случаях операторами ПД не должна обеспечиваться конфиденциальность ПД?

Вариант 14.

1. В каких случаях для обработки персональных данных (ПД) не требуется согласия субъекта ПД? Опишите 2-3 такие ситуаций на примере своей организации (такие примеры есть в любой организации).

2. Какова ответственность предусмотрена законодательством за нарушение коммерческой тайны?

Вариант 15.

1. Кто должен запрашивать согласие работников предприятия на обработку персональных данных (ПД) при их передаче для обработки другому оператору? Рассмотрите эту ситуацию на конкретном примере: предприятие «Пред» поручает охранной организации «Охр» осуществлять контроль доступа внешних посетителей на территорию «Орг», фиксируя идентификационные данные о них (ФИО, серия и номер и дата выдачи паспорта) в соответствующем журнале разовых посещений.

2. Подпадает ли финансовая информация под охрану №98-ФЗ и №152-ФЗ?

Вариант 16.

1. В каких случаях оператор вправе осуществлять обработку персональных данных (ПД) без уведомления Уполномоченного органа по защите прав субъектов ПД? Приведите конкретный пример такой ситуации.

2. Как реализуются требования ФЗ-152 по защите персональных данных при трансграничной передаче и обработке их юридическими лицами других стран

Вариант 17.

1. Что понимается под информационной системой персональных данных? Является ли корпоративный веб-сайт информационной системой персональных данных (ПД)? Поясните ответ на конкретном примере – официального веб-сайта некоторого банка.

2. Каковы критерии (условия) отнесения информации к коммерческой тайне? Приведите примеры, когда отнесение информации, подпадающей под определение коммерческой тайны, выполнено с нарушением перечисленных условий, в силу чего является некорректным.

Вариант 18.

1. Каковы функции Уполномоченного органа по защите прав субъектов ПД? Кто отвечает за соблюдение законности обработки персональных данных (ПД) на предприятии? Если при обработке ПД предприятием нарушаются права сотрудника как субъекта ПД, куда он может обратиться согласно закону о ПД для разрешения таких конфликтных ситуаций внутри предприятия и вне его? Ответ обосновать.

2. Закон «О государственной тайне». Основные понятия и сфера действия. При каких условиях информация, составляющая государственную тайну, может обрабатываться в коммерческой организации?

Вариант 19.

1. Какая ответственность предусмотрена за нарушение оператором требований №152-ФЗ? Какова величина штрафов при нарушении требований по защите информации, в том числе персональных данных (ПД), каким документом она определяется? Приведите примеры привлечения операторов к ответственности (использовать информацию официального сайта Уполномоченного органа по защите прав субъектов персональных данных и его территориальных представительств).

2. Какая информация включается в Перечень сведений, составляющих государственную тайну? Опишите кратко, как осуществляется засекречивание сведений и отнесение их к государственной тайне.

Вариант 20.

1. Какие персональные данные необходимы для принятия решения о кредитовании физических лиц и чем обосновывается эта необходимость? Вправе ли кредитная организация обрабатывать персональные данные (ПД) физических лиц, получивших отказ в кредитовании? Ответ обосновать.

2. Что понимается под защитой информации в соответствии с ФЗ-149? Какие задачи должен решить оператор информационной системы для обеспечения защиты информации? Приведите примеры мер и средств для решения задач из каждой группы.

Вариант 21.

1. В каких формах предоставляется согласие субъекта на обработку его персональных данных (ПД)? Возможно ли хранить формы анкет-заявок на получе-

ние кредита в формате цифровых копий: если возможно, то при каких условиях, а если нет – то почему?

2. Как классифицируется информации в зависимости от порядка доступа к ней, от порядка её предоставления и распространения? Приведите примеры информации, относимой к каждому классу.

Вариант 22.

1. Возможно ли получение согласия на обработку персональных данных (ПД) по телефону? Как должна действовать кредитная организация, если ей необходимо получить подтверждение подлинности предоставленных заёмщиком сведений о его месте работы и должности.

2. Какие информационные системы называются государственными и муниципальными в соответствии с ФЗ-149? Приведите примеры, когда государственные (ГосИС) и муниципальные информационные системы могут быть в коммерческой организации. Какие особые требования к защите информации предъявляются к ГосИС? В каких нормативных актах подробно описаны требования по обеспечению безопасности ГосИС?

Вариант 23.

