МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего профессионального образования

**«Дальневосточный федеральный университет»**

(ДВФУ)

## ШКОЛА ЕСТЕСТВЕННЫХ НАУК

| «СОГЛАСОВАНО» | «УТВЕРЖДАЮ» |
|---|---|
| Руководитель образовательной программы | Заведующий кафедрой компьютерных систем |
| Должиков С.В. | Кулешов Е.Л. |
| 18 июня 2015 г. | 18 июня 2015 г. |

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

Информационная безопасность и защита информации

**Направление подготовки – 09.03.02 «Информационные системы и технологии»**

Профиль «Информационные системы и технологии в связи»

**Форма подготовки (очная)**

курс 2 семестр 4
лекции 36 час.
практические занятия 18 час.
лабораторные работы час.
в том числе с использованием МАО лек. 0 / пр.11 / лаб. 0 час.
всего часов аудиторной нагрузки – 54 час.
в том числе с использованием МАО – 11 час.
самостоятельная работа 90 час.
контрольные работы (количество)
курсовая работа / курсовой проект – не предусмотрен
зачет 4 семестр
экзамен - семестр

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 12 марта 2015 г. № 219.

Рабочая программа обсуждена на заседании кафедры компьютерных систем, протокол № _14_ от «_18_» _июня 2015 г.

Заведующий кафедрой компьютерных систем. д.т.н., профессор Кулешов Е.Л.
Составитель (ли): доцент кафедры компьютерных систем Должиков С.В. к.т.н., доцент

**Оборотная сторона титульного листа РПУД**

**I. Рабочая программа пересмотрена на заседании кафедры**:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

**II. Рабочая программа пересмотрена на заседании кафедры**:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

# АННОТАЦИЯ

Дисциплина «Информационная безопасность и защита информации» предназначена для бакалавров, обучающихся по направлению подготовки 09.03.02 «Информационные системы и технологии», профиль «Информационные системы и технологии в связи», входит в блок Дисциплины (модули) учебного плана, является базовой дисциплиной вариативной части (индекс Б1.В.ОД.8).

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часа. Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (18 часов, том числе с МАО - 18 часов), самостоятельная работа студентов (90 часов). Дисциплина реализуется на 2 курсе в 4 семестре. Форма контроля по дисциплине - зачет.

Цели освоения дисциплины: сформировать у студентов терминологический фундамент, научить проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности и защиты информации, формирование целостного представления о сущности и понятии информационной безопасности, характеристике ее составляющих; месте информационной безопасности в системе национальной безопасности страны; источниках угроз информационной безопасности и мерах по их предотвращению; жизненных циклах конфиденциальной информации в процессе ее создания, обработки, передачи; современных средствах и способах обеспечения информационной безопасности.

Дисциплина формирует следующие компетенции:

- знание своих прав и обязанностей как гражданина своей страны, способностью использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии (ОК-9);

- понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);

- способность к организации работы малых коллективов исполнителей (ПК-19);

- способность оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-научно-технических отчетов, статей и докладов на научно-технических конференциях (ПК-26)

| **Код и формулировка компетенции** | **Этапы формирования компетенции** | |
|---|---|---|
| ОК-9, знание своих прав и обязанностей как гражданина своей страны, способностью использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии | знает | закономерности и этапы исторического процесса, основные исторические факты, даты, события и имена исторических деятелей России; основные события и процессы отечественной истории в контексте мировой истории |
| | умеет | критически воспринимать, анализировать и оценивать историческую информацию, факторы и механизмы исторических изменений |
| | владеет | навыками анализа причинно-следственных связей в развитии российского государства и общества; места человека в историческом процессе и политической организации общества; навыками уважительного и бережного отношения к историческому наследию и культурным традициям |
| ОПК-4, понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к | знает | сущность и значение информации в развитии современного информационного общества, основные требования к информационной безопасности, закон о защите государственной тайны |

| | | |
|---|---|---|
| информационной безопасности, в том числе защите государственной тайны | умеет | проектировать и реализовывать механизмы защиты информации |
| | владеет | навыками построения защищенных систем, формулирования требований к ним |
| ПК-19, способность к организации работы малых коллективов исполнителей | знает | методы работы в коллективе и способы организации работы малых коллективов исполнителей |
| | умеет | сотрудничать с коллегами по работе |
| | владеет | навыками организации работы малых коллективов исполнителей |
| ПК-26, способность оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-научно-технических отчетов, статей и докладов на научно-технических конференциях | знает | основные принципы построения отчетов, статей, докладов и презентаций |
| | умеет | оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно- технических конференциях |
| | владеет | современными программными средствами создания презентаций и текстовых документов |

Для формирования вышеуказанных компетенций в рамках дисциплины «Информационная безопасность и защита информации» применяются следующие методы активного обучения, интерактивного обучения: лекция-беседа, лекция-конференция, круглый стол (дискуссия).

## I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

**Трудоемкость теоретической части курса 36 час.**

**Раздел 1. Правовая основа информационной безопасности информационных систем. (8 час.)**

Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия.

Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ.

**Раздел 2. Информационная безопасность и методология защиты информации в корпоративных системах (8 час.)**

Классификация информации, циркулирующей в корпоративных системах. Информационные ресурсы и информационная инфраструктура сетей, как объекты защиты.

Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический.

**Раздел 3. Криптографические методы защиты информации (8 час.)**

Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89.

Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей.

Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами. Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция.

**Раздел 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей (6 час.)**

Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. Применение паролей и

биометрических средств аутентификации пользователей. Протоколы взаимной проверки подлинности объектов сети.

Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI.

Обеспечение целостности информации. Аутентификация информации и ЭЦП сообщений. Однонаправленные хэш-функции. Коды проверки подлинности информации.

Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов.

**Раздел 5. Архитектура и методы организации систем защиты информации. (6 час.)**

Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.

Специализированные программно-аппаратные средства защиты информации. Средства и механизмы обеспечения безопасности сетевого оборудования Cisco systems. Серверы доступа (брандмауэры) Cisco ASA5500. Средства обнаружения вторжений IDS 4200

## II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

### Практические занятия (18 час.)

**Занятие 1. Анализ рисков информационной безопасности ( 6 час.)**.

Ознакомиться с алгоритмами оценки риска информационной безопасности. Изучить ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий». Пользуясь одним

из методов (см. вариант) предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.

**Занятие 2. Обеспечение информационной безопасности в ведущих зарубежных странах (6 час.)**.

Ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах. Подготовить краткий доклад по заданному вопросу (см. вариант), используя доступные источники информации.

**Занятие 3. Построение концепции информационной безопасности предприятия (6 час.)**.

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры. Используя предложенные образцы, разработать концепцию информационной безопасности компании.

## Ш. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Информационная безопасность и защита информации» представлено в Приложении 1 и включает в себя: план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию; характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению; требования к представлению и оформлению результатов самостоятельной работы; критерии оценки выполнения самостоятельной работы.

## III. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

| № п/п | Контролируемые разделы/темы дисциплины | Коды и этапы формирования компетенций | | Оценочные средства - наименование | |
|---|---|---|---|---|---|
| | | | | текущий контроль | промежуточная аттестация |
| 1. | Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия. Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ. | ОК9<br>ОПК4<br>ПК19<br>ПК26 | знает | Устный опрос (собеседование) | Зачет |
| 2. | Классификация информации, циркулирующей в корпоративных системах ФЖТ. Информационные ресурсы и информационная инфраструктура сетей ФЖТ как объекты защиты. Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический. | ОК9<br>ОПК4<br>ПК19<br>ПК26 | знает | Устный опрос (собеседование) | зачет |
| | | | Умеет владеет | Индивидуальный проект | |
| 3. | Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. Средства антивирусной защиты. Классификация вирусов и средств защиты | ОК9<br>ОПК4<br>ПК19<br>ПК26 | знает | Устный опрос (собеседование) | зачет |
| | | | Умеет владеет | Индивидуальный проект | |

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования

компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

## V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Основная литература

| | название | Ссылка в ЭК НБ ДВФУ | Внешняя ссылка |
|---|---|---|---|
| 1 | Петров, С. В. Информационная безопасность [Электронный ресурс] : учебное пособие / С. В. Петров, П. А. Кисляков. — Электрон. текстовые данные. — Саратов : Ай Пи Ар Букс, 2015. — 326 c. — 978-5-906-17271-6. | http://lib.dvfu.ru:8080/lib/item?id=IPRbooks:IPRbooks-33857&theme=FEFU | http://www.iprbookshop.ru/33857.html. |
| 2 | Информационная безопасность предприятия : учебное пособие для вузов / Н. В. Гришина. Москва: Форум, 2015. 238 с | http://lib.dvfu.ru:8080/lib/item?id=chamo:795581&theme=FEFU | |
| 3 | Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: Учебное пособие. - СПб: СПбГУ ИТМО, 2009. - 84 с. | | http://www.ict.edu.ru/ft/006193/itmo378.pdf |
| 4 | Пилиди В.С. Криптография. Вводные главы: Учебное пособие. - Ростов-на-Дону: ЮФУ, 2009. - 110 с. | | http://www.ict.edu.ru/ft/006193/itmo378.pdf |
| 5 | Бетелин В.Б., Галатенко В.Б. Информационная (компьютерная) безопасность с точки зрения технологии программирования [Электронный ресурс] // Сайт "Cryptography.ru". | | http://www.cryptography.ru:8200/pubd/2001/10/23/0001161428/word5.pdf |

