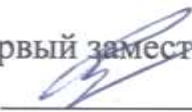


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ЧИТИНСКИЙ ИНСТИТУТ  
КОЛЛЕДЖ

УТВЕРЖДАЮ:  
Первый заместитель директора  
  
Н.В. Раевский  
«25» июня 2024 г.

# **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

## **ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**

Информационная безопасность

Специальность 09.02.07 Информационные системы и программирование

Чита, 2024

## Структура фонда оценочных средств

### по дисциплине «Информационная безопасность»

по специальности 09.02.07 Информационные системы и программирования

№	Содержание	Основные показатели оценки результата	Методы оценки
<b>Умения:</b>			
ОК 1	У 1 определять необходимый уровень безопасности информации У 2 правильно организовать мероприятия по защите информации; У 3 применять в профессиональной деятельности нормативно-правовую базу информационной безопасности.	Создание устного и письменного текста в соответствии с ситуацией общения, коммуникативной задачей, самостоятельное выполнение семинарских и практических работ, решение ситуационных задач	Контрольная работа, контрольный тест, мини-сочинение, публичное выступление, промежуточная аттестация в форме устного зачета, экспертное наблюдение
ПК 4.4	У 4 использовать методы защиты программного обеспечения компьютерных систем; У 5 выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами.	Самостоятельное выполнение семинарских и практических работ, решение ситуационных задач Выполнение исследовательской творческой работы, самостоятельное выполнение семинарских и практических работ, решение ситуационных задач	Публичное выступление, промежуточная аттестация в форме устного зачета, экспертное наблюдение
<b>Знания:</b>			
ОК 1	З 1 основные понятия, объекты, цели и задачи защиты информации; З 2 угрозы информационной безопасности – их классификацию и источники возникновения; З 3 приемы защиты информации; З 4 виды и характеристики современных средств защиты. З 5 классификацию и характеристику компьютерных вирусов;	Дифференциация понятий, связанных с защитой информации; формулирование основных целей и задач защиты информации Перечисление основных угроз информационной безопасности, классификации их по признаку; описание источников возникновения угроз.	Устный опрос, промежуточная аттестация в форме устного зачета, экспертное наблюдение

		<p>Перечисление приемов защиты, видов и характеристик средств защиты информационной безопасности; описание современных средств защиты;</p> <p>дифференциация вида и характеристики средств защиты</p> <p>Перечисление компьютерных вирусов, классификации их по признаку и виду; описание источников возникновения вирусов.</p>	
ПК 4.4	<p>3.6 общую характеристику средств нейтрализации компьютерных вирусов</p> <p>3.7 нормативно-правовую базу информационной безопасности.</p>	<p>Перечисление средств нейтрализации компьютерных вирусов; описание характеристик современных средств защиты;</p> <p>дифференциация средств защиты</p> <p>Дифференциация нормативно-правовой базы; перечисление документов; описание нормативных и правовых документов</p>	<p>Устный опрос, промежуточная аттестация в форме устного зачета, экспертное наблюдение, анализирующая таблица, публичное выступление</p>

№п/п	Тема из рабочей программы	Проверяемые умения, знания, ОК, ПК	Наименование оценочного средства	Критерии оценивания
1.	Основные понятия теории информационной безопасности.	У 1, 2, 3; З 1, 2; ОК 1; ПК 4.4	Устный опрос по теме (5 вопросов)  Практическая работа «Основные типы угроз информационной системы».  Самостоятельная работа по теме «История развития информационной безопасности»	5 правильных ответов – 8-9 баллов 4 правильных ответов – 6-7 баллов 3 правильных ответов – 4-5 баллов 2-0 правильных ответов – 0 баллов  Выполнение практической работы 6-7 балла  Выполнение самостоятельной работы -4 балла Использование дополнительного материала – 2 балл
2.	Методы защиты информационной системы	У 3, 4, 5; З 2, 3, 4, 5, 6, 7; ОК 1; ПК 4.4	Устный опрос по теме (5 вопросов)  Практическая работа № 1 Симметричные алгоритмы. Шифры перестановки. Практическая работа № 2 Потокное и блочное шифрование  Самостоятельная работа «Изучение воздействия компьютерных вирусов»  Самостоятельная работа «Механизмы идентификации и аутентификации»  Исследовательская работа «Изучение компьютерных вирусов и антивирусных программ»	5 правильных ответов – 8-9 баллов 4 правильных ответов – 6-7 баллов 3 правильных ответов – 4-5 баллов 2-0 правильных ответов – 0 баллов  Выполнение практической работы 5-6 балла Выполнение самостоятельной работы -4 балла  Выполнение исследовательской работы - 5 балла