1. Что является документом, подтверждающим получение согласия на обработку ПД при покупке товаров в интернет-магазинах? Как корректно оформить такой документ? Ответ обосновать.

2. Реквизиты носителей сведений, составляющих государственную тайну. Опишите кратко, кто и на каком основании может получить допуск к информации, содержащей сведения, составляющие государственную тайну.

Вариант 24.

1. При каких условиях оператор персональных данных (ПД) вправе запрашивать сведения о судимости? Опишите пример, когда это возможно и порядок запроса таких сведений.

2 Какая административная ответственность предусмотрена за нарушение защиты персональных данных и информации, составляющей коммерческую тайну?

Вариант 25.

1. Какие иностранные государства обеспечивают адекватную защиту персональных данных (ПД)? Как это узнать? Как правильно с точки зрения закона о ПД осуществить передачу ПД клиента в государство, не обеспечивающее адекватной защиты ПД?

2. Уголовно-правовая защита информации, составляющей гостайну.

Вариант 26.

1. В каких случаях для обработки персональных данных (ПД) не требуется согласия субъекта ПД? Опишите 2-3 такие ситуаций на примере своей организации (такие примеры есть в любой организации).

2. Что понимается под защитой информации в соответствии с ФЗ-149? Какие задачи должен решить оператор информационной системы для обеспечения защиты информации? Приведите примеры мер и средств для решения задач из каждой группы.

Вариант 27.

1. Каковы условия обработки персональных данных (ПД)? Опишите ситуации, когда кредитно-финансовая организация на законном основании может обрабатывать персональные данные клиентов без их согласия? (такие ситуации точно есть).

2. Закон «О государственной тайне». Основные понятия и сфера действия. При каких условиях информация, составляющая государственную тайну, может обрабатываться в коммерческой организации?

Вариант 28.

1. Что понимается под информационной системой персональных данных? Является ли корпоративный веб-сайт информационной системой персональных данных (ПД)? Поясните ответ на конкретном примере – официального веб-сайта некоторого банка.

2. Определите основные понятия, используемые в №98-ФЗ.

Вариант 29.

1. Что представляет собой согласие субъекта персональных данных (ПД) на обработку его ПД? Составьте пример согласия для обработки ПД клиента, открывающего вклад в некотором банке.

2. Какая информация включается в Перечень сведений, составляющих государственную тайну? Опишите кратко, как осуществляется засекречивание сведений и отнесение их к государственной тайне.

Вариант 30.

1. 1. Что такое биометрические персональные данные (ПД)? Приведите примеры биометрических ПД. Опишите основные требования по их обработке.

2. Какие информационные системы называются государственными и муниципальными в соответствии с ФЗ-149? Приведите примеры, когда государственные (ГосИС) и муниципальные информационные системы могут быть в коммерческой организации.

3.2 Практическое задание.

Основные понятия криптографической защиты информации.

В переводе с греческого языка криптография означает «тайнопись». Криптографические методы играют важную роль в обеспечении безопасности информации при её передаче и хранении. Исторически криптография возникла как средства защиты конфиденциальности информации, содержание которой должен знать строго ограниченный круг лиц. Основным понятием в криптографии является понятие шифра.

Шифр – это семейство обратимых математических преобразований, каждое из которых определяется некоторым параметром (ключом) и порядком применения (режимом шифрования). Построение шифров опирается на два базовых принципа. Принцип замены состоит в том, что символы открытого текста заменяются другими символами этого же или другого алфавита по некоторому правилу. Принцип перестановки заключается в том, что символы шифруемого текста переставляются между собой по некоторому правилу. Часто применяются оба этих принципа, чтобы полученная шифрограмма как можно больше была похожа на хаотичный набор символов (не только внешне, но и при проверке её на случайность строгими математическими методами).

Процесс преобразования текста из открытого вида в зашифрованный называется *зашифрованием*. Результат преобразования называют *криптограммой* или *шифрограммой*. Процесс восстановления открытого текста из криптограммы с помощью обратного преобразования и известного ключа называется *расшифрованием*. Расшифрование - это способ восстановления открытого текста законным пользователем, поэтому оно должно выполняться столь же просто, как и зашифрование.