## Дополнительная литература

| | название | Ссылка в ЭК НБ ДВФУ | Внешняя ссылка |
|---|---|---|---|
| 1 | Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. - Москва: Наука, 2015. - 552 с. | | |
| 2 | Щеглов А.Ю. Антивирусная защита. Реализация на основе разграничительной политики доступа к ресурсам / Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы", 2008. - 35 с. | | http://www.ict.edu.ru/ft/005718/68364e2-st20.pdf |
| 3 | Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Основы информационно-психологической безопасности: моногр. . - М.: Международный гуманитарный фонд "Знание", 2014. - 416 с. | | |
| 4 | Информационная безопасность открытых систем. В 2 томах. Том 2. Средства защиты в сетях / С.В. Запечников и др. - Москва: СПб. [и др.] : Питер, 2014. - 560 с. | | |
| 5 | Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации | | |
| 6 | Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных | | |
| 7 | ГОСТ Р 50922-2006. Защита информации. Основные термины и определения | | |
| 8 | Авторский курс лекций «Информационная безопасность» на CD. | | |

**Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

1. http://www.securitylab.ru/ Секюрити лаб.
2. https://www.anti-malware.ru/ Информационно-аналитический центр, посвященный информационной безопасности. Anti-Malware проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие в дискуссиях на форуме..
3. https://geektimes.ru/hub/infosecurity/ Популярный хаб сайта geektimes.ru про информационную безопасность. Десятки тысяч просмотров статей, публикации о новинках индустрии и активное обсуждение в комментариях.
4. http://safe.cnews.ru/ Раздел новостного издания о высоких технологиях CNEWS, посвященный информационной безопасности. Публикуются новости и экспертные статьи.
5. http://www.iso27000.ru/ Интернет-портал ISO27000.RU – это площадка для общения специалистов по ИБ. Есть тематический каталог ссылок на ресурсы по информационной безопасности и защите информации..

## VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Дисциплина изучается в следующих организационных формах: лекционное занятие; крактическое занятие. самостоятельное изучение теоретического материала; самостоятельное выполнение индивидуального проекта; индивидуальные и групповые консультации.

Основной формой самостоятельной работы студента является изучение конспекта лекций, их дополнение рекомендованной литературой, выполнение проекта, а также активная работа на лабораторных и практических занятиях.

К прослушиванию лекции следует готовиться, для этого необходимо знать программу курса и рекомендованную литературу. Тогда в процессе лекции легче отделить главное от второстепенного, легче сориентироваться: что записать, что самостоятельно проработать, что является трудным для понимания, а что легко усвоить.

Контроль за выполнением самостоятельной работы студента производится в виде контроля каждого этапа работы, отраженного в документации и защиты проекта.

Студент должен планировать график самостоятельной работы по дисциплине и придерживаться его.

## VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Лекции и практические занятия проводятся с использованием проектора и внутренней системы портала ДВФУ.

| Наименование оборудованных помещений и помещений для самостоятельной работы | Перечень основного оборудования |
|---|---|
| Владивосток, о. Русский, п. Аякс д.10, корпус L, ауд. L 565 учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Мультимедийное оборудование: ЖК-панель 47", Full HD, LG M4716 CCBA - 1 шт. Парты и стулья |
| Владивосток, о. Русский, п. Аякс д.10, корпус L, ауд. L 507 специализированная лаборатория кафедры КС: Лаборатория | Стеллажи, столы и стулья |

| | |
|---|---|
| микропроцессорной техники | |
| Владивосток, о. Русский, п. Аякс д.10, корпус L, ауд. L 565<br>учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Мультимедийное оборудование:<br>ЖК-панель 47", Full HD, LG M4716 CCBA - 1 шт.<br>Парты и стулья |

*Приложение 1*

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
**«Дальневосточный федеральный университет»**
(ДВФУ)

# ШКОЛА ЕСТЕСТВЕННЫХ НАУК

## УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Информационная безопасность и защита информации
**Направление подготовки – 09.03.02 «Информационные системы и технологии»**
Профиль «Информационные системы и технологии в связи»

**Форма подготовки (очная)**

**Владивосток**
**2015**

Самостоятельная работа студентов состоит из подготовки к практическим занятиям, работы над рекомендованной литературой, решения задач и написания компьютерных графических программ. При организации самостоятельной работы преподаватель должен учитывать уровень подготовки каждого студента. Преподаватель дает каждому студенту индивидуальные и дифференцированные задания.

| п/п | Вид самостоятельной работы | Дата/сроки выполнения | Примерные нормы времени на выполнение | Форма контроля |
|---|---|---|---|---|
| 1 | Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия. Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ. | 1-4 неделя обучения | 14 часов | ПР-9 |
| 2 | Классификация информации, циркулирующей в корпоративных системах ФЖТ. Информационные ресурсы и информационная инфраструктура сетей ФЖТ как объекты защиты. Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический. | 5-8 неделя обучения | 16 часов | ПР-9 |
| 3 | Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. Средства антивирусной защиты. Классификация вирусов и средств защиты | 9-18 неделя обучения | 60 часов | ПР-9 |

**Задания для самостоятельного выполнения**

1. Знакомство с рекомендованной научной и научно-популярной литературой по проблемам информационной безопасности и защите информации.

2. Составление  глоссария терминов.

3. Знакомство с широко применяемыми программными продуктами защиты информации.

3. Решение задач по анализу угроз информационной безопансости.

4. Разработка программ  и концепций защиты ИБ предприятия.

## Рекомендации по работе с литературой

Для более эффективного освоения и усвоения материала рекомендуется ознакомиться с теоретическим материалом по той или иной теме до проведения лабораторного занятия. Всю учебную литературу желательно изучать «под конспект».

Цель написания конспекта по дисциплине – сформировать навыки по поиску, отбору, анализу и формулированию учебного материала.

Работу с теоретическим материалом по теме можно проводить по следующей схеме:

- название темы;

- цели и задачи изучения темы;

- основные вопросы темы;

- характеристика основных понятий и определений, необходимых для усвоения данной темы;

- краткие выводы, ориентирующие на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить.

При работе над конспектом обязательно выявляются и отмечаются трудные для самостоятельного изучения вопросы, с которыми уместно обратиться к преподавателю при посещении консультаций, либо в индивидуальном порядке.

## Подготовка к практическим занятиям

Подготовку к каждому практическому занятию каждый студент должен

начать с изучения теоретического материала и ознакомления с планом, который отражает содержание предложенной темы. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы по теме задания, правильном выполнении лабораторной работы.

В процессе занятия студент должен создать требуемый документ с помощью предлагаемого программного средства и выполнить требуемые в задании операции. Задание по лабораторной работе содержит методические указания по подготовке документа, который должен быть получен в результате выполнения работы. При подготовке к лабораторной работе следует их внимательно прочесть.

## Методические указания к составлению глоссария

Глоссарий охватывает термины в рамках тематики, затрагиваемой в лекциях. Глоссарий должен содержать не менее 50 терминов, они должны быть перечислены в алфавитном порядке, соблюдена нумерация. Глоссарий должен быть оформлен по принципу реферативной работы, в обязательном порядке присутствует титульный лист и нумерация страниц. Объем работы должен составлять 10-15 страниц. Тщательно проработанный глоссарий помогает избежать разночтений и помочь углубленному изучению материала. Глоссарии могут содержать отдельные слова, фразы, аббревиатуры, слоганы и даже целые предложения.

## Критерии оценки отчетов по проектам

– 100-86 баллов выставляется, если содержание и составляющие части соответствуют выданному заданию. Продемонстрировано владение навыками подготовки документа по теме. Фактических ошибок, связанных с пониманием структуры и содержания задания нет.

– 85-76 - баллов выставляется, если при выполнении задания допущено не более одной ошибки. Продемонстрировано владение навыками подготовки документа по теме. Фактических ошибок, связанных с пониманием структуры и содержания задания нет.

– 75-61 балл выставляется, если при выполнении задания допущено не более двух ошибок. Продемонстрировано знание и владение навыками подготовки документа по теме. Допущено не более 2 ошибок, связанных с пониманием структуры и содержания задания.

– 60-50 баллов - если структура и содержание задания не соответствуют требуемым.

*Приложение 2*

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
**«Дальневосточный федеральный университет»**
(ДВФУ)

**ШКОЛА ЕСТЕСТВЕННЫХ НАУК**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

Информационная безопасность и защита информации
**Направление подготовки – 09.03.02 «Информационные системы и технологии»**
Профиль «Информационные системы и технологии в связи»

**Форма подготовки (очная)**

**Владивосток**
**2015**

# Паспорт ФОС

| Код и формулировка компетенции | Этапы формирования компетенции | |
|---|---|---|
| ОК-9, знанием своих прав и обязанностей как гражданина своей страны, способностью использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии | Знает | закономерности и этапы исторического процесса, основные исторические факты, даты, события и имена исторических деятелей России; основные события и процессы отечественной истории в контексте мировой истории |
| | Умеет | критически воспринимать, анализировать и оценивать историческую информацию, факторы и механизмы исторических изменений |
| | Владеет | навыками анализа причинно-следственных связей в развитии российского государства и общества; места человека в историческом процессе и политической организации общества; навыками уважительного и бережного отношения к историческому наследию и культурным традициям |
| ОПК-4, пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны | Знает | сущность и значение информации в развитии современного информационного общества, основные требования к информационной безопасности, закон о защите государственной тайны |
| | Умеет | проектировать и реализовывать механизмы защиты информации |
| | Владеет | навыками построения защищенных систем, формулирования требований к ним |
| ПК-19, способностью к организации работы малых коллективов исполнителей | Знает | методы работы в коллективе и способы организации работы малых коллективов исполнителей |
| | Умеет | сотрудничать с коллегами по работе |
| | Владеет | навыками организации работы малых коллективов исполнителей |
| ПК-26, способностью оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-научно-технических отчетов, статей и докладов на научно-технических конференциях | знает | основные принципы построения отчетов, статей, докладов и презентаций |
| | умеет | оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях |
| | владеет | современными программными средствами создания презентаций и текстовых документов |

| № п/п | Контролируемые разделы/темы дисциплины | Коды и этапы формирования компетенций | | Оценочные средства - наименование | |
|---|---|---|---|---|---|
| | | | | текущий контроль | промежуточная аттестация |
| 1 | Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия. Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ. | ОК9 ОПК4 ПК19 ПК26 | знает | Устный опрос (собеседование) | Зачет |
| 2. | Структура и функционирование графического программного обеспечения | ОК9 ОПК4 ПК19 ПК26 | знает | Устный опрос (собеседование) | зачет |
| | | | Умеет владеет | Индивидуальный проект | |
| 3. | Методы и алгоритмы компьютерной графики | ОК9 ОПК4 ПК19 ПК26 | знает | Устный опрос (собеседование) | зачет |
| | | | Умеет владеет | Индивидуальный проект | |

