**МИНОБРНАУКИ РОССИИ**

**Ярославский государственный университет им. П.Г. Демидова**

Кафедра компьютерных сетей

УТВЕРЖДАЮ

Декан факультета ИВТ



Д.Ю. Чалый

«\_22\_» мая 2024 г.

Рабочая программа дисциплины

«Информационная безопасность»

Направление подготовки

09.03.03 Прикладная информатика

**Направленность (профиль)**

«Информационные технологии в цифровой экономике»

Квалификация выпускника

Бакалавр

Форма обучения

очная

Программа рассмотрена на заседании кафедры

от 22 апреля 2024 г.,

протокол № 8

Программа одобрена НМК факультета ИВТ

протокол № 6 от

26 апреля 2024 г.

Ярославль

1. Цели освоения дисциплины

Целями дисциплины «Информационная безопасность» являются:

* освоение теоретических основ современных методов применяемых при решении задачи информационной безопасности;
* формирование конкретных практических навыков информационной безопасно- стив компьютерных технологиях.

1. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы.

Для освоения данной дисциплиной студенты должны обладать знаниями по матема- тике и информатике в объеме школьной программы, проявлять настойчивость, целе- устремленность и инициативу в процессе обучения. Для программной реализации алго- ритмов студенты должны иметь понятие об одном из языков программирования.

Полученные в рамках дисциплины знания необходимы для развития алгоритмиче- ского мышления, развития навыков решения сложных задач.

1. Планируемые результаты обучения по дисциплине, соотнесенные с пла- нируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

|  |  |  |
| --- | --- | --- |
| **Формируемая компе- тенция**  **(код и формулировка)** | **Индикатор достижения компетенции**  **(код и формулировка)** | **Перечень планируемых результатов обучения** |
| **Общепрофессиональные компетенции** | | |
| ОПК-3. Способен решать стандартные задачи профессио- нальной деятельности на основе информаци- онной и биб- лиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ОПК-3.1 демонстриру- ет навыки использова- ния научных и образо- вательных ресурсов сети интернет для раз- работки программ и программной докумен- тации с учетом требо- вания информационной безопасности | Знать:   * некоторые криптографические алго- ритмы; * некоторые хэш функции.   Уметь:   * реализовывать некоторые криптографи- ческие алгоритмы   Владеть навыками:   * вычислять хэш значение; * создавать ЭЦП. |
|  | ОПК-3.2 демонстрирует навыки использования основных методов передачи, обработки и хранения информации  ОПК-3.3 способен рационально выбрать программный продукт в зависимости от решения поставленной задачи | Знать:   * юридические вопросы информационной безопасности * о каналах утечки информации, их классификация.   Уметь:   * уметь выполнять передачу или генера- цию ключей. * реализовывать некоторые криптографи- ческие алгоритмы |
|  |  | Владеть навыками:   * построения модели информационной |

|  |  |  |
| --- | --- | --- |
|  | ОПК-3.4-демонстрирует умение оставлять, научные обзоры, рефераты и библиографии по тематике научных исследований | безопасности. |

1. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5зач.ед., 180акад.час.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Темы (разделы) дисциплины, их содержание** | **Семестр** | **Виды учебных занятий, включая самостоятельную работу студентов,**  **и их трудоемкость**  **(в академических часах)** | | | | | | **Формы текущего контроля успеваемо- сти**  **Форма промежуточ- ной аттестации (по семестрам)** |
|  |  |  | **Контактная работа** | | | | |  |  |
|  |  |  | лекции | практические | лабораторные | консультации | аттестационные испытания | самостоятельная работа |  |
| 1. | Определение безопасно- сти. | 7 | 1 | 1 |  |  |  | 5 |  |
| 2. | Каналы утечки информации, их классификация. | 7 | 2 | 2 |  |  |  | 5 |  |
| 3. | Модели информацион- ной безопасности. | 7 | 2 | 2 |  | 1 |  | 5 | Самостоятельная работа |
| 4. | Аутентикация, авториза- ция, пароли. | 7 | 2 | 2 |  | 1 |  | 5,7 | Самостоятельная работа |
| 5. | Асимметричные шифры. Электронные цифровые подписи | 7 | 6 | 6 |  | 1 |  | 8 | Самостоятельная работа |
| 6. | Безопасность программ- ного обеспечения | 7 | 2 | 2 |  |  |  | 2 | Контрольная работа  №1 |
| 7. | Стандарты и специфика- ции в области информа- ционной безопасности. | 7 | 2 | 2 |  |  |  | 2 |  |
|  | *в том числе с ЭО и ДОТ* |  |  |  |  |  |  | *2* | *2*Тест для самопроверки по результатам освоения дисциплины  *ЭУК в LMS Moodle* |
|  | **Всего за 7 семестр 72 часов** |  | **0** | **0** |  | **3** | **0,3** | **0** | **Зачет** |
| 8. | Шифрование. Симметричные шифры. | 8 | 2 | 14 |  | 2 |  | 13 | Самостоятельная работа |
| 9. | Юридические вопросы информационной без- опасности | 8 | 2 |  |  |  |  |  |  |
| 10. | Хэш-функции | 8 | 2 | 7 |  | 1 |  | 9 | Самостоятельная |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  | работа |
| 11. | Поточные шифры | 8 | 6 | 3 |  | 1 |  | 8 | Контрольная работа  №2 |
|  | *в том числе с ЭО и ДОТ* |  |  |  |  |  |  | *2* | *2*Тест для самопроверки по результатам освоения дисциплины  *ЭУК в LMS Moodle* |
|  |  |  |  |  |  | **2** | **0,5** | **33,5** | **Экзамен** |
|  | **Всего за 8 семестр**  **108 часов** |  | **0** | **0** |  | **6** | **0,5** | **65,5** |  |
|  | **Итого** |  | **29** | **41** |  |  |  | **66,7** |  |

**Содержание разделов дисциплины: Раздел 1**. Определение безопасности.

Определение информации, данных, знаний. Определение безопасности. Несанкци- онированный доступ. Информационные системы. Доступность, целостность, конфиденци- альность. Основные понятия об угрозах.

**Раздел 2**. Каналы утечки информации, их классификация.

Каналы утечки информации технических средств обработки, хранения и передачи информации. Каналы утечки речевой информации. Каналы утечки информации при её пе- редаче по каналам связи. Технические каналы утечки видовой информации. Каналы утеч- ки информации, создаваемые атаками извне и внутрикорпоративных систем ИКТ

**Раздел 3**. Модели защиты информации.

Модели разграничения доступа по принципу предоставления прав. Модели дис- кретного доступа. Вероятностные модели. Информационные модели. Модель мандатного доступа. Модель Бела-Лападулы, игровая модель. Матрица доступов.

**Раздел 4**. Аутентикация, авторизация, пароли.

Аутентикация, авторизация, пароли, токены, "рукопожатие". Протоколы аутен- тификации без передачи секретной информации, одноразовые ключи. Доказательство с нулевым знанием.

**Раздел 5**. Асимметричные шифры. Электронные цифровые подписи.

Асимметричные шифры, шифры с открытым ключом.Электронные цифровые подписи. Трудоемкость дешифрования. Рюкзачная криптосистема. Алгоритм RSA. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Алгоритм Эль-Гамаля. Алгоритм Рабина.

**Раздел 6**. Безопасность программного обеспечения.

Введение в защиту ПО. Угрозы безопасности ПО. Примеры уязвимостей ПО. Раз- рушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО. Компьютерные вирусы и антивирусные программы.

**Раздел 7**.Стандарты и спецификации в области информационной безопасности. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оце-

ночный стандарт. Информационная безопасность распределенных систем. Рекомендации X.800

**Раздел 8**. Шифрование. Cимметричные шифры.

Шифрование. Терминология шифрования. Трудоемкость дешифрования. Cиммет- ричные шифры. Рюкзачная криптосистема. Схема Фейстеля,SP-сеть.Режимы шифрования, гаммирование. Алгоритмы AES, Гост28147-89, DES, Serpent, Mars

**Раздел 9**. Юридические вопросы информационной безопасности

Понятие о законодательном уровне информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Закон «Об информации, информатизации и защите информации». Другие законы и нормативные акты.