Нахождение текста без знания ключа называют *дешифрованием* – это должна быть существенно более достаточно сложная задача, так решат её пытается противник, не имеющий законного доступа к содержанию информации. Именно в этом и состоит смысл шифрования. Следует отметить, что популярной и общеобразовательной литературе термин «дешифрование» используют нередко для

обозначения любой процедуры получения открытого текста по шифрограмме, относя его как к законному процессу расшифрования (т.е. при известном ключе), так и ко «взлому» шифра (т.е при неизвестном ключе шифрования), но в профессиональной литературе эти термины различаются и используются в соответствии с введёнными выше определениями.

Криптография - это наука о методах преобразования информации с целью её защиты посредством создания и использования шифров. Наука о методах «взлома» шифров называется криптоанализ. Задачи криптоанализа заключаются в нахождении секретного ключа на основе доступной информации о криптограммах и, возможно, некоторых соответствующих им открытых текстов, а также о методах вычисления открытого текста без знания ключа. Иногда используют термин к*риптология* - наука, объединяющая криптографию и криптоанализ.

Важнейшим компонентом любого шифра является *ключ* — параметр криптографического алгоритма, обеспечивающий выбор одного преобразования для зашифрования конкретного сообщения из совокупности преобразований, возможных для этого алгоритма.

Шифры могут использовать один ключ для шифрования и расшифрования или два различных ключа, связанных между собой определённой зависимостью.

Пусть M – открытое, C – зашифрованное сообщение, тогда процессы зашифрования E, зависящий от ключа k_e, и расшифрования D, зависящий от ключа k_d, можно записать в виде: $E_{k_e}(M) = C$ и $D_{k_d}(C) = M$. При этом выполняется соотношение $D_{k_d}(E_{k_e}(M)) = M$.

Различают симметричные и ассиметричные криптоалгоритмы. *В симметричных алгоритмах* знание ключа для зашифрования k_e позволяет легко найти ключ расшифрования k_d (как правило, они совпадают: $k_e = k_d = k$). Отсюда следует, что ключ симметричного алгоритма должен быть доставлен абонентам до начала обмена сообщениями конфиденциальным образом и храниться ими также с соблюдением данного требования. Симметричные алгоритмы могут быть поточными и блочными. Поточные алгоритмы осуществляют зашифрование отдель-

ных символов открытого сообщения. Блочные алгоритмы шифруют фрагменты (блоки) текста, каждый из которых содержит фиксированное число символов, последовательно идущих в открытом тексте.

В асимметричных криптоалгоритмах знание ключа k_e не даёт возможности вычислить ключ расшифрования k_d, поэтому в секрете нужно хранить только один ключ для расшифрования k_d (секретный ключ), а второй ключ k_e можно сделать общедоступным (открытый ключ). После зашифрования информации на открытом ключе, восстановить исходный текст может лишь обладатель секретного ключа. По этой причине криптосистемы, основанные на асимметричных алгоритмах, называют по-другому криптосистемами с открытым ключом. Такие системы позволяют легко организовать передачу конфиденциальной информации в открытой сети: для того, чтобы отправить конфиденциальное сообщение, отправитель связывается с получателем, который по открытому каналу передаёт ему ключ k_e.(например, пересылая по электронной почте или помещая на общедоступный сервер). Отправитель использует этот ключ для зашифрования сообщения, которое после получения будет расшифровано получателем с использованием своего секретного ключа k_d. Если изменить порядок применения ключей, то получаем схему, на которой основана электронная цифровая подпись. Вначале отправитель производит преобразование текста с использованием своего «секретного ключа» (формирует «подпись») и пересылает открытый текст вместе с подписью. Получатель применяет к «подписи» преобразование, зависящее от открытого ключа отправителя, и сравнивает его с полученным открытым текстом. Отличия возможны в двух случаях – при искажении текста или несоответствия открытого ключа секретному ключу отправителя. Из этого следует, что совпадение полученного текста и текста, восстановленного из подписи, позволяет получателю подтвердить целостность сообщение и подлинность отправителя - решить те же задачи, что и при получении документа на бумажном носителе, подписанного собственноручной подписью отправителя.

Следует отметить, что, хотя в отношении открытого ключа не требуется соблюдение конфиденциальности, важным аспектом является обеспечение гарантий того, что при передаче и хранении некий злоумышленник не сможет подменить открытый ключ абонента на свой ключ (в противном случае, он сможет контролировать и подменять все передаваемые сообщения). Для обеспечения доверенной среды вводятся понятия сертификата и центра сертификации. Сертификат – это электронный документ, фиксирующий соответствие открытого ключа его законному владельцу, заверенный подписью центра сертификации – третьей стороны, обеспечивающей доверенное хранение сертификатов.