## Шкала оценивания уровня сформированности компетенций

| **Код и формулировка компетенции** | **Этапы формирования компетенции** | | **критерии** | **показатели** |
|---|---|---|---|---|
| ОК-9, знанием своих прав и обязанностей как гражданина своей страны, способностью использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствовани ю и развитию общества на принципах | знает (пороговый уровень) | Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия. | Знание определений понятий и методов ИБ | Способность дать ответы на вопросы |
| | умеет (продвинут ый) | Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ. | Умение определять требуемые операции решения задач обеспечения ИБ | Способность продемонстрироват ь операции и дать к ним пояснения |
| | владеет (высокий) | Классификация информации, циркулирующей в корпоративных системах. Информационные ресурсы и информационная | Владение методами классификации | Способность классифицировать объекты защиты |

| | | | | |
|---|---|---|---|---|
| гуманизма, свободы и демократии | | инфраструктура сетей, как объекты защиты. | | |
| ОПК-4, пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны | знает (пороговый уровень) | Классификация и анализ угроз информационной безопасности корпоративным системам. | Знание угроз ИБ и методов их анализа | Способность дать ответы на вопросы |
| | умеет (продвинутый) | Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический | Умение программы безопасности для ИС | Наличие программ |
| | владеет (высокий) | Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический | Владение методами использования существующих инструментальных систем | Способность создавать системы защиты помощью существующих программных средств |
| ПК-19, способностью к организации работы малых коллективов исполнителей | знает (пороговый уровень) | методы работы в коллективе и способы организации работы малых коллективов исполнителей | Знание методов работы | Способность дать ответы на вопросы |
| | умеет (продвинутый) | сотрудничать с коллегами по работе | Умение создавать программы ИБ в коллективе | Наличие созданных программ |
| | владеет (высокий) | навыками организации работы малых коллективов исполнителей | Владение методами определения возможностей членов коллектива | Наличие созданных программ |

## Вопросы к зачету

1. Классификация угроз информации
2. Угрозы информации из внутренней среды.
3. Угроза информации от непреднамеренных ошибок пользователей
4. Угроза информации от краж и подлогов
5. Угрозы информации, исходящие из внешней среды
6. Классификация компьютерных вирусов

7. Классификация методов защиты информации
8. Правовой уровень защиты информации
9. Организационный уровень защиты информации
10. Политика безопасности
11. Работа с персоналом по защите информации
12. Физическая защита помещений и оборудования
13. Аппаратно-программный уровень защиты информации
14. Защита от несанкционированного доступа к информации
15. Идентификация и аутентификация. Основные понятия и определения
16. Перехватчики сканкодов клавиатуры. Основные понятия и определения
17. Токены, как средство защиты от НСД
18. Управление доступом к информации
19. Шифрование информации как средство защиты информации
20. Протоколирование и аудит
21. Защита информации с использованием экранов
22. Защита от компьютерных вирусов
23. Профилактика заражения компьютерными вирусами
24. Классификация антивирусных программ
25. Антивирусный центр AVP
26. Криптографический уровень защиты информации
27. Принципы шифрования информации
28. Концепция организации систем защиты информации
29. Этапы создания СЗИ
30. Виды обеспечения СЗИ
31. Модель эшелонированной обороны
32. Основные принципы разработки СЗИ
33. Методика организации СЗИ
34. Криптографический алгоритм DES.
35. Криптографический алгоритм RSA.

## Критерии выставления оценки студенту

| **Баллы** (рейтинговой оценки) | **Оценка зачета/ экзамена** (стандартная) | **Требования к сформированным компетенциям** |
|---|---|---|
| 86-100 | «зачтено»/ «отлично» | Оценка «отлично» (зачтено) выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. |
| 76-85 | «зачтено»/ «хорошо» | Оценка «хорошо» (зачтено) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. |
| 61-75 | «зачтено»/ «удовлетворительно» | Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. |
| 0-60 | «не зачтено»/ «неудовлетворительно» | Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. |

## Текущий контроль

Текущая аттестация студентов проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме защиты проекта и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

- степень усвоения теоретических знаний - оценивается в форме собеседования;
- уровень овладения практическими умениями и навыками –

оценивается в форме защиты проекта.

**Критерии оценки проектов**

- 100-86 баллов выставляется, если студент/группа точно определили содержание и составляющие части задания, умеют аргументированно отвечать на вопросы, связанные с заданием. Продемонстрировано знание и владение навыками самостоятельной исследовательской работы по теме. Фактических ошибок, связанных с пониманием проблемы, нет.
- 85-76 - баллов - работа студента/группы характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет.
- 75-61 балл – проведен достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимание базовых основ и теоретического обоснования выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы
- 60-50 баллов - если работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок смыслового содержание раскрываемой проблемы

**Шкала оценивания**

| | | |
|---|---|---|
| Менее 60 баллов | незачтено | неудовлетворительно |
| От 61 до 75 баллов | зачтено | удовлетворительно |
| От 76 до 85 баллов | зачтено | хорошо |
| От 86 до 100 балов | зачтено | отлично |

## Оценочные средства для текущей аттестации

### Тестовые задания для текущего контроля

1. Каковы возможные последствия (экономические) атак на информацию?

#5 а) Раскрытие коммерческой информации может привести к серьезным прямым убыткам на рынке.

б) Известие о краже большого объема информации обычно серьезно влияет на репутацию фирмы, приводя косвенно к потерям в объемах торговых операций

в) Фирмы-конкуренты могут воспользоваться кражей информации, если та осталась незамеченной, для того чтобы полностью разорить фирму, навязывая ей фиктивные либо заведомо убыточные сделки

г) Подмена информации как на этапе передачи, так и на этапе хранения в фирме может привести к огромным убыткам

д) Многократные успешные атаки на фирму, предоставляющую какой-либо вид информационных услуг, снижают доверие к фирме у клиентов, что сказывается на объеме доходов

#4 а) Раскрытие коммерческой информации может привести к серьезным прямым убыткам на рынке.

б) Известие о краже большого объема информации обычно серьезно влияет на репутацию фирмы, приводя косвенно к потерям в объемах торговых операций

в) Фирмы-конкуренты могут воспользоваться кражей информации, если та осталась незамеченной, для того чтобы полностью разорить фирму, навязывая ей фиктивные либо заведомо убыточные сделки

г) Подмена информации как на этапе передачи, так и на этапе хранения в фирме может привести к огромным убыткам

#3 а) Известие о краже большого объема информации обычно серьезно влияет на репутацию фирмы, приводя косвенно к потерям в объемах торговых операций

б) Фирмы-конкуренты могут воспользоваться кражей информации, если та осталась незамеченной, для того чтобы полностью разорить фирму, навязывая ей фиктивные либо заведомо убыточные сделки

в) Подмена информации как на этапе передачи, так и на этапе хранения в фирме может привести к огромным убыткам

#2 а) Раскрытие коммерческой информации может привести к небольшим убыткам на рынке.

б) Атаки на информационные ресурсы фирмы могут послужить своего рода рекламой для фирмы

#1 Атаки на информацию не приводят к существенным потерям на рынке.

2. Какими категориями обладает информация с точки зрения информационной безопасности?

#5 Информация обладает следующими категориями: конфиденциальность, целостность, аутентичность, апеллируемость.

#4 Информация обладает следующими категориями: конфиденциальность, целостность, аутентичность.

#3 Информация обладает следующими категориями: конфиденциальность, целостность.

#2 Информация обладает конфиденциальностью с точки зрения информационной безопасности.

#1 У информации нет категорий с точки зрения информационной безопасности.

3. Дайте определение конфиденциальности.

#5 конфиденциальность – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации.

#4 конфиденциальность – гарантия того, что конкретная информация доступна только определенному кругу лиц; нарушение этой категории называется хищением либо раскрытием информации.

#3 конфиденциальность – гарантия того, что конкретная информация доступна лицам, которым она необходима для работы; нарушение этой категории называется хищением либо раскрытием информации.

#2 конфиденциальность – гарантия того, что конкретная информация доступна всем сотрудникам организации и не доступна лицам не работающим в организации.

#1 конфиденциальность – гарантия того, что любая информация доступна всем сотрудникам организации и не доступна лицам не работающим в организации.

4. Дайте определение категории – целостность информации.

#5 целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения.

#4 целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения.

#3 целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть не было произведено изменений; нарушение этой категории называется фальсификацией.

#2 целостность – гарантия того, что информация существует в ее исходном виде, то есть даже если было произведено изменение, то оно незначительно.

#1 целостность – гарантия того, что информация, даже если было произведено изменение, существует в ее исходном виде.

5. Что такое аутентичность информации?

#5 аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения.

#4 аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории называется фальсификацией.

#3 аутентичность – гарантия того, что источником информации является ее автор.

#2 аутентичность – гарантия того, что у информации есть автор.

#1 аутентичность – гарантия того, что информация правильная.

6. Какие с точки зрения информационной безопасности существуют категории в отношении информационных систем?

#5 В отношении информационных систем применяются следующие категории: надежность, точность, контроль доступа, контролируемость, контроль идентификации, устойчивость к умышленным сбоям.