**Раздел 10**. Хэш-функции

Свойства криптографических хэш-функций. Их использование в протоколах аутен- тификации и для контроля изменения чувствительной информации. Хэш-функции MD5, SHA1.

**Раздел 11**. Поточные шифры

Генераторы случайных и псевдослучайных чисел, их использование при аутен- тификации. Криптографические ГПСЧ, их свойства. Виды поточных шифров. Трудоем- кость дешифрования. Генератор LFSR, и его модификации. Алгоритмы А5, RC4

1. Образовательные технологии, используемые при осуществлении образо- вательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии: Вводная лекция – дает первое целостное представление о дисциплине и ориентиру-

ет студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, до- стижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особен- ности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно- методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требова- ния к академической лекции: современный научный уровень и насыщенная информатив- ность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и на- выков и закреплению полученных на лекции знаний.

1. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимо- сти)

В процессе осуществления образовательного процесса используются:

* для формирования текстов материалов для промежуточной и текущей аттестации, для разработки документов, презентаций, для работы с электронными таблицами - программы OfficeStd 2013 RUSOLPNLAcdmc 021-10232, LibreOffice (свободное), из- дательская система LaTeX;

- компиляторы с высокоуровневых языков программирования;

* для поиска учебной литературы библиотеки ЯрГУ–Автоматизированная биб- лиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

1. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освое- ния дисциплины

а) основная:

1. *Зенков, А. В.* Информационная безопасность и защита информации : учебное по- собие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образо- вательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/477968>(дата обращения: 24.11.2021).
2. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образо- вательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/470279>(дата обращения: 24.11.2021)
3. *Лось, А. Б.* Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образо- вательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469133>(дата обращения: 24.11.2021).

б) дополнительная:

*1. Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электрон- ный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/473348> (дата обращения: 24.11.2021).

1. Блэк, У., Интернет протоколы безопасности : учеб. курс / У. Блэк ; пер. с англ., СПб., Питер, 2001, 282c
2. Ярочкин, В. И., Информационная безопасность : учебник для вузов, М., Между- народные отноше, 2000, 399c

8. Материально-техническая база, необходимая для осуществления образо- вательного процесса по дисциплине

Аудитории, оборудованные для проведения лекций, практических занятий и консультаций,фонд библиотеки, компьютерная техника.

Автор(ы) :

Доцент кафедры компьютерных сетей, к.ф.-м.н. М.В.Краснов

Приложение №1 к рабочей программе дисциплины

**«Информационная безопасность»**

Фонд оценочных средств

**для проведения текущей и промежуточной аттестации студентов по дисциплине**

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы

**формирования компетенций**

1.1. Контрольные задания и иные материалы,используемые в процессе текущей ат- тестации

**Заданиядля самостоятельной работы**

Пример заданийдля самостоятельной работык разделу3

(проверка ОПК-4)

|  |  |
| --- | --- |
| Задания | Ответы: |
| 1.Задает ли решетку граф | Напомним несколько определений:  Опр1. Бинарное отношение « ¿ » на множестве *X* назовемотношением частичного порядка, когда для любых *a , b , c* ∈ *X* выполняются три свойства:  *a*≤*a ;*   * рефлексивность   ( *a*≤*b, b*≤*c* )⟶( *a*≤*c* )   * транзитивность   мметричность (*a*≤*b , b*≤*a*)⟶(*a*=*b*)   * антиси   Опр2. Для *a , b* ∈ *X* элемент *с*=*a*⊕ *b* ∈ *X* называется наименьшей верхней  границей, когда выполняются условия:  *a*≤*c ,b*≤*c*  -   * для *d* ∈ *X* истинно ( *a*≤*d ,b*≤*d* )⟶ (*c*≤*d* )   Опр 3. Для *a , b* ∈ *X* элемент *с*=*a*⊗ *b* ∈ *X* называется наибольшей нижней  границей, когда выполняются условия:  *с*≤*a ,c* ≤*b*  -   * для *d* ∈ *X* истинно ( *d*≤*a ,d* ≤*b* )⟶ (*d*≤*c* )   Опр 4. Пусть *X* − частично упорядоченное множество. ( *X ,*≤)− называет- ся решеткой, когда для любых *a , b* ∈ *X* существуют *a* ⊕ *b* ∈ *X* и *a* ⊗ *b* ∈ *X*  Рассмотрим заданный граф Выполняются условия:  ( *a*≤*b, b*≤*c* )⟶( *a*≤*c* )  (*a*≤*c , c*≤*d* )⟶( *a*≤*d* )  ( *a*≤*d ,d* ≤*a* )⟶(*a*=*d* )*,* но *a*≠*d* и в соответствии с Опр1 не выполняется свойство антисимметричности отношения частичного порядка « ¿ » на  множестве {*a, b, c, d*}. Следовательно, по Опр2 граф не задает решетку. |
| 2.Модель Харрисона- Руззо-Ульмана (ХРУ) Сформулируйте команду создания субъектом *s* личного файла *f* | CommandCreateFile( *s , f* )  *f ;*  «создать» объект  *M* [ *s, f* ]*;*  «внести» право владения ownв  «внести» право чтение readв *M* [ *s, f* ]*;* |