3.	Правовое обеспечение информационной безопасности	У 3, 4, 5; З 3, 4, 5, 7; ОК 1 ПК 4.4	<p>Устный опрос по теме (5 вопросов)</p> <p>Практическая работа №1. «Поиск правовых документов для защиты информации в системе КОНСУЛЬТАНТ+»</p> <p>Практическая работа № 2 «Решение правовых аспектов защиты информации»</p> <p>Индивидуальная работа «Создание системы защиты информации на предприятии»</p>	<p>5 правильных ответов – 8-9 баллов 4 правильных ответов – 6-7 баллов 3 правильных ответов – 4-5 баллов 2-0 правильных ответов – 0 баллов</p> <p>Выполнение практических работ № 1-2 - 5-6 балла</p> <p>Выполнение индивидуальной работы – 10-15 баллов</p>

## **Перечень вопросов для устного опроса по теме 1.**

1. Понятие информационной безопасности
2. Составляющие информационной безопасности
3. Основные определения информационной безопасности
4. История развития информационной безопасности
5. Реализация понятия «информационная безопасность»
6. Нормативные документы по ИБ
7. Органы (подразделения) обеспечивающие ИБ
8. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
9. Программно-технические способы и средства обеспечения информационной безопасности
10. Понятие угрозы и ее основные свойства
11. Классы угроз информационной безопасности
12. Каналы несанкционированного доступа к информации

## Семинар «История развития информационной безопасности»

[illegible]

## **Перечень вопросов для устного опроса по теме 2.**

1. Вирусы, как угроза информационной безопасности
2. Классификация компьютерных вирусов
3. Характеристика "вирусоподобных" программ
4. Антивирусные программы
5. Профилактика компьютерных вирусов
6. Обнаружение неизвестного вируса
7. Определение понятий "идентификация" и "аутентификация"
8. Механизм идентификация и аутентификация пользователей
9. Общие сведения о криптографии
10. Программные средства криптографической защиты
11. Общие сведения о шифровании
12. Симметричные и асимметричные методы шифрования
13. Механизм электронной цифровой подписи
14. Методы разграничения доступа
15. Мандатное и дискретное управление доступом
16. Определение и содержание регистрации и аудита информационных систем
17. Этапы регистрации и методы аудита событий информационной системы
18. Межсетевое экранирование
19. Характеристика межсетевых экранов



## **Самостоятельная работа «Изучение воздействия компьютерных вирусов»**

1. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
2. Сформулируйте признаки стелс-вирусов.
3. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
4. Поясните механизм функционирования "троянской программы" (логической бомбы).
5. Для создания каких вирусов используются полиморфик-генераторы?
6. Принципы функционирования блокировщиков и иммунизаторов.
7. Какие факторы определяют качество антивирусной программы?
8. Какие особенности заражения вирусами при использовании электронной почты?
9. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
10. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?

## Исследовательская работа «Анализ компьютерных вирусов и антивирусных программ»

1. Анализ 3 самых популярных компьютерных вирусов. Заполнить таблицу:

Название вируса	Признаки наличия его в ПК	Класс КВ (3 классификатора)			Способы профилактики и лечения данного вируса
		Среда обитания	Особенности алгоритма работы	Деструктивные возможности	

2. Анализ 3 самых популярных Антивирусных программ. Заполните таблицу:

Название АП	История, версии.	Причина популярности.	Класс АП	Дополнительные сведения

## **Самостоятельная работа «Механизмы идентификации и аутентификации»**

1. Перечислите возможные идентификаторы при реализации механизма идентификации.
2. Перечислите возможные идентификаторы при реализации механизма аутентификации.
3. Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
4. Опишите подробно механизм аутентификации пользователя.
5. Какие методы шифрования используются в вычислительных сетях?
6. Поясните механизм шифрования "налету".
7. Как реализуется симметричный метод шифрования?
8. Как реализуется асимметричный метод шифрования?
9. Что понимается под ключом криптосистемы?
10. Какой метод шифрования используется в электронной цифровой подписи?