#4 В отношении информационных систем применяются следующие категории: надежность, контроль доступа, контролируемость, контроль идентификации, устойчивость к умышленным сбоям.

#3 В отношении информационных систем применяются следующие категории: надежность, контролируемость, устойчивость к умышленным сбоям.

#2 В отношении информационных систем применяются следующие категории: надежность, контролируемость.

#1 В отношении информационных систем применяются такие же категории как и для информации.

7. Дайте определение надежности и точности информационных систем.

#5 Надежность – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано, точность – гарантия точного и полного выполнения всех команд.

#4 Надежность – гарантия того, что система ведет себя в нормальном и внештатном режимах надежно, точность – гарантия точного и полного выполнения всех команд.

#3 Надежность – гарантия того, что система ведет себя в нормальном режиме так, как запланировано, точность – гарантия точного выполнения всех команд.

#2 надежность – гарантия того, что система работает без сбоев, точность – гарантия выполнения всех команд.

#1 надежность – гарантия того, что система работает, точность – гарантия выполнения команд.

8. Что за категории контроль доступа и контролируемость для информационных систем?

#5 Контроль доступа – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются; контролируемость – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса.

#4 Контроль доступа – гарантия того, что группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются; контролируемость – гарантия того, что может быть

произведена полноценная проверка любого компонента программного комплекса.

#3 Контроль доступа – гарантия того, что лица имеют различный доступ к информационным объектам, и эти ограничения доступа выполняются; контролируемость – гарантия того, что может быть произведена проверка программного комплекса.

#2 Контроль доступа – гарантия того, что существуют ограничения доступа к информации; контролируемость – гарантия того, что можно провести контроль системы.

#1 Контроль доступа – гарантия того, что можно вести ограничения доступа к информации; контролируемость – гарантия того, что ограничения можно контролировать.

9. Дайте определение категорий: контроль идентификации, устойчивость к умышленным сбоям.

#5 Контроль идентификации – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает. Устойчивость к умышленным сбоям – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

#4 Контроль идентификации – гарантия того, что пользователь, подключенный в данный момент к системе, является именно тем, за кого себя выдает. Устойчивость к умышленным сбоям – гарантия того, что при внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

#3 Контроль идентификации – гарантия того, что пользователь является именно тем, за кого себя выдает. Устойчивость к умышленным сбоям – гарантия того, что при внесении небольшого количества ошибок система будет вести себя так, как оговорено заранее.

#2 Контроль идентификации – гарантия того, что пользователь является именно тем, за кого себя выдает. Устойчивость к умышленным сбоям – гарантия того, что при внесении ошибок система будет вести себя так, как оговорено заранее.

#1 Контроль доступа – гарантия того, что можно вести ограничения доступа к информации; контролируемость – гарантия того, что ограничения можно контролировать.

10. Когда и кем были опубликованы и как они назывались первые наставления по информационной безопасности?

#5 В августе 1983 Министерством обороны США были в первые опубликованы «Критерии оценки надежных компьютерных систем», получившие название по цвету обложки «Оранжевая книга».

#4 В 1983 Министерством обороны США были в первые опубликованы «Критерии оценки надежных компьютерных систем», получившие название по цвету обложки «Оранжевая книга».

#3 В начале 80-х годов Министерством обороны США были опубликованы «Критерии оценки надежных компьютерных систем».

#2 В 80-х годах Министерство обороны США опубликовало наставления по информационной безопасности («Оранжевую книгу).

#1 В конце 80-х годов Министерство обороны США опубликовало наставления по информационной безопасности.

11. Как «Оранжевая книга» поясняет понятие безопасной системы?

#5 "Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, посредством соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию".

#4 "Оранжевая книга" поясняет понятие безопасной системы, которая "управляет доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию".

#3 "Оранжевая книга" поясняет понятие безопасной системы, которая "управляет доступом к информации, так что авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию".

#2 "Оранжевая книга" поясняет понятие безопасной системы, которая "управляет доступом к информации, так что все лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию".

#1 "Оранжевая книга" никак не поясняет понятие безопасной системы.

12. Как «Критерии оценки надежных компьютерных систем» определяют понятие надежная система?

#5 Надежная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

#4 Надежная система определяется как "система, использующая аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

#3 Надежная система определяется как "система, использующая программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей ".

#2 Надежная система определяется как "система, использующая все средства, чтобы обеспечить одновременную обработку информации группой пользователей ".

#1 Надежная система определяется как "система, позволяющая одновременно обрабатывать информацию группами пользователей ".

13. По каким критериям оценивается надежность систем?

#5 Надежность систем (степень доверия) оценивается по двум основным критериям: политика безопасности и гарантированность, но надо добавить и подотчетность (протоколирование).

#4 Надежность систем (степень доверия) оценивается политикой безопасности и гарантированностью.

#3 Надежность систем (степень доверия) оценивается политикой безопасности.

#2 Надежность систем (степень доверия) оценивается монитором обращений.

#1 Надежность систем (степень доверия) оценивается надежной вычислительной базой

14. Дайте определение политики безопасности.

#5 Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

#4 Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Чем надежнее система, тем строже должна быть политика

безопасности. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

#3 Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает и распространяет информацию. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

#2 Политика безопасности - набор правил и норм поведения работников организации, распространяющих информацию. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз со стороны персонала и выбор мер наказания.

#1 Политика безопасности - набор правил и норм поведения работников организации. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз со стороны персонала и выбор мер наказания.

15. Что такое гарантированность?

#5 Гарантированность - мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки (формальной или нет) общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты, надзирающим за самими защитниками.

#4 Гарантированность - мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность определяется проверкой общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности.

#3 Гарантированность - мера доверия, которая может быть оказана системе. Гарантированность определяется всей системой в целом. Гарантированность показывает, насколько корректны механизмы безопасности.

#2 Гарантированность – характеристика системы. Гарантированность определяется политикой безопасности. Гарантированность показывает, насколько важны механизмы безопасности.

#1 Гарантированность – характеристика системы. Гарантированность определяется механизмами безопасности.

16. Каковы основные элементы политики безопасности?

#5 Политика безопасности должна включать в себя по крайней мере следующие элементы: произвольное управление доступом; безопасность повторного использования объектов; метки безопасности; принудительное управление доступом.

#4 Политика безопасности должна включать следующие элементы: произвольное управление доступом; метки безопасности; принудительное управление доступом.

#3 Политика безопасности включает следующие элементы: произвольное управление доступом; принудительное управление доступом.

#2 Политика безопасности включает следующие элементы: управление доступом; метки безопасности.

#1 Политика безопасности включает ряд элементов, которым относится управление доступом.

17. Что такое произвольное управление доступом?

#5 Произвольное управление доступом - это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению

давать другим субъектам или отбирать у них права доступа к объекту. С концептуальной точки зрения текущее состояние прав доступа при произвольном управлении описывается матрицей, в строках которой перечислены субъекты, а в столбцах - объекты. В клетках, расположенных на пересечении строк и столбцов, записываются способы доступа, допустимые для субъекта по отношению к объекту - например, чтение, запись, выполнение, возможность передачи прав другим субъектам и т.п. Большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Главное его достоинство - гибкость, главные недостатки - рассредоточенность управления и сложность централизованного контроля, а также оторванность прав доступа от данных, что позволяет копировать секретную информацию в общедоступные файлы.

#4 Произвольное управление доступом - это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что владелец объекта может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту. С концептуальной точки зрения текущее состояние прав доступа при произвольном управлении описывается матрицей, в строках которой перечислены субъекты, а в столбцах - объекты.

#3 Произвольное управление доступом - это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что владелец объекта может по своему усмотрению давать другим пользователям или отбирать у них права доступа к объекту.

#2 Произвольное управление доступом - это метод доступа к объектам, основанный на учете пользователей. Произвольность управления состоит в том, что любой пользователь объекта может по своему усмотрению давать другим пользователям или отбирать у них права доступа к объекту.

#1 Произвольное управление доступом - это метод доступа к объектам, он состоит в том, что любой пользователь объекта может по своему усмотрению давать другим пользователям или отбирать у них права доступа к объекту.

18. Что такое безопасность повторного использования объектов?

#5 Безопасность повторного использования объектов - важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом. Поскольку информация о субъектах также представляет собой объект, необходимо позаботиться о безопасности "повторного использования субъектов". Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. Современные интеллектуальные периферийные устройства усложняют обеспечение безопасности повторного использования объектов, поэтому необходимо предпринять специальные меры, чтобы "вытолкнуть" данные оттуда.

#4 Безопасность повторного использования объектов - важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом, а также для интеллектуальных периферийных систем.

#3 Безопасность повторного использования объектов, предохраняет от случайного или преднамеренного извлечения информации из "мусора".

Безопасность повторного использования должна гарантироваться для всех устройств, входящих в вычислительную систему.

#2 Безопасность повторного использования объектов, предохраняет от случайного или преднамеренного извлечения информации из "мусора". Безопасность повторного использования должна гарантироваться уничтожением всех устройств, входящих в вычислительную систему, после вывода из эксплуатации.

#1 Безопасность повторного использования объектов, предохраняет извлечения информации из различных устройств. Безопасность повторного использования должна достигаться уничтожением всех устройств, входящих в вычислительную систему, после вывода из эксплуатации.

19. Дайте характеристику меток безопасности.

#5 Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень закрытости содержащейся в нем информации. Метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так совершенно секретно, секретно, конфиденциально, несекретно. Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные. В военном окружении каждая категория может соответствовать, например, определенному виду вооружений. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности.

#4 Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень закрытости содержащейся в нем информации. Метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности,

поддерживаемые системой, образуют упорядоченное множество. Категории образуют неупорядоченный набор. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности.

#3 Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество. Категории образуют неупорядоченный набор.