|  |  |
| --- | --- |
|  | «внести» право запись writeв *M* [ *s,f* ]*;*  End. |
| 3.Классическая модель Take-Grant. Проверьте, яв- ляется ли мостом граф до- ступов | Опр Мостом в графе доступов *G*0 называется tg-путь, концами которого яв- ляются вершины субъекты, проходящий через вершины объекты, словарная за- пись которого имеет вид ⃗*t* ¿ *,t*¿ *,*⃗*t* ¿ ⃗*gt*¿ *,* ⃗*t*∗*gt*¿ *,* где \* означает многократное (в том числе нулевое) повторение.  Используем следующие обозначения для вершин графа доступов  *s*1 *, s*2 - субъекты; *o*1 *, o*2 - объекты |
|  | получим |
|  |  |
|  | Так как в определении нет ограничений на повтор объектов на мосту, то граф  доступов задает мост со словарной записью ⃗*t ,*⃗*t gt ,* с концами в вершинах- субъектах *s*1 *, s*2 и проходящий через объекты *o*2 *, o*1 *, o*2 . |

Критерииоценивания

|  |  |  |
| --- | --- | --- |
| Номер  зада- чи | Критерии | Шкала оценивания |
| 1 | *Владеть навыками:*построение модели информационной безопасности. | 1. баллов – студент полностью не вер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разо- брался в решении задачи |
| 2 | *Владеть навыками:* построение модели информационной безопасности | 0 баллов – студент полностью не вер- но решил задачу  2 балла – студент полностью разо-  брался в решении задачи |
| 3 | *Владеть навыками:* построение модели информационной безопасности | 1. баллов – студент полностью не вер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разо- брался в решении задачи |

Набранное количество баллов соответствует оценке за выполнение работы:

* менее 3 баллов— оценка «неудовлетворительно»;
* от 3 до 4 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
* 5 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
* 6 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу 4

(проверка ОПК-4)

|  |  |
| --- | --- |
| Задания | Ответы: |
| 1.Приведите пример работы протоко- ла типа «точка-точка»  Предположим, что пользователи | Два варианта ответа:  1. передачу сеансового ключа можно описать следующей символь- ной записью: |