## Практическая работа №1 Симметричные алгоритмы. Шифры перестановки.

**Цель:** Познакомиться с различными симметричными алгоритмами шифрования

**Задание:** Зашифровать свои ФИО различными способами

При шифровании перестановкой символы шифруемого текста переставляются по определенному правилу в пределах блока этого текста. Шифры перестановки являются самыми простыми и, вероятно, самыми древними шифрами.

### Шифр перестановки "скитала"

Известно, что в V веке до нашей эры правители Спарты, наиболее воинственного из греческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью *скитала*, первого простейшего криптографического устройства, реализующего метод простой перестановки.

Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который назывался *скитала*, наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения, как на рисунке 1. Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично. Такой же результат можно получить, если буквы сообщения писать по кольцу не подряд, а через определенное число позиций до тех пор, пока не будет исчерпан весь текст.

	Н	А	С	Т	
	У	П	А	Й	
	Т	Е			

Рисунок 1 Шифр "скитала"

Сообщение НАСТУПАЙТЕ при размещении его по окружности стержня по три буквы дает шифртекст НУТАПЕСА\_ТЙ

Для расшифрования такого шифртекста нужно не только знать правило шифрования, но и обладать ключом в виде стержня определенного диаметра. Зная только вид шифра, но не имея ключа, расшифровать сообщение было непросто. Шифр скитала многократно совершенствовался в последующие времена.

### Шифрующие таблицы

С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. Наряду с традиционными применениями криптографии в политике, дипломатии и военном деле появляются и другие задачи - защита интеллектуальной собственности от преследований инквизиции или заимствований злоумышленников. В разработанных шифрах перестановки того времени применяются шифрующие таблицы, которые в сущности задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

- размер таблицы;
- слово или фраза, задающие перестановку;
- особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром *скитала*. Например, сообщение

ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ

записывается в таблицу поочередно по столбцам. Результат заполнения таблицы из 5 строк и 7 столбцов показан на рисунке 2.

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам.



Рисунок 2 Заполнение таблицы из 5 строк и 7 столбцов

Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение:

ТНПВЕ ГЛЕАР АДОНР ТИЕБВ ОМОБТ МПЧИР ЫСООБ

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровании действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим в качестве ключа, например, слово

ПЕЛИКАН,

П	Е	Л	И	К	А	Н
7	2	5	3	4	1	6
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Б	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Б

До перестановки

А	Е	И	К	Л	Н	П
1	2	3	4	5	6	7
Г	Н	В	Е	П	Л	Т
О	А	А	Д	Р	Н	Е
В	Т	Е	Б	И	О	Р
П	О	Т	М	Б	Ч	М
О	Р	С	О	Ы	Б	И

После перестановки

Рисунок 3 Таблицы, заполненные ключевым словом и текстом сообщения

а текст сообщения возьмем из предыдущего примера. На рисунке 3 показаны две таблицы, заполненные текстом сообщения и ключевым словом, при этом левая таблица соответствует заполнению до перестановки, а правая таблица - заполнению после перестановки.

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были пронумерованы слева направо. В правой таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

При считывании содержимого правой таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение:

ГНВЕП ЛТООА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОБЫИ

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется *двойной перестановкой*. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

Пример выполнения шифрования методом двойной перестановки показан на рисунке 4. Если считать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее:

ТЮАЕ ООГМ РЛИП ОБСВ

Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Б
2	М	О	Г	О

Исходная  
таблица

	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Б	С	В
2	О	О	Г	М

Перестановка  
столбцов

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Б	С	В

Перестановка  
строк

Рисунок 4 Пример выполнения шифрования методом двойной перестановки

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

- для таблицы 3x3 36 вариантов;
- для таблицы 4x4 576 вариантов;
- для таблицы 5x5 14400 вариантов.

Однако двойная перестановка не отличается высокой стойкостью и сравнительно просто "взламывается" при любом размере таблицы шифрования.

### Применение магических квадратов

В средние века для шифрования перестановкой применялись и магические квадраты.