#2 Для реализации управления доступом необходимы метки безопасности. Метки безопасности повышают уровень секретности. Уровни секретности образуют упорядоченное множество.

#1 Для реализации произвольного управления доступом используются метки безопасности. Метки безопасности повышают уровень секретности, что способствуют лучшей защищенности системы. Уровни секретности образуют неупорядоченное множество.

20. Охарактеризуйте такой элемент политики безопасности, как принудительное управление доступом.

#5 Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может писать в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий). Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс

вполне возможен. Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

#4 Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. "Конфиденциальный" субъект может писать в секретные файлы, но не может - в несекретные (должны также выполняться ограничения на набор категорий). Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен. Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов. После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

#3 Принудительное управление доступом основано на сопоставлении меток безопасности. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. Например, "конфиденциальный" субъект может писать в секретные файлы, но не может - в несекретные. Ни при каких операциях уровень секретности информации не должен понижаться. Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов.

#2 Принудительное управление доступом основано на сопоставлении меток безопасности. Субъект может читать информацию из объекта, если

уровень секретности субъекта не выше, чем у объекта. Субъект может записывать информацию в объект, если метка безопасности объекта соответствует метке субъекта. Например, "конфиденциальный" субъект может писать в конфиденциальные файлы, но не может - в секретные. Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов.

#1 Принудительное управление доступом основано на сопоставлении меток безопасности. Субъект может читать информацию из объекта, если уровень секретности субъекта не выше, чем у объекта. Субъект может записывать информацию в объект, если метка безопасности объекта соответствует метке субъекта. Например, "конфиденциальный" субъект может писать в несекретные файлы, но не может - в секретные. Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов.

21. Каковы цели и средства подотчетности?

#5 Цель подотчетности - в каждый момент времени знать, кто (пользователь, процесс от имени пользователя) работает в системе и что он делает. Средства подотчетности делятся на три категории: идентификация и аутентификация, предоставление надежного пути, анализ регистрационной информации.

#4 Цель подотчетности - в каждый момент времени знать, кто работает в системе и что он делает. Средства подотчетности делятся на три категории: идентификация, предоставление надежного пути, анализ регистрационной информации.

#3 Цель подотчетности - знать, кто работает в системе и что он делает. Средства подотчетности делятся на категории: идентификация, анализ регистрационной информации.

#2 Цель подотчетности - фиксировать всю информацию о системе. Средства подотчетности делятся на категории: идентификация систем и процессов, анализ информации о событиях.

#1 Цель подотчетности - фиксировать всю информацию о событиях, приводящих к ошибкам в работе. Средства подотчетности делятся на категории: идентификация процессов, анализ информации о событиях.

22. Дайте характеристику идентификации и аутентификации.

#5 Идентификация и аутентификация - первый и важнейший программно-технический рубеж информационной безопасности. Если не составляет проблемы получить доступ к системе под любым именем, то другие механизмы безопасности, например, управление доступом, очевидно, теряют смысл. Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. Обычный способ идентификации - ввод имени пользователя при входе в систему. В свою очередь, система должна проверить подлинность личности пользователя, то есть что он является именно тем, за кого себя выдает. Стандартное средство проверки подлинности (аутентификации) - пароль, хотя в принципе могут использоваться также разного рода личные карточки, биометрические устройства (сканирование роговицы или отпечатков пальцев) или их комбинация. Без идентификации пользователей невозможно протоколирование их действий. В силу перечисленных причин проверке подлинности должно придаваться первостепенное значение. Декларируется, что пользователю должно быть позволено менять свой пароль, что пароли, как правило, должны быть машинно-сгенерированными (а не выбранными "вручную"), что пользователю должна предоставляться некоторая регистрационная информация (дата и время последнего входа в систему и т.п.).

#4 Идентификация и аутентификация - первый и важнейший программно-технический рубеж информационной безопасности. Каждый

пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. Обычный способ идентификации - ввод имени пользователя при входе в систему. При этом система должна проверить подлинность личности пользователя, то есть что он является именно тем, за кого себя выдает. Стандартное средство проверки подлинности (аутентификации) - пароль, хотя в принципе могут использоваться также разного рода личные карточки, биометрические устройства (сканирование роговицы или отпечатков пальцев) или их комбинация. Без идентификации пользователей невозможно протоколирование их действий. В силу перечисленных причин проверке подлинности должно придаваться первостепенное значение.

#3 Идентификация и аутентификация - важнейший программно-технический рубеж информационной безопасности. Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. Обычный способ идентификации - ввод имени пользователя при входе в систему. При этом система проверяет подлинность личности пользователя, то есть что он является именно тем, за кого себя выдает. Стандартное средство проверки подлинности (аутентификации) – пароль. Проверке подлинности должно придаваться первостепенное значение.

#2 Идентификация и аутентификация - важнейший программный рубеж информационной безопасности. Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя с помощью пароля. После чего ему разрешены все действия с информационными ресурсами системы.

#1 Идентификация и аутентификация - важнейший аппаратный рубеж информационной безопасности. Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен вести информацию о себе и подтвердить ее паролем. После чего ему разрешены все действия с информационными ресурсами системы.

23. Что такое гарантированность, какие виды гарантированности бывают?

#5 Гарантированность - это мера уверенности, с которой можно утверждать, что для проведения в жизнь сформулированной политики безопасности выбран подходящий набор средств, и что каждое из них правильно исполняет отведенную ему роль. В "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая - к методам построения и сопровождения.

#4 Гарантированность - это мера уверенности, с которой можно утверждать, что для проведения в жизнь политики безопасности имеется подходящий набор средств. В "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая - к методам построения и сопровождения.

#3 Гарантированность - это мера уверенности, с которой можно утверждать, что для выполнения политики безопасности имеется набор средств. Существует два вида гарантированности - операционная и технологическая. Операционная гарантированность относится к архитектурным аспектам системы, в то время как технологическая – соответствует методам сопровождения.

#2 Гарантированность - это мера уверенности, с которой можно утверждать набор средств соответствует стандартам системы защиты. Можно два вида гарантированности – системная (техническая) и технологическая. Системная гарантированность относится к реализационным аспектам компьютерной системы, в то время как технологическая - к методам построения систем.

#1 Гарантированность - это мера уверенности, с которой можно утверждать набор средств соответствует стандартам системы защиты. Можно два вида гарантированности –техническая и технологическая. Техническая гарантированность определяется производителем компьютерной системы, в то время как технологическая - к методам построения информационных систем.

24. Что включает в себя операционная гарантированность?

#5 Операционная гарантированность включает в себя проверку следующих элементов:

- Архитектура системы.
- Целостность системы.
- Анализ тайных каналов передачи информации.
- Надежное администрирование.
- Надежное восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.

#4 Операционная гарантированность включает в себя проверку следующих элементов:

- Архитектура и целостность системы.
- Анализ тайных каналов передачи информации.
- Надежное администрирование.
- Надежное восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.

#3 Операционная гарантированность включает в себя проверку следующих элементов:

- Архитектура и целостность системы.

- Анализ каналов передачи информации.
- Администрирование и восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.

#2 Операционная гарантированность включает в себя проверку следующих элементов:

- Архитектура и техническое обеспечение системы.
- Программное обеспечение системы.
- Каналы передачи информации.
- Восстановление после сбоев.
- Аппаратные средства защиты системы.
- Программные средства защиты системы.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.

#1 Операционная гарантированность включает в себя проверку следующих элементов:

- Техническое обеспечение системы.
- Программное обеспечение системы.
- Каналы передачи информации.
- Восстановление после сбоев.
- Аппаратные средства защиты системы.
- Программные средства защиты системы.

Операционная гарантированность - это способ убедиться в том, что техническое системы и ее реализация действительно хорошо защищают систему.

25. Что такое технологическая гарантированность?

#5 Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок". Технологическая гарантированность включает тестирование, средства конфигурационного управления, которые защищают систему в процессе проектирования, реализации и сопровождения, надежное распределение.

#4 Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок".

#3 Технологическая гарантированность охватывает цикл системы, от реализации и тестирования до продажи и сопровождения. Все действия выполняются в соответствии с жесткими стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок".

#2 Технологическая гарантированность затрагивает цикл системы, связанный продажей и сопровождением. Все действия выполняются в соответствии со стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок".

#1 Технологическая гарантированность определяется технологией разработки системы. Все действия выполняются в соответствии со стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок".

26. Сколько и какие классы безопасности согласно «Критериев» Министерства обороны США существует?

#5 "Критерии" Министерства обороны США открыли путь к ранжированию информационных систем по степени надежности. В

"Оранжевой книге" определяется четыре уровня безопасности (надежности) - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять требованиям, которые характерны для каждого класса.

#4 "Критерии" Министерства обороны США определяют четыре уровня безопасности (надежности) - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять определенным требованиям.

#3 "Критерии" Министерства обороны США определяют четыре уровня безопасности (надежности) - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, C3, B1, B2) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности - C1, C2, C3, B1, B2, A1. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять требованиям класса.

#2 "Критерии" Министерства обороны США определяют четыре уровня безопасности (надежности) - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Таким образом, всего имеется три класса безопасности - C, B, A. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять требованиям класса.

#1 "Критерии" Министерства обороны США определяют четыре уровня безопасности (надежности) - D, C, B и A. По мере перехода от уровня D к A к надежности систем предъявляются все более жесткие требования. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять требованиям класса.

27. Как распределяются требования к политике безопасности при переходе от класса классу?

#5 Политика безопасности в «младших» классах довольно быстро ужесточается, достигая пика к классу B1.

#4 Политика безопасности в «младших» классах довольно быстро ужесточается, достигая пика к классу B2.

#3 Политика безопасности в «младших» классах довольно быстро ужесточается, достигая пика к классу C3.

#2 Политика безопасности в «старших» классах довольно быстро ужесточается, достигая пика к классу B3.