|  |  |
| --- | --- |
| *A* и обладают общей секретной информацией (секретным ключом  *k AB* ). | *A* →*B* : *Ek* (*k , T ,b* )*,*  *AB*  которая означает, что пользователь *A* создал сеансовый ключ  *k* и отправил пользователю *B* сообщение *Ek AB* (*k ,T , b*) *,*  *Ek*  где *AB* - алгоритм шифрования с ключом *k AB* , - сеансовый  ключ, *T* − временная метка, *b* -идентификатор пользователя  *B* . Зная секретный ключ *k AB* пользователь *B* легко может найти ключ *k* .  2. Если дополнительно требуется аутентификация сеанса, то можно использовать протокол, состоящий из следующих действий:   1. *B* → *A* : *rB* 2. *A* →*B* : *Ek AB* ( *k ,r B ,T , b*)   где запись *B* → *A* : *rB* означает, что пользователь *B* сгене- рировал случайное число *rB* и отправил его пользователю *А ;* запись *A* →*B* : *Ek AB* ( *k ,r B ,T , b*)  означает, что пользователь *A* создал сеансовый ключ *k* и отправил пользователю *B* сообщение *Ek AB* (*k , rB , T , b*)  *Ek*  где *AB* - алгоритм шифрования с ключом *k AB* , - сеансовый  ключ, *T* − временная метка, *b* -идентификатор пользователя *B* . Зная секретный ключ *k AB* пользователь *B* легко может найти ключ *k ,* а по числу *rB* убедиться, что его послал  пользовать *A* . |
| 2. Есть два пользователя *A* и *B*  используя протокол DIFFIE- HELLMAN сгенерируйте общий сек- ретный ключ | Числовые значения могут отличаться от тех, которые приведены в  данном решении   1. Пользователи *A* и *B* выбирают в открытом доступе боль- шое простое число *n* и *g* , где *g* образующий элемент   *Z*¿ .  мультипликативной группы *n*  Пусть *n*=13 и *g*=2   1. Пользователь *A* выбирает случайное большое натуральное число *x* и отправляет пользователю *B* величину   *X* =*gx* mod¿*n* ¿ ; Пусть *x*=5 и *X* =6   1. Пользователь *B* выбирает случайное большое натуральное-   число *y* и отправляет пользователю *A* величину  *Y* =*gy* mod ¿*n* ¿ ; Пусть *y*=7 и *Y* =11   1. Пользователь *A* вычисляет величину *k* =*Y x* mod¿*n* ¿ ; Вычисляем *k*=115mod ¿13=7 ¿ 2. Пользователь *B* вычисляет величину ~*k* =*X y* mod ¿*n* ¿ .   Вычисляем ~*k* =67 mod ¿13=7 ¿  ~*k* =*k* =7  Получили |
| 3. Есть два пользователя *A* и *B* используя протокол MTI сгенерируй- те общий секретный ключ | Числовые значения могут отличаться от тех, которые приведены в данном решении  1.Пользователи *A* и *B* выбирают в открытом доступе боль- шое простое число *n* и *g* , где *g* образующий элемент |

|  |  |
| --- | --- |
|  | *Z*¿ .  мультипликативной группы *n*  Пусть *n*=13 и *g*=2  2. Пользователи *A* и *B* должны сгенерировать секретные ключи *a ,* 1≤*a*≤*n*−2 *,* и *b,* 1≤*b*≤*n*−2 *,* соответственно,  *z* =*ga* mod *n*  и публикуют свои открытые ключи *A* и  *z* =*gb* mod *n*  *B* ;  Пусть Пользователь *A* генерирует число *a*=5 и публикует  *z* =25 mod13=6 *B*  *A* , соответственно пользователь генериру-  *b*=3 *z* =23 mod 13=8  ет число и публикует *B* ;   1. Пользователь *A* выбирает случайное натуральное число *x* , 1≤*x*≤*n*−2 и отправляет пользователю *B* величину *X* =*gx* mod¿ *n* ¿ ;   Пусть пользователь *A* генерирует число *x*=2 и отправляет пользователю *B* величину *X* =22 mod ¿13=4 ¿ ;   1. Пользователь *B* выбирает случайное большое натуральное число *y* , 1≤ *y* ≤*n*−2 и отправляет пользователю *A* вели- чину *Y* =*gy* mod ¿*n* ¿ ;   Пусть пользователь *B* генерирует число *y*=4 и отправляет пользователю величину *Y* =24 mod ¿ 13=3 ¿ ;  *A k* =*Y a z x* mod *n*   1. Пользователь вычисляет величину *B* ;   Пусть пользователь *A* на настоящий момент знает величины: *n , g , a , z A , zB , x , X ,Y* . Пользователь *A* вычисляет величину *k* =(*Y a zx* )mod ¿ *n*= ¿ (3582)mod 13= (9∗12) mod13=4  *B*  ~*k* =*Xb z y* mod *n*.   1. Пользователь *B* вычисляет величину *A*   Пусть пользователь *B* на настоящий момент знает величины:  *n , g ,b , z A , zB , y , X , Y* . Пользователь *B* вычисляет величину  ~*k* =( *Xb z y* ) mod ¿ *n*= ¿ ( 3 4 )  *A* 4 6 mod ¿13= ¿ 12∗9 mod¿13=4 ¿  ~*k* =*k* =4  Получили |
| 4. Постройте схему разделения секре-  та на примере пороговой схемы Шамира (*n,t* )*;* где *n*=5 *,t*=3 . В качестве конечного поля возьмем *Z*13 , секретной информацией бу- дем считать число 11 | Числовые значения могут отличаться от тех, которые приведены в  данном решении  Схема разделения секрета включает два протокола:   * протокол формирования частичных секретов и распределе- ния их между пользователями; * протокол восстановления секрета группой пользователей. В качестве примера рассмотрим пороговую схему Шамира.   Для построения пороговой схемы (*n ,t* ) Шамир воспользовался  *f* (*x* )=*b xt*−1+*b xt*−2+…+*b x* +*b*  многочленами вида *t*−1 *t* −2 1 0 в  конечном поле. Секретным считается свободный член *b*0 .  В качестве конечного поля возьмем *Z*13 , а в качестве многочлена,на котором основана схема Шамира (5,3)*;* возьмем *f* ( *x* )=(7 *x*2+8 *x* +11) ¿¿ .   * протокол формирования частичных секретов состоит в вы- числении *f* (*x* )   *a*1=*f* ( 1)=(7 +8+11 )mod ¿ 13=0 ¿ ; |

