Министерство науки и высшего образования Российской Федерации
Лысьвенский филиал
федерального государственного автономного образовательного учреждения
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
**для проведения промежуточной аттестации обучающихся
по дисциплине
«Защита информации в компьютерных системах»**
***Приложение к рабочей программе дисциплины***

| | |
|---|---|
| **Направление подготовки:** | 09.03.01Информатика и вычислительная техника |
| **Направленность (профиль) образовательной программы:** | Компьютерные системы |
| **Квалификация выпускника:** | «Бакалавр» |
| **Выпускающая кафедра:** | Технических дисциплин |
| **Форма обучения:** | Очная, очно-заочная, заочная |

**Курс:** 3 (5, 4) **Семестр**: 6 (9, 8)

**Трудоёмкость:**
Кредитов по рабочему учебному плану: 5 ЗЕ
Часов по рабочему учебному плану: 180 ч.

**Форма промежуточной аттестации:**
Экзамен: 6 (9,8 ) семестр

Лысьва 2024

**Фонд оценочных средств** для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

## 1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД освоение учебного материала дисциплины запланировано в течение одного семестра (6- го семестра учебного плана очной формы обучения, 9-го семестра учебного плана очно-заочной формы обучения, 8-го семестра учебного плана заочной формы обучения). В семестре предусмотрены аудиторные лекционные, лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

| **Контролируемые результаты обучения по дисциплине (ЗУВы)** | **Вид контроля** | | | |
|---|---|---|---|---|
| | **Текущий** | **Рубежный** | | **Итоговый** |
| | **ТО** | **ОЛР** | **КР/Т** | **экзамен** |
| **Усвоенные знания** | | | | |
| **З.1** *Знать:*<br>- основные понятия и направления в защите программного обеспечения;<br>-основные понятия и направления в защите программного обеспечения;<br>- источники, риски, формы атак на информацию;<br>-основные стандарты оценивания защищенности;<br>-основные уязвимости программного обеспечения. | ТО1 | | Т1<br>Т2 | ТВ |
| **Освоенные умения** | | | | |
| **У.1** *Уметь:*<br>- инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного | | ОЛР1-ОЛР8 | Т1<br>Т2 | ПЗ |

| | | | | |
|---|---|---|---|---|
| обеспечения;<br>-использовать парольные системы аутентификации;<br>-применять средства и методы предотвращения вторжений | | | | |
| **Приобретенные владения** | | | | |
| **В.1** *Владеет навыками:*<br>- осуществления мер противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты.<br>- установки и настройки программного обеспечения для защиты от вредоносного программного обеспечения. | | ОЛР1-ОЛР8 | | ПЗ |

*С – собеседование по теме; ТО –теоретический опрос; КЗ – комплексное задание (индивидуальное задание); ОЛР – отчет по лабораторной работе; КР/Т – рубежная контрольная работа, тестирование; ТВ – теоретический вопрос; ПЗ – практическое задание.*

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в форме экзамена, проводимая с учётом результатов текущего и рубежного контроля.

## 2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

**2.1. Текущий контроль усвоения материала**

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

**2.2. Рубежный контроль**

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) в форме защиты лабораторных работ и рубежного тестирования

**2.2.1. Защита лабораторных работ**

Всего запланировано 8 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторных работ проводится индивидуально каждым студентом или группой студентов.

Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

**2.2.2. Рубежное тестирование**

Запланировано 4 рубежных тестирования (Т) после освоения студентами лекционного материала и лабораторных работ. Первое ТР - «Понятие информационной безопасности», второе Т – «Источники опасности для информации», третье Т – «Средства защиты информации», четвертое Т «Криптографическая защита информации»,

Типовые шкала и критерии оценки рубежного тестирования приведены в общей части ФОС образовательной программы.