#1 Политика безопасности в «старших» классах довольно быстро ужесточается, достигая пика к классу A1.

28. Как распределяются требования к гарантированности при переходе от класса классу?

#5 Меры гарантированности отнесены в основном в «старшие» классы, начиная с B2.

#4 Меры гарантированности отнесены в основном в «старшие» классы, начиная с B1.

#3 Меры гарантированности отнесены в основном в «старшие» классы, начиная с B3.

#2 Меры гарантированности отнесены в основном в «младшие» классы, начиная с C1 и достигая пика к классу B2.

#1 Меры гарантированности отнесены в основном в «младшие» классы, начиная с C1 и достигая пика к классу B1.

29. На кого и на какие системы в основном ориентированы «Критерии» Министерства обороны США?

#5 «Критерии» явно ориентированы на производителя и оценщика (производящего сертификацию систем), а не на покупателя систем. Они не дают ответ на вопрос, как безопасно строить систему, как наращивать отдельные компоненты и конфигурацию в целом. «Критерии» рассчитаны в основном на статичные, замкнутые системы, которые редки в коммерческой среде.

#4 «Критерии» явно ориентированы на производителя и оценщика, а не на покупателя систем. Они только частично дают ответ на вопрос, как безопасно строить систему, как наращивать отдельные компоненты и конфигурацию в целом. «Критерии» рассчитаны в основном на некоммерческие системы.

#3 «Критерии» явно ориентированы на производителя и оценщика, а не на покупателя систем. Они хотя и дают ответ на вопрос, как безопасно строить систему, как наращивать отдельные компоненты и конфигурацию в целом, но рассчитаны в основном на некоммерческие системы.

#2 Хотя «Критерии» ориентированы на производителя и оценщика, но и покупатель систем может найти ответ на вопрос, как безопасно строить систему, как наращивать отдельные компоненты и конфигурацию в целом.

#1 «Критерии» ориентированы как на производителя и оценщика, так и покупателя систем. В «Критериях» можно найти ответ на вопрос, как безопасно строить систему, как наращивать отдельные компоненты и конфигурацию в целом.

30. Европейские критерии оценки безопасности информационных систем.

#5 Следуя по пути интеграции, в 1991 года от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании были приняты согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC). Выгода от использования согласованных критериев очевидна для всех - и для производителей, и для потребителей, и для самих органов сертификации. Принципиально важной чертой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система. По Европейским Критериям организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации - оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных организацией условиях. Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к политике безопасности и к наличию защитных механизмов не являются составной частью Критериев. Хотя Критерии содержат в качестве

приложения описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем.

#4 В 1991 года от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании были приняты согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC). Согласованные критерии применимы и для производителей, и для потребителей, и для самих органов сертификации. Принципиально важной чертой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система. По Европейским Критериям организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации - оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных организацией условиях. Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к политике безопасности и к наличию защитных механизмов не являются составной частью Критериев.

#3 В начале 90-х годов от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании были приняты согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC). Согласованные критерии применимы как для производителей, так и для потребителей. Важной чертой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система. По Европейским Критериям организация сама формулирует и описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа

сертификации - оценить насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных организацией условиях. Европейские Критерии относятся к гарантированности безопасной работы системы.

#2 В начале 90-х годов европейские страны приняли свои согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC). Согласованные критерии применимы для потребителей. Важной чертой Европейских Критериев является наличие априорных требований к условиям, в которых должна работать информационная система. По Европейским Критериям организация сама или с помощью органа сертификации подбирает систему для условий, в которых должна она работать, с учетом возможных угроз безопасности и предоставляемых ею защитных функций. Европейские Критерии относятся к гарантированности безопасной работы системы.

#1 В начале 90-х годов европейские страны приняли свои согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC), основываясь на «Критериях» Министерства обороны США. Согласованные критерии применимы в основном для производителей. Важной чертой Европейских Критериев является наличие априорных требований к условиям, в которых должна работать информационная система. По Европейским Критериям организация сама или с помощью органа сертификации подбирает систему для условий, в которых должна она работать, с учетом возможных угроз безопасности и предоставляемых ею защитных функций. Европейские Критерии относятся к гарантированности безопасной работы системы.

31. Основные составляющие информационной безопасности согласно Европейским Критериям.

#5 Европейские Критерии рассматривают следующие составляющие информационной безопасности:

- конфиденциальность, то есть защиту от несанкционированного получения информации;

- целостность, то есть защиту от несанкционированного изменения информации;

- доступность, то есть защиту от несанкционированного удержания информации и ресурсов.

#4 Европейские Критерии рассматривают следующие составляющие информационной безопасности:

- конфиденциальность, то есть защиту информации;

- целостность, то есть защиту от изменения информации;

- доступность, то есть защиту от удержания информации и ресурсов.

#3 Европейские Критерии рассматривают следующие составляющие информационной безопасности:

- целостность, то есть защиту от изменения информации;

- доступность, то есть защиту от удержания информации и ресурсов.

#2 Европейские Критерии рассматривают следующие составляющие информационной безопасности:

- секретность данных;

- целостность баз данных;

- доступность ресурсов и баз данных.

#1 Европейские Критерии рассматривают следующие составляющие информационной безопасности:

- целостность баз данных;

- доступность ресурсов и баз данных.

32. Существуют ли различия в Европейских критериях между системами и продуктами, если да то в чем отличия?

#5 Да, отличия существуют. Система – это конкретная аппаратно-программная конфигурация, построенная с определенными целями и функционирующая в известном окружении. Продукт – это аппаратно-

программный «пакет», который можно купить и встроить в ту или иную систему.

#4 Да, отличия существуют. Система – это конкретная аппаратно-программная конфигурация, построенная с согласно определенным целям и функционирующая в известном окружении. Продукт – это программный «пакет», который можно купить и встроить в ту или иную систему.

#3 Да, отличия существуют. Система – это конкретная аппаратно-программная конфигурация, функционирующая в известном окружении. Продукт – это программный «пакет», который встроить в любую систему.

#2 Нет. Но по Европейским Критериям система – это конкретная аппаратно-программная конфигурация, функционирующая в известном окружении. Продукт – это программный «пакет», который встроить в любую систему.

#1 Нет. Европейским Критериям система и продукт – это конкретная аппаратно-программная конфигурация, функционирующая в известном окружении.

33. Что называют гарантированностью и от чего она зависит?

#5 Гарантированностью называют степень уверенности в наборе функций и механизмов безопасности. Она зависит от тщательности проведения оценки безопасности.

#4 Гарантированностью называют уверенность в наборе функций и механизмов безопасности. Она зависит от способа проведения оценки безопасности.

#3 Гарантированностью называют набор функций и механизмов безопасности. Она зависит от способа проведения оценки механизмов безопасности.

#2 Гарантированность - это уверенность в безопасной работе системы (пакета). Она зависит от способа реализации функций и механизмов безопасности.

#1 Гарантированность - это уверенность в безопасной работе системы. Она зависит от способа реализации механизмов безопасности.

34. Какие аспекты затрагивает гарантированность?

#5 Гарантированность затрагивает два аспекта – эффективность и корректность средств безопасности.

#4 Гарантированность затрагивает следующие аспекты: эффективность и корректность безопасности.

#3 Гарантированность затрагивает следующие аспекты: эффективность, корректность и функциональность безопасности системы.

#2 Гарантированность затрагивает следующие аспекты: функциональность и набор механизмов безопасности.

#1 Гарантированность затрагивает следующие аспекты: функции безопасности и набор механизмов безопасности.

35. Что определяет эффективность средств безопасности?

#5 При проверке эффективности анализируется соответствие между целями, которые сформулированы для объекта оценки, и имеющимся набором функций безопасности, а также способность механизмов защиты противостоять прямым атакам (мощность механизма).

#4 При проверке эффективности анализируется соответствие между целями защиты  и имеющимся набором функций безопасности, а также способность защиты противостоять прямым атакам.

#3 При проверке эффективности анализируется соответствие между защитой  и имеющимся набором функций безопасности, а также способность защиты противостоять атакам на информацию.

#2 Эффективность определяет соответствие между возможными атаками  и имеющимся набором механизмов защиты и функций безопасности.

#1 Эффективность определяет соответствие между атаками и имеющимся набором механизмов, защищающих конкретные устройства.

36. Сколько и какие градации мощности защитных механизмов определяют Европейские критерии.

#5 Европейские критерии определяют три градации мощности защитных механизмов – базовая, средняя и высокая.

#4 Европейские критерии определяют три градации мощности защитных механизмов – начальная, средняя и высокая.

#3 Европейские критерии определяют три градации мощности защитных механизмов – начальная, промежуточная и высокая.

#2 Европейские критерии определяют две градации мощности защитных механизмов – начальная и высокая.

#1 Европейские критерии определяют две градации мощности защитных механизмов – начальная и конечная.

37. Сколько уровней гарантированности корректности определяют Европейские критерии?

#5 Европейские критерии определяют семь возможных уровней гарантированности корректности (от E0 до E6 в порядке возрастания).

#4 Европейские критерии определяют семь возможных уровней гарантированности корректности.

#3 Европейские критерии определяют шесть возможных уровней гарантированности корректности (от E1 до E6).

#2 Европейские критерии определяют пять возможных уровней гарантированности корректности.

#1 Европейские критерии определяют восемь возможных уровней гарантированности.

38. Из чего складывается общая оценка безопасности системы?

#5 Общая оценка безопасности системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности.

#4 Общая оценка системы складывается из мощности механизмов безопасности и уровня гарантированности корректности.

#3 Общая оценка системы складывается из мощности механизмов безопасности и уровня гарантированности.

#2 Общая оценка системы складывается из максимальной мощности механизмов безопасности и уровня эффективности этих механизмов.