Асимметричные алгоритмы позволяют решать большое количество и других задач защиты информации к компьютерных сетях, в том числе формировать абонентам общий секретный ключ для дальнейшего шифрования сообщений симметричными алгоритмами.

Для полноты обзора базовых понятий криптографии следует сказать несколько слов о том, как оценивается *качество шифров*. Для этого вводится понятие стойкости шифра. Стойкость шифра определяется тем, насколько сложно осуществить его криптоанализ (дешифровать сообщение или определить секретный ключ). Например, симметричные шифры, получаемые простой взаимнооднозначной заменой букв алфавита любого естественного языка на буквы другого алфавита стойкими не являются, так шифрограммы сохраняют все статистические свойства исходного текста, связанные с частотой встречаемости отдельных букв и сочетаний из конкретных букв. Для повышения стойкости шифра должны быть более сложные правила замены символов (или их блоков), дополненные процедурами сдвига и перестановки их в шифрограмме. Доказано, что наибольшей стойкостью обладают такие шифры, которые позволяют получать криптограммы, не отличимые от случайного текста, причём ключ должен быть достаточно длинным (в идеале равен длине открытого текста) и использоваться только один раз. Для построения стойких асимметричных алгоритмов используют специальные «односторонние функции», которые легко и быстро вычисляются (шифрование), но выполнение обратных преобразований без знания

секретного ключа является чрезвычайно сложной задачей, требующей многолетних компьютерных вычислений.

В практических заданиях студентам необходимо: выполнить шифрование и расшифрование информации с применением одного из классических (исторических) симметричных шифров. Более конкретные теоретические сведения по каждому пункту изложены ниже.

Рассмотрим *симметричные* (одноключевые) системы шифрования.

Симметричные системы или алгоритмы шифрования с одним ключом используют для шифрования и дешифрования один и тот же ключ *k*. Ниже рассматриваются простейшие алгоритмы шифрования, представляющие принципиальную основу современных компьютерных алгоритмов шифрования.

1. Алгоритм простой перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключами в этих алгоритмах являются размеры таблицы и порядок перестановки. Пример данного метода шифрования текста «**И БУМАЖКОЙ ПРИКРОЕМ БРЕШЬ**» показан в таблицах на рисунок 1. Сначала в таблицу записывается текст сообщения (рисунок 1 а), а потом поочередно переставляются столбцы в определенном порядке (на рисунок 1 б) в первой строке, а затем строки (на рисунок 1 в) в последнем столбце. При расшифровании порядок перестановок -обратный. Пример данного метода шифрования показан в следующих таблицах:

	1	*2*	*3*	*4*	*5*
1	**И**		**Б**	**У**	**М**
2	**А**	**Ж**	**К**	**О**	**Й**
3		**П**	**Р**	**И**	**К**
4	**Р**	**О**	**Е**	**М**	
5	**Б**	**Р**	**Е**	**Ш**	**Ь**

а)

4	*2*	*1*	*3*	*5*
У		И	Б	М
О	Ж	А	К	Й
И	П		Р	К
М	О	Р	Е	
Ш	Р	Б	Е	Ь

б)

И	**П**		**Р**	**К**	*3*
М	**О**	**Р**	**Е**		*4*
Ш	**Р**	**Б**	**Е**	**Ь**	*5*
О	**Ж**	**А**	**К**	**Й**	*2*
У		**И**	**Б**	**М**	*1*

в)

Рисунок 1-Двойная перестановка столбцов и строк

В результате перестановки текста «**И БУМАЖКОЙ ПРИКРОЕМ БРЕШЬ**» получена шифрограмма «**ИП РКМОРЕ ШРБЕЬОЖАКЙУ ИБМ**». Ключом к шифру служат номера столбцов 4 2 1 3 5 и номера строк 3 4 5 2 1 исходной таблицы.

Для удобства запоминания ключей можно использовать в их качестве слова. При этом порядок перестановки определяется нумерацией букв в слове в алфавитном порядке. В приведенном примере использованы *Ключ1* – «СПОРТ», буквы в алфавите располагаются в порядке 4 2 1 3 5 (ОПРСТ – 12345) и *Ключ2* – «СТУЖА», буквы в алфавите располагаются в порядке 3 4 5 2 1 (АЖСТУ– 12345). Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5 х 5 их 14400.