*Магическими квадратами* называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила.

Пример магического квадрата и его заполнение сообщением

ПРИЛЁТАЮ ВОСЬМОГО показан на рисунке 5.

16	3	2	13	О	И	Р	М
5	10	11	8	Е	О	С	Ю
9	6	7	12	В	Т	А	Ь
4	15	14	1	Л	Г	О	П

Рисунок 5 Пример магического квадрата 4x4 и его заполнения сообщением

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид:

ОИРМ ЕОСЮ ВТАЬ ЛГОП

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3x3 (если не учитывать его повороты). Количество магических квадратов 4x4 составляет уже 880, а количество магических квадратов 5x5 - около 250000.

## Практическая работа № 2 Потокное и блочное шифрование

**Цель:** на конкретных примерах рассмотреть шифрование сообщений симметричного алгоритма шифрования, определить какое программное обеспечение на ваш взгляд является оптимальным.

### Ход работы

При шифровании симметричным ключом используются одинаковые ключи для шифрования и расшифровывания сообщений. Ключ этот имеют (если он используется для шифрования сообщения) только отправитель и адресат, он не должен быть известен третьему лицу. Поэтому главная проблема симметричной криптографии состоит в предварительной передаче секретного ключа одним абонентом другому по надежному каналу. Это неудобство, однако, не мешает в случае, когда создатель и получатель сообщения одно и то же лицо (т.е. вы шифруете свою информацию на компьютере, храните ее какое-то время в зашифрованном виде, а затем расшифровываете, чтобы использовать).

Кроме деловой переписки у вас есть ведь, конечно, и личные секреты, о которых нежелательно знать другим: список телефонов «нужных людей»; каталог избранных сайтов; письма информатора из фирмы конкурента; план рекламной компании; бизнес-план производства нового продукта и т.д. Нет ничего некорректного в том, что вы хотите сохранить в тайне свою конфиденциальную информацию.

### Задание

Установите программы для симметричного и асимметричного шифрования сообщений. Заполните таблицу 1 (в бланке отчета по практическим работам), зашифровав сообщение, папку с файлами, проверяя возможность смены типа данных и т.д. После работы с программой удалите ее. Сделайте выводы.

**Таблица 1**

Программа	Характеристики
Бесплатное ПО	
<b>AES Free</b>	Очень простая в пользовании программа. Использует алгоритм шифрования <b>AES</b> , длина ключа 128 бит, максимальная длина пароля — 7 символов. Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся зашифрованные файлы, изменять расширение шифруемых файлов, шифровать целиком папки со всем содержимым.
<b>FineCrypt</b>	Очень мощная, но довольно сложная в пользовании программа. Предлагает на выбор 10 алгоритмов шифрования, имеет шредер и архиватор, позволяет создавать самораспаковывающиеся файлы.
<b>Dpccrypto</b>	Очень простая в использовании программа для шифрования отдельных файлов. Использует 8 алгоритмов. Не имеет никаких дополнительных функций.
Платное ПО	
<b>EasyCrypto Deluxe</b>	Отлично оформленная программа для шифрования отдельных файлов. Использует алгоритм Blowfish с длиной ключей от 40 до 128 бит и паролями до 8 букв.
<b>Crypto-Lock</b>	Очень простая программа для шифрования отдельных файлов. Использует алгоритм Blowfish. Способна создавать самораспаковывающиеся файлы.
<b>Iron Key</b>	Не очень удобная в пользовании программа. Использует алгоритм DES, длина ключа 56 бит. Не имеет никаких дополнительных функций. Пригодна для шифрования отдельных файлов.
<b>SafeGuard PrivateCrypto</b>	Отлично оформленная и очень простая программа для шифрования отдельных файлов. Использует алгоритм AES. Способна создавать самораспаковывающиеся файлы.

Большинство их настолько просты в пользовании, что любой ребенок, владеющий компьютером, является нынче лучшим шифровальщиком, чем знаменитые математики и разведчики прошлого. Давайте посмотрим, как осуществляется защита документов на примере перечисленных в таблице программ.