**Типовое задание первого Т**:

**1) К правовым методам, обеспечивающим информационную безопасность, относятся:**

1) Разработка аппаратных средств обеспечения правовых данных
2) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2) Основными источниками угроз информационной безопасности являются все указанное в списке:**

1) Хищение жестких дисков, подключение к сети, инсайдеров
2) Перехват данных, хищение данных, изменение архитектуры системы
3) Хищение данных, подкуп системных администраторов, нарушение регламента работы

**3) Виды информационной безопасности:**

1) Персональная, корпоративная, государственная
2) Клиентская, серверная, сетевая
3) Локальная, глобальная, смешанная

**4) Цели информационной безопасности – своевременное обнаружение, предупреждение:**

1) несанкционированного доступа, воздействия в сети
2) инсайдерства в организации
3) чрезвычайных ситуаций

**5) Основные объекты информационной безопасности:**

1) Компьютерные сети, базы данных
2) Информационные системы, психологическое состояние пользователей

**6) Основными рисками информационной безопасности являются:**

1) Искажение, уменьшение объёма перекодировка информации
2) Техническое вмешательство, выведение из строя оборудование сети
3) Потеря, искажение, утечка информации

**7) К основным принципам обеспечения информационной безопасности относится:**

1) Экономической эффективности системы безопасности
2) многоплатформенной реализации системы
3) Усиление защищенности всех звеньев системы

**8) Основными субъектами информационной безопасности являются:**……..

**9) К основным функциям системы безопасности можно отнести все перечисленное:**…….

**10) Принципом информационной безопасности является принцип недопущения:**……

**11) Принципом политики информационной безопасности является принцип:**……..

**12) Принципом политики информационной безопасности является принцип:**…….

**13) Принципом политики информационной безопасности является принцип:**…….

**14) К основным типам средств воздействия на компьютерную сеть относится:**……

**15) Когда получен спам по e-mail с приложенным файлом, следует**……

**16) Принцип Кирхгофа:**…….

**17) ЭЦП – это:**……

**18) Наиболее распространены угрозы информационной безопасности корпоративной системы:**……

**19) Наиболее распространены угрозы информационной безопасности сети:**……..

**20) Наиболее распространены средства воздействия на сеть офиса:**……

**21) Утечкой информации в системе называется ситуация, характеризуемая:**…….

**22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**……...

**23) Угроза информационной системе (компьютерной сети) – это:**……

**24) Информация, которую следует защищать (по нормативам, правилам**…….

**25) Разновидностями угроз безопасности (сети, системы) являются :**……

**26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:**…….

**27) Политика безопасности в системе (сети) – это комплекс:**……..

**28) Наиболее важным при реализации защитных мер политики безопасности является**:…….

Ключ к тесту:

| № вопр | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Отв. | 3 | 2 | 2 | 1 | 1 | 3 | 1 |

| | |
|---|---|
| 8 | органы права, государства, бизнеса |
| 9 | установление регламента, аудит системы, выявление рисков |
| 10 | неоправданных ограничений при работе в сети (системе) |
| 11 | невозможности миновать защитные средства сети (системы) |
| 12 | усиления защищенности самого незащищенного звена сети (системы) |
| 13 | разделения доступа (обязанностей, привилегий) клиентам сети (системы) |
| 14 | логические закладки («мины») |
| 15 | сохранить приложение в парке «Спам», выяснить затем IP-адрес |
| 16 | секретность закрытого сообщения определяется секретностью ключа |
| 17 | электронно-цифровая подпись |
| 18 | ошибки эксплуатации и неумышленного изменения режима работы системы |
| 19 | сбой (отказ) оборудования, нелегальное копирование данных |
| 20 | вирусы в сети, логические мины (закладки), информационный перехват |
| 21 | потерей данных в системе |
| 22 | Целостность |
| 23 | вероятное событие |
| 24 | Правовой |
| 25 | программные, технические, организационные, технологические |
| 26 | владелец сети |
| 27 | руководств, требований обеспечения необходимого уровня безопасности |
| 28 | аудит, анализ уязвимостей, риск-ситуаций |