Для обеспечения дополнительной защиты можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. При этом размеры второй таблицы должны быть взаимно простыми с размерами первой таблицы.

Для шифрования также применялись *магические квадраты* – квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Свойство магического квадрата используется для повышения эффективности шифра при данном алгоритме шифрования. Для шифрования необходимо вписать исходный текст «ЧИСЛОШЕСТНАДЦАТЬ» по приведенной в магическом квадрате нумерации и затем переписать содержимое таблицы по строкам (рисунок 2). В результате получается шифротекст «ЬСИЦОНАСТШЕДЛТАЧ», сформированный благодаря перестановке букв исходного сообщения.

Исходный текст: Ч И С Л О Ш Е С Т Н А Д Ц А Т Ь

Ч	И	С	Л	О	Ш	Е	С	Т	Н	А	Д	Ц	А	Т	Ь
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Магический квадрат

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Шифрование

Ь	С	И	Ц
О	Н	А	С
Т	Ш	Е	Д
Л	Т	А	Ч

Шифрограмма: Ь С И Ц О Н А С Т Ш Е Д Л Т А Ч

Рисунок 2 - Шифрование с помощью магического квадрата

Расшифрование происходит в обратном порядке: вначале текст вписывается последовательно слева направо в квадрат, затем буквы с квадрата выбираются в порядке, определенном в магическом квадрате.

2. Шифры простой замены (подстановки)

Шифры простой замены использовались еще в древней Греции (V–VI до н.э.), которые и в настоящее время являются частью отдельных алгоритмов шифрования.

Система шифрования Цезаря – частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Например, необходимо зашифровать исходный текст без ключа, используя в качестве новых символов шифрования буквы русского алфавита.

Исходный текст: ВЫПЛАТИТЬ СТО РУБЛЕЙ.

В качестве символов шифрования используются буквы русского алфавита, смещенные относительно исходного алфавита на некоторую величину q, например, q=3. В этом случае оба алфавита расположатся следующим образом

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

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

Зашифрованный текст примет вид: ЕЮТОГХЛХЭФХСУЦДОИМ.

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый *квадрат Полибия* размером 5 х 5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

3. Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда сообщение «**ТРУДНО В УЧЕНИИ**» преобразуется в шифрограмму «**ХСШЖОТВГГЧШИРКН**» (рисунок 3).

Сообщение	**Т Р У Д Н О В У Ч Е Н И И**
Ключ	**3 1 4 3 1 4 3 1 4 3 1 4 3 1 4**
Шифрограмма	**Х С Ш Ж О Т В Г Г Ч Ш И Р К Н**

Рисунок 3-Реализация шифра Гронсфельда

В *шифрах многоалфавитной замены (Виженера)* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (рисунок 4).

	АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
А	АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Б	БВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯА

В	ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБ
Г	ГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
.	……
Я	ЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮ

Рисунок 4-Таблица для реализации шифра многоалфавитной замены

Сообщение	СООБЩЕНИЕ
Ключ	ОКНООКНОО
Шифрограмма	ЯШЪПЖПЬЦУ

Рисунок 5-Пример реализации шифра многоалфавитной замены

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы (рисунок 5) по букве текста и строке, соответствующей букве ключа. Например, используя ключ «ОКНО», из сообщения «СООБЩЕНИЕ» получаем следующую шифрограмму «ЯШЪПЖПЬЦУ».

Задания для самостоятельной работы

1. Зашифровать с использованием любого из рассмотренных алгоритмов свои данные: ФамилияИмяОтчество.
2. Используя алгоритмы двойной перестановки строк и столбцов выполнить шифрование следующих фраз (ключ выбирать самостоятельно, номер варианта выбрать по номеру в списке группы):

1) Он досрочно завалил экзамен.

2) Закон суров, но это закон.
3) Умному легче доказать, что он дурак.
4) И у дурака вырастает зуб мудрости.
5) Свободу симулировать нельзя.
6) Подумай, прежде чем подумать.
7) Каждый век имеет свое средневековье.
8) Брюки протираются даже на троне.
9) Окно в мир можно закрыть газетой.
10) Чаще всего выход там, где был вход.
11) Безграмотные вынуждены диктовать.
12) Хлеб открывает любой рот.
13) Деньги не пахнут, но улетучиваются.
14) Сны зависят от положения спящего.
15) Труднее всего поджечь ад.
16) Ужасен кляп, смазанный медом.
17) Не пиши кредо на заборе.
18) Беззубым многое легче выговаривать.
19) И регалии звенят по-разному.
20) Лицемерный палач ослабляет петлю.
21) Интеллектуальная узость ширится.
22) Вписывайся во влиятельные круги.
23) Иные ступени карьеры ведут на виселицу.
24) И маятник идет в ногу со временем.
25) И ненужные постоянно нужны.
26) Что посеешь, то и пожнешь.
27) Яблоко от яблони недалеко падает.
28) Шила в мешке не утаишь.
29) Что написано пером, не вырубишь топором.
30) Чем дальше в лес, тем больше дров.