### **Перечень вопросов для устного опроса по теме 3.**

1. Принципы построения системы информационной безопасности
2. Требования к защите информации
3. Этапы разработки систем защиты
4. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации
5. Ответственность за нарушения в сфере информационной безопасности
6. Понятие угрозы и ее основные свойства
7. Классы угроз информационной безопасности
8. Каналы несанкционированного доступа к информации



## **Индивидуальная работа «Создание системы защиты информации на предприятии»**

Система защиты информации — это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия. Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления (АСУ) и задействованы при выполнении бизнес-процессов.

Основные угрозы для информационной безопасности любой компании связаны с кражей данных (например, промышленный шпионаж), использованием непроверенного программного обеспечения (например, содержащего вирусы), хакерскими атаками, получением спама (также может содержать вирусы), халатностью сотрудников. Реже утрата данных вызвана такими причинами, как сбой в работе аппаратно-программного обеспечения или кража оборудования. В результате компании несут значительные потери.

Процесс создания системы защиты информации можно разделить на три этапа:

- формирование политики предприятия в области информационной безопасности;
- выбор и внедрение технических и программных средств защиты;
- разработка и проведение ряда организационных мероприятий.

При этом следует учитывать государственные нормативные документы и стандарты, которые регулируют вопросы информационной безопасности на предприятиях нефтегазового комплекса.

### **Политика предприятия в области информационной безопасности**

Фундаментом для создания системы защиты информации является документ, в котором формулируются принципы и основные положения политики предприятия в области информационной безопасности. Какие вопросы он охватывает?

**1. Разработка правового обеспечения защиты информации.** Фактически это система нормативно-правовых документов, актуальных для деятельности предприятия. С ее помощью, с одной стороны, определяются правила обеспечения информационной безопасности на предприятии (например, обязанности сотрудников), а с другой — устанавливается ответственность за их нарушение. В состав правового обеспечения включаются государственные законы и акты (например, закон о государственной тайне), внутренние нормативные и организационные документы предприятия (устав, правила внутреннего распорядка, инструкции для сотрудников о сохранении коммерческой или иной тайны и т.д.).

**2. Определение потенциальных угроз безопасности информации.** Их можно разделить на три группы — это угрозы, возникающие:

- вследствие действий человека — это могут быть как случайные ошибки специалистов предприятия при работе с информационной системой (неправильный ввод данных или их удаление), так и преднамеренные действия (кража документов или носителей информации);
- вследствие некорректной работы или отказа технических или программных средств (например, сбой в работе операционной системы, вызванный вирусом);
- из-за стихийных бедствий, природных катаклизмов, форс-мажорных обстоятельств (наводнения, пожары, смерчи, военные действия и т.д.).

Список потенциальных угроз для информационной безопасности предприятия может быть очень велик. Рекомендуется оценить каждую из них с позиции здравого смысла или данных статистики, а затем проранжировать по степени вероятности возникновения и объема потенциального ущерба.

**3. Составление перечня данных, подлежащих защите.** Информация, которая используется на предприятии, может быть открытой (доступна для всех) или закрытой (доступна для ограниченного круга лиц). К первому типу относятся сведения, которые не составляют государственной или коммерческой тайны, не относятся к категории конфиденциальной информации (согласно законодательству или внутренним документам предприятия). Ущерб от потери подобного рода сведений не является значительным, поэтому их защита не приоритетна.

Ко второму типу относятся:

- данные, являющиеся государственной тайной — их перечень определяется законодательством;
- коммерческие или служебные сведения — любая информация, связанная с производством, финансами, использующимися технологиями, утечка или утрата которой может нанести ущерб интересам предприятия;
- персональные данные сотрудников.

Эта информация должна быть защищена в первую очередь. Для каждого типа такого рода данных указывается, как и где они возникают, с помощью каких программных или технических средств ведется их обработка, какие подразделения (сотрудники) с ними работают и т.д.

**4. Создание подразделения, ответственного за вопросы защиты информации.** Как правило, на российских предприятиях существует разделение функций, связанных с обеспечением информационной безопасности. Это подразумевает, что за разработку политики защиты данных, выполнение организационных мер отвечает служба безопасности компании, а вопросы, связанные с применением любых программных и аппаратных средств, включаются в компетенцию ИТ-подразделения. Нередко возникают ситуации, когда стремление как можно надежнее защитить данные вступает в противоречие с потребностями бизнеса предприятия. В том числе это происходит, если меры безопасности разрабатываются без учета возможностей современных ИТ-средств.