**Типовое задание второго Т**:
**Тестовые задания**

**1.Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это**

1. информационная война
2. информационное оружие
3. информационное перво

**2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами**

1. служебная информация
2. Коммерческая тайна

3. банковская тайна
4. конфиденциальная информация

**3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена**

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. аппелеруемость

**4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано**

1. надежность
2. точность
3. контролируемость
4. устойчивость
5. доступность

**5. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые**

1. принцип системности
2. принцип комплексности
3. принцип непрерывный защиты
4. принцип разумной достаточности
5. принцип гибкости системы

**6. В классификацию вирусов по способу заражения входят**

1. опасные
2. файловые
3. резидентные

**7. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это**

1. комплексное обеспечение
2. безопасность АС
3. угроза ИБ
4. атака на АС
5. политика безопасности

**8. Что не относится к информационной инфекции:**……..

**9. К видам системы обнаружения атак относятся :**……..

**10. Автоматизированная система должна обеспечивать**……..

**11. Основными компонентами парольной системы являются** ……..

**12. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это** ……..

**13. К принципам информационной безопасности относятся**……

**14. К вирусам изменяющим среду обитания относятся:**…….

**15. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это**…….

**16. Система физической безопасности включает в себя следующие подсистемы:**…….

**17. Какие степени сложности устройства Вам известны**……..

**18. К механическим системам защиты относятся:**……..

**19. Какие компоненты входят в комплекс защиты охраняемых объектов:**…….

**20. К выполняемой функции защиты относится:**……

**21. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:**…….

**22. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:**……..

**23. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:**…….

**24. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:**…….

**25. Гарантия точного и полного выполнения команд в АС:**……

**26. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:**……..

**27. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:**……..

**28. Особенностями информационного оружия являются:**…….

Ключ к тесту:

| № вопр. | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Отв. | 1 | 4 | 1 | 1 | 5 | 3 | 1 |

| | |
|---|---|
| 8 | фальсификация данных |
| 9 | все варианты верны |
| 10 | Доступность, целостность |
| 11 | интерфейс администратора, база данных учетных записей |
| 12 | пароль пользователя |
| 13 | Системность, законность, открытости алгоритмов |
| 14 | системность |
| 15 | Защита информации |
| 16 | оценка обстановки, строительные препятствия, аварийная и пожарная сигнализация |
| 17 | Простые, сложные |
| 18 | Проволока, стена, вы |
| 19 | Сигнализация, охрана, датчики, телевизионная система |
| 20 | внешняя защита, внутренняя защита |
| 21 | коммерческая тайна |
| 22 | Компьютерная безопасность |
| 23 | коммерческая тайна |
| 24 | целостность |
| 25 | точность |
| 26 | принцип разумной достаточности |
| 27 | политика безопасности |
| 28 | Универсальность, скрытность |

## Типовое задание третьего Т:
## Тестовые задания

**1.Идентификатор субъекта доступа, который является его секретом**:

1. пароль
2. ключ
3. электронно-цифровая подпись

**2. Исследование возможности расшифрования информации без знания ключей:**

1. криптология
2. криптоанализ
3. взлом

**3. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:**

1. информационная безопасность
2. безопасность
3. защита информации

**4. Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:**

1. информационная война
2. информационное оружие
3. информационное превосходство

**5. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:**

1. интересы государства
2. интересы личности
3. интересы личности ИБ

**6. Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:**

1. служебная информация
2. банковская тайна
3. конфиденциальная информация

**7. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:**

1. атака на автоматизированную систему
2. безопасность АС
3. политика безопасности

**8. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы**……

**9. Вся накопленная информация об окружающей нас дейст вительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными**

**потребителями для решения научных, производст венных, управленческих и других задач**……..

**10. К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан** ……»

**11. Состояние защищенности при котором не угрожает опасность это:**……

**12. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:**……..

**13. Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств:**……

**14. Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя , суверенитета и территориальной целостности это:**…….

**15. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы**

**16. К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право**…….»

**17. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:**……..

**18. Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:**……..

**19. Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:**……

**20. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:**……..

**21. Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:**……..

**22. Гарантия того, что в любой момент времени может быть произведена полноценная проверка любого компонента программного комплекса АС:**……..