3. Для вариантов №1-10, используя магический квадрат (таблица 1), расшифровывать шифрограммы (шифрограммы приведены в таблице 2):

Таблица 1

11	24	7	20	3
4	12	25	8	16
17	5	13	21	9
10	18	1	14	22
23	6	19	2	15

Таблица 2

1	ОЛ__ЕЛ_ОДУЛА-СЕЛЯС_МЕЛЙДГ
2	ВТТЙЕБА_КЛЮ_Е_РЫБХТРООЛ_
3	ОЕР_Д__ТОАЛОЗЗЧНИОААЧСЛНВ
4	УЗУНОБЛЯСВАОИЕИМТСРЛЬДЬВО
5	ЕТЙДДУЖЬ_ЧЕМДУПРМПЕМАА_О_
6	ЕАЕЕУДГД_ПОНОЧВСДТ_Ь_ЕЖР_
7	КРШЗ__РЕИ_НПЕА_А_НДБОИ_ЕО
8	ОНЫ_НУСЫЕННЖТН_ПОНОУЖН_ЕЯ
9	ЕМИАГАНУ_ПОЛЯЗЗВ_РТНОИРЕ_
10	НУУ_З_Е!ДЛЬТ_РА_КБТЫБРОЕО

4. Для вариантов №11-20, используя алгоритмы двойной перестановки строк и столбцов, выполнить расшифрование шифрограмм, приведенные в таблице 3. В шифротексте следует обратить внимание на наличие пробелов в тексте, длина текста по всем вариантам равняется 25 символам:

Таблица 3

Вариант	Шифротекст	Ключ 1	Ключ 2
11	В ОН, Т ОЭЗКНОА УОРСЗКНОА	КРУТО	СТУЖА
12	ЗВАОЛИ ЛАН ОДОРОНЧСАЧТЕЗ	ВЕСНА	ОСЕНЬ
13	ПАЙРДЕЕЖ М ЧЕДАТУМЬДУПОМ	ОСЕНЬ	ДОСУГ
14	ДОВХЫМА Т ЕД Г ДО ХВ ИИЩ	ТРАВА	ДОСУГ
15	Т! РООЙЛЮББ ХЛЕТ ВАЕРЫОТК	ПРАВО	ТРАВА
16	ОЖЧЕДЬА Д ТУНДРЕ СВЕЕОП Г	КРУТО	ПРАВО
17	ЕН ПОЕРД ЕОБР!ЗАН А ШИИК	СПОРТ	КРУТО
18	Е ВГОБЫ-М БЕУЗЗ ЛЧЕГОРЬИТ	ВЕТЕР	СПОРТ
19	ГАЛЕР ЗВИИОМУНЗЯТ НЕ РАОП	СТУЖА	ВЕТЕР
20	СЯТООН ОН УЫЖННЫПЕН ЕЖННУ	ДРЕВО	СТУЖА

5. Для вариантов №21-30, используя шифр многоалфавитной замены расшифровать фразу, используя «Ключ» (шифрограммы и ключи приведены в таблице 4).

Таблица 4

Вариант	Шифротекст	Ключ
21	РПЮЫВОНБЩОИТЯФАМХМЯЬЕЕШТТРО	ВЕСНА
22	ПЦМРМОЭУЯЙЙЦЗИЙБЧЙТЙЙХНЧОЬУЕЯШ	ОСЕНЬ
23	ЩЦЦФСЦШБОЕДУГЮБЕЬЪГСЦ	ДОСУГ
24	ГЭЫЙАФШСБТАВПРЛАЦЕПИСБПБЩЧУО	ТРАВА
25	РХЗЙБРЛМОЫЭУОЗЩФУЧЗРКУОДОЯШВВАЛ	ПРАВО
26	ХШЙЧЪПААНЧЩРЮТЕШБЮТПХПШДЭПВЮР	КРУТО
27	ЩЬАХЭЬФШВЕСЪКЭТРВХЮГГЛЖШВЩБЯП	СПОРТ
28	ДФЪЦЛДЕЫЦПДУФРШБЧЧРМПАЧПАХИЪ	ВЕТЕР
29	УБЫЧЫУТЬЧЯУАХСИРДШСЬЮНШРРДХЫ	СТУЖА
30	МЬЕБАСШПКТЙВЗПЬЗГЦРРФХСЗЫЙЬ	ДРЕВО

Расшифрованный текст привести с пробелами.