Например, на одном из предприятий служба безопасности запретила сотрудникам иметь доступ к рабочему адресу электронной почты из внешней среды, мотивируя свое решение необходимостью избежать утечек информации. В результате стали возникать задержки при выполнении бизнес-процессов: сотрудники не могли оперативно принимать необходимые управленческие решения, если они находились не в офисе предприятия. Участие в разработке подобной меры сотрудников ИТ-подразделения позволило бы избежать этой проблемы: доступ к рабочей почте был бы сохранен, а защита данных обеспечивалась бы за счет применения дополнительных программных средств.

Поэтому более правильным подходом является создание единой точки принятия решений, а именно создание подразделения, задачей которого будет решение всего спектра вопросов по защите информации на предприятии. В его состав необходимо включить как сотрудников службы безопасности, так и ИТ-специалистов.

**5. Определение основных направлений обеспечения информационной безопасности.** В рамках решения этой задачи, в частности, обозначаются компоненты АСУ, которые нуждаются в защите, определяются необходимые программные и технические средства, формулируются организационные меры, направленные на защиту информации.

**Защита автоматизированной системы управления: программные и технические средства**

Основным вопросом в плане обеспечения информационной безопасности является защита автоматизированной системы управления (ее возможная структура приведена на рис. 1), которая осуществляется за счет применения программных и технических средств.

Сложность решения этой задачи обуславливается двумя факторами. Во-первых, доступ к ресурсам системы имеет огромное количество пользователей (несколько тысяч человек), которые находятся в нескольких территориально-распределенных подразделениях. Во-вторых, ее работа строится на взаимодействии целого ряда программных и аппаратных компонентов.

## **Структура контрольно-оценочных материалов для аттестации по учебной дисциплине**

По дисциплине проводится зачет.

Вопросы к зачету:

1. Свойства информации.
2. Понятие информационной системы.
3. Структура информационной системы.
4. Классификация информационных систем.
5. Понятие и виды угроз безопасности информации.
6. Модель нарушителя в автоматизированных системах обработки информации.
7. Понятие несанкционированного доступа к информации.
8. Основные способы несанкционированного доступа к информации.
9. Концепция обеспечения информационной безопасности.
10. Методы обеспечения информационной безопасности.
11. Правила и средства разграничения доступа в автоматизированных информационных системах.
12. Классификация автоматизированных систем по степени защищенности от несанкционированного доступа к информации.
13. Классификация средств вычислительной техники по степени защищенности от несанкционированного доступа к информации.
14. Понятие информационного права.
15. Принципы информационного права.
16. Субъекты информационных правоотношений.
17. Понятие государственной тайны
18. Понятие коммерческой и служебной тайн.
19. Понятие персональных данных.
20. Правовые аспекты компьютерной сети Интернет.
21. Административная ответственность за информационные правонарушения.
22. Уголовная ответственность за информационные преступления.
23. Информационные аспекты трудовых отношений.
24. Основы стандартизации и сертификации информационных технологий.
25. Принципы построения защиты автоматизированной информационной системы.
26. Основные понятия криптографии.
27. Шифры сложной замены (на примере системы шифрования Вижинера).
28. Американский стандарт шифрования данных DES.
29. ГОСТ 28147-89. Шифрование данных в режиме простой замены.
30. ГОСТ 28147-89. Шифрование данных в режиме гаммирования.
31. ГОСТ 28147-89. Шифрование данных в режиме гаммирования с обратной связью.
32. ГОСТ 28147-89. Выработка имитовставки.
33. Криптосистема шифрования данных RSA.
34. Хэш-функции. Свойства хэш-функций.
35. Функция хеширования ГОСТ Р 34.11-94.
36. Электронная цифровая подпись (общие понятия). Алгоритм цифровой подписи RSA.

- 37.Алгоритм цифровой подписи Эль Гамала (EGSA).
- 38.Алгоритм цифровой подписи DSA.
- 39.Отечественный стандарт цифровой подписи ГОСТ Р 34.11-94.
- 40.Правовые основы использования электронной цифровой подписи.