#1 Общая оценка системы складывается из максимальной мощности механизмов безопасности и эффективности этих механизмов противостоять атакам.

39. Какие разделы в спецификации функций безопасности Европейские Критерии рекомендуют выделит?

#5 Критерии рекомендуют выделять следующие разделы: идентификация и аутентификация; управление доступом; подотчетность; аудит; повторное использование объектов; точность информации; надежность обслуживания; обмен данными.

#4 Критерии рекомендуют выделять следующие разделы: идентификация; управление доступом; подотчетность и аудит; повторное использование объектов; точность информации; надежность обслуживания; обмен данными.

#3 Критерии рекомендуют выделять следующие разделы: идентификация; управление доступом; подотчетность и аудит; повторное использование объектов; точность информации; надежность обслуживания.

#2 Критерии рекомендуют выделять следующие разделы: идентификация; аудит; повторное использование объектов; точность информации; надежность обслуживания.

#1 Критерии рекомендуют выделять разделы, согласно американским наставлениям по безопасности: идентификация; протоколирование; аудит; повторное использование объектов; надежность обслуживания.

40. Что понимается под идентификацией и аутентификацией в Европейских критериях?

#5 Критерии понимают не только проверку подлинности пользователей в узком смысле, но и функции для регистрации новых пользователей и удаления старых, а также функции для генерации паролей и проверки аутентификационной информации, в том числе средства контроля целостности и ограничения числа повторных попыток аутентификации.

#4 Критерии понимают проверку подлинности пользователей в узком смысле, функции для регистрации новых пользователей и удаления старых, функции для генерации паролей и проверки аутентификационной информации, в том числе средства контроля целостности.

#3 Критерии понимают проверку подлинности пользователей, функции для регистрации пользователей, функции проверки аутентификационной информации, в том числе средства контроля целостности.

#2 Критерии понимают проверку подлинности пользователей в узком смысле, с добавкой функции регистрации и проверки аутентификационной информации.

#1 Критерии понимают проверку подлинности пользователей в узком смысле (пароль и логин).

41. Как трактуются в Европейских критериях средства управления доступом?

#5 Критерии трактуют управления доступом достаточно широко. В этот раздел, помимо известных по американским критериям функций, попадают функции, которые обеспечивают временное ограничение доступа (для поддержания целостности), а также функции для управления

распространением прав доступа и для контроля за получением информации путем логического вывода и агрегирования данных.

#4 Критерии трактуют управления доступом широко. В этот раздел попадают все известные по американским критериям функции, а также функции для управления распространением прав доступа и для контроля за получением информации путем логического вывода и агрегирования данных.

#3 Критерии трактуют управления доступом широко. В этот раздел попадают все известные по американским критериям функции, а также ряд функций для управления правами доступа и для контроля за информацией.

#2 Критерии трактуют управления доступом широко. В этот раздел попадают все известные по американским критериям функции, а также ряд функций для контроля за пользователями, в частности их паролями.

#1 Критерии трактуют управления доступом также, как и американские критерии.

42. Что в Европейских критериях понимается под точностью информации?

#5 Под точностью в Критериях понимается поддержание определенного соответствия между различными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникаций).

#4 Под точностью в Критериях понимается поддержание определенного соответствия между различными частями данных и обеспечение неизменности данных при передаче между процессами.

#3 Под точностью в Критериях понимается поддержание связей между различными частями данных и обеспечение неизменности данных.

#2 Под точностью в Критериях понимается поддержание связей между различными данными и обеспечение доступности данных.

#1 Под точностью в Критериях понимается поддержание связей между различной информацией и обеспечение доступности информации для пользователей.

43. Как специфицируются функции безопасности в Европейских критериях?

#5 Набор функций безопасности специфицируется с использованием ссылок на определенные классы функциональности. Классов функциональности в Европейских критериях их десять, причем пять из них соответствуют классам безопасности в «Оранжевой книге» (F-C1, F-C2, F-B1, F-B2, F-B2) и пять новых (F-IN, F-AV, F-DI, F-DC, F-DX).

#4 Набор функций безопасности специфицируется с использованием ссылок на определенные классы функциональности. Классов функциональности в Европейских критериях их десять, причем пять из них соответствуют классам безопасности в «Оранжевой книге» и пять новых.

#3 Набор функций безопасности специфицируется с использованием ссылок на определенные классы функциональности, в Европейских критериях их десять, пять новых.

#2 Набор функций безопасности специфицируется с использованием ссылок на определенные классы функциональности. В Европейских критериях их девять.

#1 Набор функций безопасности специфицируется с использованием ссылок на определенные классы функциональности. В Европейских критериях их семь.

44. Какие вопросы рассматриваются для получения гарантий эффективности средств безопасности?

#5 Для получения гарантий эффективности средств безопасности рассматриваются следующие вопросы: соответствие набора функций безопасности провозглашенным целям, то есть их пригодность для

противодействия угрозам, перечисленным в описании объекта оценки; взаимная согласованность различных функций и механизмов безопасности; способность механизмов безопасности противостоять прямым атакам; возможность практического использования слабостей в архитектуре объекта оценки, то есть наличие способов отключения, обхода, повреждения и обмана функций безопасности; возможность небезопасного конфигурирования или использования объекта оценки при условии, что администраторы и/или пользователи имеют основание считать ситуацию безопасной; возможность практического использования слабостей в функционировании объекта оценки.

#4 Для получения гарантий эффективности средств безопасности рассматриваются следующие вопросы: соответствие набора функций безопасности провозглашенным целям, то есть их пригодность для противодействия угрозам, перечисленным в описании объекта оценки; взаимная согласованность различных функций и механизмов безопасности; способность механизмов безопасности противостоять прямым атакам; возможность практического использования слабостей в архитектуре объекта оценки, то есть наличие способов отключения, обхода, повреждения и обмана функций безопасности; возможность небезопасного конфигурирования или использования объекта оценки при условии, что администраторы и/или пользователи имеют основание считать ситуацию безопасной.

#3 Для получения гарантий эффективности средств безопасности рассматриваются следующие вопросы: соответствие набора функций безопасности провозглашенным целям; взаимная согласованность различных функций и механизмов безопасности; способность механизмов безопасности противостоять прямым атакам; возможность практического использования слабостей в архитектуре объекта оценки, то есть наличие способов отключения, обхода, повреждения и обмана функций безопасности.

#2 Для получения гарантий эффективности средств безопасности рассматриваются следующие вопросы: соответствие функций безопасности системе защиты объекта оценки; взаимная поддержка различных функций и механизмов безопасности; способность механизмов безопасности защищаться от прямых атак; возможность использования слабостей в объекте оценки; возможность безопасного конфигурирования или использования объекта оценки; возможность использования защиты в функционировании объекта оценки.

#1 Для получения гарантий эффективности средств безопасности рассматриваются следующие вопросы: соответствие функций безопасности системе защиты объекта оценки от прямого проникновения; взаимная поддержка различных защитных функций и механизмов безопасности; способность механизмов безопасности защищаться от прямого доступа (проникновения); возможность использования слабостей в объекте оценки; возможность использования защиты в функционировании объекта оценки.

45. Как Европейские Критерии определяют базовую мощность средств защиты?

#5 Мощность считается базовой, если механизм способен противостоять отдельным случайным атакам. При этом защищенность системы не может быть выше самого слабого из критически важных механизмов.

#4 Мощность считается базовой, если механизм способен противостоять отдельным атакам. При этом защищенность системы не может быть выше самого слабого из критически важных механизмов.

#3 Мощность считается базовой, если механизм способен противостоять случайным атакам. При этом защищенность системы не может быть выше самого слабого из механизмов.

#2 Мощность считается базовой, если механизм способен противостоять атакам. При этом защищенность системы может быть выше самого слабого из механизмов защиты.

#1 Мощность считается базовой, если механизм не способен противостоять случайным атакам. При этом защищенность системы может быть выше самого слабого из механизмов защиты.

46. Как Европейские Критерии определяют среднюю мощность средств защиты?

#5 Мощность считается средней, если механизм способен противостоять злоумышленникам с ограниченными ресурсами и возможностями. При этом защищенность системы не может быть выше самого слабого из критически важных механизмов.

#4 Мощность считается средней, если механизм способен противостоять отдельным злоумышленникам с ограниченными возможностями. При этом защищенность системы не может быть выше самого слабого из критически важных механизмов.

#3 Мощность считается средней, если механизм способен противостоять отдельным злоумышленникам. При этом защищенность системы не может быть выше самого слабого из критически важных механизмов.

#2 Мощность считается средней, если механизм способен противостоять случайным атакам и ограниченному числу злоумышленников. При этом защищенность системы может быть выше самого слабого из критически важных механизмов.

#1 Мощность считается средней, если механизм способен противостоять случайным атакам злоумышленников. При этом защищенность системы может быть выше самого слабого из критически важных механизмов.

47. Как Европейские Критерии определяют высокую мощность средств защиты?

#5 Мощность считается высокой, если механизм может быть преодолен только злоумышленником с высокой квалификацией, набор возможностей и ресурсов которого выходит за пределы практичности.

#4 Мощность считается высокой, если механизм может быть преодолен только злоумышленником с достаточной квалификацией, соответствующий набор ресурсов которого выходит за пределы практичности.

#3 Мощность считается высокой, если механизм может быть преодолен только квалифицированным злоумышленником, соответствующий набор ресурсов которого значительный, чтобы преодолеть защиту.

#2 Мощность считается высокой, если механизм способен противостоять случайным атакам и неограниченному числу квалифицированных злоумышленников.

#1 Мощность считается высокой, если механизм способен противостоять случайным атакам квалифицированных злоумышленников.

48. По каким критериям оценивается гарантированность корректности средств безопасности?

#5 При проверке корректности объекта оценки применяются две группы критериев. Первая группа относится к конструированию и разработке системы или продукта, вторая - к эксплуатации. Оцениваются следующие аспекты: процесс разработки; среда разработки; эксплуатационная документация; операционное окружение.