6. Используя шифр многоалфавитной замены зашифровать фразу из п. 2 (исключив пробелы и знаки препинания) с помощью ключа «Ключ 1» из пункта 3 или 4 или 5 (в зависимости от варианта). Для шифрования использовать алфавит замены из таблицы 5.

Таблица 5

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

РАЗДЕЛ 4. ПРАВИЛА ОЦЕНИВАНИЯ КОНТРОЛЬНОЙ РАБОТЫ

Верное выполнение заданий включает в себя представленные корректные результаты по каждому из пунктов варианта. Недостатками выполнения считаются логическая непоследовательность и внутренняя противоречивость разработанных документов, несогласованность их между собой, несоответствие описанному процессу и действующей нормативно-правовой базе по работе с персональными данными, отсутствие ссылок на нормативно-правовые документы, грамматические и синтаксические ошибки (более 3 на одной странице). За каждый разработанный документ начисляются баллы, указанные в таблице 6. При выявлении указанных недостатков оценка снижается на 1 балл за каждый выявленный недостаток. За полное и правильно выполненное теоретического задания начисляется в сумме 30 баллов.

За верное решение заданий работы начисляются баллы в соответствии со следующей таблицей 6:

Таблица 6

	Список заданий расчетно-графической работы	Начисляемые баллы за верное решение
1	Теоретическая часть	30
2	Практическая часть	60

Верное решение практического задания – это правильное описание требуемых процедур выполнения основных действий.

Таким образом, по каждому блоку студент может набрать максимально по 30 баллов.

Зачёт (без дифференциации) проставляется при получении более 50% по каждому блоку вопросов, а в общей сумме – не менее 60% (т.е. не менее 54 баллов).

Итоговая дифференцированная оценка формируется на основе дифференцированных оценок для каждого блока, определяемых по следующему правилу:

Баллы	0-44	45-50	50-70	70-90
Оценка	Неудовлет-ворительно	Удовлетво-рительно	Хорошо	Отлично

Работы, в которых хотя бы одна из частей оценена менее чем на 50%, подлежат доработке. Работы, в которых присутствуют очевидные признаки несамостоятельного выполнения, к защите не принимаются. В процессе защиты преподаватель может задать дополнительные вопросы по выполненной работе. В случае, если студент не ответил или не верно ответил на вопрос, из общей оценки вычитается 1 балл за каждый неверный ответ или отсутствие ответа. Неверный ответ может быть скомпенсирован двумя правильными ответами на другие вопросы по данной теме.

В случае неудовлетворительной оценки по контрольной работе преподаватель пишет рецензию, которая содержит следующие элементы:

- оценка выполненных заданий в баллах;
- оценка невыполненных элементов задания;
- степень самостоятельности студента при написании работы;
- указания на характер выявленных ошибок, рекомендации по доработке.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Учебные пособия:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. /Источник: Электронно-библиотечная система Znanium [электр]: http://znanium.com/bookread2.php?book=405000

2. Минин, И. В. Защита конфиденциальной информации при электронном документообороте/МининИ.В., МининО.В. - Новосиб.: НГТУ, 2011. - 20 с. /Источник: Электронно-библиотечная система Znanium [электр]: http://znanium.com/bookread2.php?book=546492

3. Малюк, А. А. Защита информации в информационном обществе: Учебное пособие для вузов / Малюк А.А. - М.: Гор. линия-Телеком, 2015. - 230 с. /Источник: Электронно-библиотечная система Znanium [электр]: http://znanium.com/bookread2.php?book=536930

Источники (нормативно-правовые документы):

– Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации» // СПС Консультант Плюс.

– Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне" // СПС Консультант Плюс.

– Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» // СПС Консультант Плюс.

– Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне" // СПС Консультант Плюс.

– Перечень нормативных актов, относящих сведения к категории ограниченного доступа. – [Электронный ресурс] http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=93980