**23. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:**……..

**24. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:**……

**25. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а так же системы регулирования возникающих при этом общественных отношений**……

**26. К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками**…….»

**27. Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:**……..

**28. Защищенность от негативных информационно-психологических и информационно- технических воздействий:**……

Ключ к тесту:

| № вопр. | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Отв. | 1 | 2 | 1 | 2 | 2 | 3 | 1 |

| | |
|---|---|
| 8 | Атака на автоматизированную систему |
| 9 | Информационные ресурсы |
| 10 | Информация без ограничения права доступа |
| 11 | Безопасность |
| 12 | Защита информации |
| 13 | Информационная война |
| 14 | Интересы государства в информационной сфере |
| 15 | Информационная система |
| 16 | Объект интеллектуальной собственности |
| 17 | Национальная безопасность |
| 18 | Защищенность потребителей информации |
| 19 | Информационное оружие |
| 20 | Государственная тайна |

| | |
|---|---|
| 21 | Доступность |
| 22 | Контролируемость |
| 23 | Принцип непрерывной защиты |
| 24 | Угрозы информационной безопасности |
| 25 | Информационная сфера |
| 26 | Информация, распространение которой наносит вред интересам общества |
| 27 | Национальная безопасность |
| 28 | Защищенность потребителей информации |

**Типовое задание четвертого Т**:
**Тестовые задания**

1. ***Преобразование открытого текста сообщения в закрытый называется***:

1) процедура шифрования;
2) алгоритм шифрования;
3) обеспечение аутентификации;
4) цифровая запись.

2. ***Входные параметры процесса шифрования {несколько верных ответов)***:

1) зашифрованный текст;
2) ключ;
3) открытый текст;
4) алгоритм.

3. ***Какие из сервисов реализуются при использовании криптографических преобразований {несколько верных ответов*)**:

1) контроль целостности;
2) аутентификация;
3) шифрование;
4) алгоритм.

4. ***Что позволяет предотвратить использование криптографических преобразований***:

1) отказ от информации;
2) обеспечение аутентификации;
3) утечку информации;
4) использование алгоритмов асимметричного шифрования.

5. ***Знание ключа позволяет***:

1) использовать криптографические сервисы безопасности;
2) обеспечить аутентификацию;
3) предотвратить утечку информации;
4) выполнить обратное преобразование.

6. ***Что в криптографии понимается под термином «элементарное опробование»***:

1) операция над двумя «-разрядными двоичными числами;

2) проверка ключа на целостность;

3) сопоставление двух паролей;

4) передача ключа по какому-либо каналу связи.

7. ***Чем определяется уровень надежности применяемых криптографических преобразований***:

1) значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;

2) сложностью комбинации символов, выбранных случайным образом;

3) использованием большого числа ключей для шифрования;

4) отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.

**8. Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее:…….**

**9. Что называется имитовставкой:……**

**10. Как иначе называется симметричное шифрование:……**

**11. Какой алгоритм не используется при симметричном шифровании:**

**12. Какой из режимов алгоритма DES используется для построения шифров гаммирования?.....**

**13. Какова длина блока алгоритма шифрования DES:…….**

**14. Сколько всего циклов выполняется операция зашифровывания в алгоритме DES:……..**

**15. Что является преимуществом симметричного шифрования:…….**

**16. Какой размер ключа в отечественном стандарте симметричного шифрования:……**

**17. Какие из режимов шифрования данных не включает в себя отечественный стандарт симметричного шифрования:…….**

**18. Использует ли отечественный стандарт симметричного шифрования дополнительный ключ:…….**

**19. Какое из этих утверждений является верным:……..**

**20. Используется ли в отечественном стандарте симметричного шифрования процедура генерации подключей из ключей, как в DES:……**

**21. В отечественном стандарте симметричного шифрования применяется подстановка, основанная на применении S-блоков. Сколько таких блоков используется в ГОСТ:……..**