#4 При проверке корректности объекта оценки применяются две группы критериев. Первая группа относится к конструированию и разработке системы или продукта, вторая - к эксплуатации. Оцениваются следующие аспекты: процесс и среда разработки; эксплуатационная документация.

#3 При проверке корректности объекта оценки применяются две группы критериев. Первая группа относится к конструированию и разработке системы или продукта, вторая - к эксплуатации.

#2 При проверке корректности объекта оценки рассматриваются следующие критерии: процесс разработки (кто, что разрабатывал) и эксплуатационная документация.

#1 При проверке корректности объекта оценки рассматриваются следующие критерии: процесс разработки защитных механизмов и руководство для пользователя (документация).

49. Сколько уровней корректности определяют Европейские критерии?

#5 Уровни корректности от E1 до E6 выстроены по нарастанию требований к тщательности оценки. Так, на уровне E1 анализируется лишь общая архитектура объекта - вся остальная уверенность может быть следствием функционального тестирования. На уровне E3 к анализу привлекаются исходные тексты программ и схемы аппаратуры. На уровне E6 требуется формальное описание функций безопасности, общей архитектуры, а также модели политики безопасности. Распределение требований по уровням гарантированности корректности в Европейских Критериях соответствует аналогичному распределению для классов безопасности C1 - A1 из "Оранжевой книги".

#4 Уровни корректности от E1 до E6 выстроены по нарастанию требований к тщательности оценки. Так, на уровне E1 анализируется лишь общая архитектура объекта - вся остальная уверенность может быть следствием функционального тестирования. На уровне E6 требуется формальное описание функций безопасности, общей архитектуры, а также модели политики безопасности.

#3 Уровни корректности от E1 до E6 выстроены по нарастанию требований к тщательности оценки. На самом высоком уровне E6 требуется

формальное описание функций безопасности, общей архитектуры, а также модели политики безопасности.

#2 Уровни корректности от E1 до E6 выстроены по убыванию требований к тщательности оценки.

#1 Уровни корректности от E1 до E6 выстроены по убыванию требований к тщательности оценки. На самом высоком уровне E1 требуется формальное описание функций безопасности, общей архитектуры, а также модели политики безопасности.

**Примеры вариантов тестовых заданий с ответами**

1 вариант

| | Вопрос | Ответ |
|---|---|---|
| | **Распространение поддельных сообщений от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:**<br>а) спам;<br>б) фишинг;<br>в) вирусная атака | б) |
| | **Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:**<br>а) активный перехват;<br>б) пассивный перехват;<br>в) аудиоперехват;<br>г) видеоперехват; | б) |
| | **Криптографические средства – это…**<br>а) средства специальные математические и алгоритмические средства защиты информации, | а) |

| | | |
|---|---|---|
| | передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования<br>б) специальные программы и системы защиты информации в информационных системах различного назначения<br>в) механизм, позволяющий получить новый класс на основе существующего | |

2 вариант

| | Вопрос | Ответ |
|---|---|---|
| | **Криптография необходима для реализации следующих сервисов безопасности:**<br>а) идентификация;<br>б) экранирование;<br>в) аутентификация | в) |
| | **Цифровой сертификат содержит:**<br>а) открытый ключ пользователя;<br>б) секретный ключ пользователя;<br>в) имя пользователя. | а) |
| | **Экранирование на сетевом и транспортном уровнях может обеспечить:**<br>а) разграничение доступа по сетевым адресам;<br>б) выборочное выполнение команд прикладного протокола;<br>в) контроль объема данных, переданных по TCP-соединению. | а) |

## ОБЩИЕ УКАЗАНИЯ

Для выполнения работы необходимо:

- изучить методические указания и рекомендуемую литературу;
- определить свой вариант задания;
- изучить заданные алгоритмы шифрования;
- зашифровать свою фамилию и полное имя методом гаммирования и по алгоритму RSA;
- выполнить проверку путем дешифрования шифротекста.

В работе должны быть выполнены все пункты задания, которое приводится в начале работы. Работы, не соответствующие указанным требованиям, не рассматриваются.

## ЗАДАНИЕ

Работа состоит из двух задач.

## ЗАДАЧА 1

Зашифровать фамилию и полное имя студента методом гаммирования. Под гаммированием понимают процесс наложения по определенному закону (чаще всего с использованием операции сложения по модулю 2) гаммы шифра на открытые данные. Гамма шифра – это псевдослучайная последовательность целых чисел, для генерации которых наиболее часто применяется так называемый линейный конгруэнтный генератор. Закон функционирования такого генератора описывается соотношением:

$$T_i = (T_{i-1} \cdot A + C) \bmod M \qquad (1)$$

где $T_i$ – текущее число последовательности; $T_{i-1}$ - предыдущее число последовательности; A, C и M – константы; M – модуль; A – множитель; C – приращение; $T_0$ – порождающее число.

Текущее псевдослучайное число $T_i$ получают из предыдущего числа $T_{i-1}$ умножением его на коэффициент A, сложением с приращением C и вычислением целочисленного остатка от деления на модуль M. Данное уравнение генерирует псевдослучайные числа с периодом повторения,

который зависит от выбираемых значений параметров A, C и M. Значение модуля M берется равным $2^n$, либо равным простому числу, например $M = 2^{31} - 1$. Приращение C должно быть взаимно простым с M, коэффициент A должен быть нечетным числом.

Вариант задания определяется в соответствии с табл. 1.

Таблица 1

| Константа | Значение |
|---|---|
| $T_0$ | 7 |
| A | 9 |
| C | Сумма двух последних цифр шифра |
| M | 64 |

Шифрование текста методом гаммирования рекомендуется выполнять в следующей последовательности:

1. Определить константы шифрования по табл. 1.

2. Каждой букве шифруемого текста поставить в соответствие десятичное число по табл. 2.

Таблица 2

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | | | | | | | | | | | |
| 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | |

2. Сгенерировать гамму шифра в соответствии с выражением (1).

3. Полученные числа (шифруемый текст и гамма шифра) перевести в двоичный. Замечание. Каждое число представляется байтом.

4. Наложить гамму шифра на шифруемый текст по формуле (2):

$$Ш_i = C_i \oplus T_i, \qquad (2)$$

где $Ш_i - i$ - ый символ шифрограммы, представленный в двоичном коде; $C_i - i$ - ый символ исходного текста, представленный в двоичном коде.

5. Полученную шифрограмму перевести в десятичный код и по табл. 2 получить текстовую форму шифрограммы. Замечание. В процессе выполнения операции сложение по модулю 2 могут получиться числа

больше 32. В этом случае рекомендуется выполнить операцию $\mathrm{mod}\,32$. Однако при дешифровке необходимо использовать исходное число.

6. Выполнить проверку шифрования путем наложения гаммы шифра на шифрограмму.

## ЗАДАЧА 2

Зашифровать фамилию и полное имя студента по алгоритму RSA. Порождающие числа выбрать в соответствии с табл. 3. Причем число $p$ выбирается по последней цифре шифра, а число $q$ – по предпоследней цифре.

Таблица 3

| Цифра | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $p$ | | 1 | 3 | 7 | 9 | 3 | 9 | 9 | 7 | 3 |
| $q$ | 3 | 9 | 9 | | 3 | 1 | 9 | 1 | 3 | 9 |

Замечание. Если числа $p$ и $q$ совпадают, то следует взять другое большее простое число.

Шифрование текста по алгоритму RSA рекомендуется выполнять в следующей последовательности:

1. Определить порождающие числа по табл. 3.

2. Каждой букве шифруемого текста поставить в соответствие десятичное число по табл. 2.

3. Вычислить произведение порождающих чисел $N = p \cdot q$.

4. Вычислить функцию Эйлера по формуле:

$$\varphi(n) = (p-1)\cdot(q-1)$$

5. Выбрать открытый ключ шифрования $K_{OTK}$, который должен удовлетворять следующим неравенствам:

$$1 < K_{OTK} < \varphi(n);$$
$$НОД(K_{OTK},\ \varphi(n)) \equiv 1$$

Значение $K_{OTK}$ выбирается произвольным образом из указанного диапазона чисел, а наибольший общий делитель (НОД) $K_{OTK}$ и функции Эйлера должен быть равен 1, т.е. эти два числа должны быть взаимно простыми. Так как порождающие числа с точки зрения криптографии ничтожно малы, то рекомендуется соблюдать два дополнительных условия: $K_{OTK} \neq p,\ K_{OTK} \neq q$.

6. Вычислить секретный ключ $K_{CEK}$ по формуле:

$$K_{CEK} = K_{OTK}^{(\varphi(n)-1)} \bmod \varphi(n)$$

При вычислении $K_{CEK}$ рекомендуется выполнить ряд последовательных умножений, выполняя каждый раз приведение по модулю. Например, необходимо вычислить 25 степень некоторого числа *a* по модулю *n*: $a^{25} \bmod n$. Представим степень 25 в виде целых степеней 2:

$$25 = 2^4 + 2^3 + 2^0.$$

Таким образом, нам необходимо вычислить 8 и 16 степени числа *a*. Для вычисления 8 степени воспользуемся выражением:

$$((a^2 \bmod n)^2 \bmod n)^2 \bmod n.$$

Для вычисления 16 степени, полученное на предыдущем шаге число необходимо возвести в квадрат и привести его по модулю.

7. Зашифровать исходный текст по формуле:

$$Ш_i = C_i^{K_{OTK}} \bmod N,$$

где $Ш_i - i$ - ый символ шифрограммы, представленный в десятичном коде; $C_i - i$ - ый символ исходного текста, представленный в десятичном коде.

8. Выполнить проверку, дешифровав шифрограмму по формуле:

$$Ш_i = C_i^{K_{CEK}} \bmod N.$$