**22. Длинараундового ключа в отечественном стандарте симметричного шифрования:……**

**23. Выберите правильное утверждение:…….**

**24. Что означает «многократное шифрование» применительно к блочным шифрам:……**

**25 Что в переводе с греческого языка означает слово «криптография»?.....**

**26. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?.....**

**27. Когда в криптографии стало использоваться асимметричное шифрование?.....**

**28. Гарантирование невозможности несанкционированного изменения информации - это:……**

Ключ к тесту:

| № вопр. | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Отв. | 1 | 2, 3 | 1, 2 | 3 | 4 | 1 | 1 |

| | |
|---|---|
| 8 | обеспечение постоянного числа пользователей сети; |
| 9 | это блок данных фиксированной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты. |
| 10 | шифрование с закрытым ключом; |
| 11 | алгоритм Эль-Гамаля. |
| 12 | обратная связь по выходу |
| 13 | 64 бита |
| 14 | 16; |
| 15 | скорость выполнения криптографических преобразований; |

| | |
|---|---|
| 16 | 256 бит. |
| 17 | режим обратной связи по шифротексту; |
| 18 | да |
| 19 | у S-блоков ГОСТ 4-битовые входы и выходы; |
| 20 | да, но эта процедура сравнительно проста; |
| 21 | 8 |
| 22 | ) 8 бит |
| 23 | в отечественном стандарте симметричного шифрования нет начальной и конечной битовых перестановок шифруемого блока, так как они не влияют на стойкость шифра |
| 24 | шифрование одного и того же блока открытого текста несколько раз с несколькими ключами |
| 25 | тайнопись |
| 26 | шифр Цезаря |
| 27 | во второй половине XX |
| 28 | обеспечение целостности |

**2.3. Промежуточная аттестация (итоговый контроль)**

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит тест вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных компетенций.

Тест формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма теста представлена в общей части ФОС образовательной программы.

**2.3.1. Типовые вопросы и задания для экзамена по дисциплине**
**Типовые вопросы для тест контроля усвоенных знаний:**

1. Кто является основным ответственным за определение уровня классификации информации:
а) руководитель среднего звена
б) владелец
в) высшее руководство

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры

б) контрагенты
в) сотрудники

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

4. Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы

6. Что такое процедура?.....

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?.....

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?.....

9. Что такое политики безопасности?.....

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?.....

11. Что лучше всего описывает цель расчета ALE?.....

12. Тактическое планирование – это:…….

13. Что является определением воздействия (exposure) на безопасность?.....

14. Эффективная программа безопасности требует сбалансированного применения:……..

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:……..

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?.....

17. Как рассчитать остаточный риск?.....

18. Что из перечисленного не является целью проведения анализа рисков?.....

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?.....

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?.....

Ключ к тесту:

| № вопр. | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Отв. | б | в | б | в | б |

| | |
|---|---|
| 6 | Пошаговая инструкция по выполнению задачи |
| 7 | Поддержка высшего руководства |
| 8 | Когда стоимость контрмер превышает ценность актива и потенциальные потери |
| 9 | Широкие, высокоуровневые заявления руководства |
| 10 | Анализ затрат / выгоды |
| 11 | Оценить потенциальные потери от угрозы в год |
| 12 | Среднесрочное планирование |
| 13 | Нечто, приводящее к ущербу от угрозы |
| 14 | Технических и нетехнических методов |
| 15 | Уровень доверия, обеспечиваемый механизмом безопасности |
| 16 | Военным требуется больший уровень безопасности, т.к. их риски существенно выше |
| 17 | (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля |
| 18 | Делегирование полномочи |
| 19 | Выполнение анализа рисков |
| 20 | Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа |

**Типовые вопросы и практические задания для контроля освоенных умений и приобретенных владений:**

1. Система сертификации средств криптографической защиты информации.
2. Виды и схемы сертификации средств криптографической защиты информации.
3. Особенности подготовки и проведения сертификации

криптографических средств защиты информации.

### 2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

## 3. Критерии оценивания уровня сформированности компонентов и компетенций

### 3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

### 3.2.Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в форме экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.