|  |  |
| --- | --- |
|  | *a*2=*f* ( 2)=(28+16+11 )mod ¿ 13=3 ¿ ;  *a*3=*f* ( 3 )=(63+24 +11) mod ¿ 13=7 ¿ ;  *a*4=*f* ( 4 )=(112+ 32+11 ) mod ¿13=12 ¿ ;  *a*5=*f* ( 5)=(175+40+ 11) mod ¿13=5 ¿ .   * протокол восстановления секрета группой пользователей из *t* человек.   Чтобы восстановить *f* (*x* ) из трех частичных секретов. Будем считать, что нам дано *a*2 *, a*3 *, a*5 тогда решается система линейных уравнений:  ¿ ¿  Решением будет *b*2=7 *, b*1=8 *, b*0=11 . |

Критерии оценивания

|  |  |  |
| --- | --- | --- |
| Номер  зада- чи | Критерии | Шкала оценивания |
| 1 | *Уметь:* выполнять передачу или генерацию ключей. | 1. баллов – студент полностью не вер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разо- брался в решении задачи |
| 2 | *Уметь:* выполнять передачу или генерацию ключей. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или была допущена вычисли- тельная ошибка. 3. балла – студент полностью разо- брался в решении задачи |
| 3 | *Уметь:* выполнять передачу или генерацию ключей. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или была допущена вычисли- тельная ошибка.. 3. балла – студент полностью разо- брался в решении задачи |
| 4 | *Уметь:* выполнять передачу или генерацию ключей. | 1. баллов – студент полностью не вер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или была допущена вычисли- тельная ошибка.. 3. балла – студент полностью разо- брался в решении задачи |

Набранное количество баллов соответствует оценке за выполнение работы:

* менее 4 баллов— оценка «неудовлетворительно»;
* от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
* от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
* 8 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу5

(проверка ОПК-3)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Задания | | | | Ответы: |
| 1. Вычислить | *x*≡1  {*x*≡2  *x*≡3  *x*≡3 *x* ≡7 | mod mod mod mod mod | 3  5  7  11  13 | Напомним процесс вычисления.Пусть задано:  множество натуральных чисел (*m*1 *, m*2 *,*. .. *, mk* ) не равных единице, которые являются попарно взаимно простыми множество натуральных чисел (*b*1 *, b*2 *,*. .. *, bk* ). Система сравнений  *x*≡*b*1 mod *m*1  {. . .  *x* ≡*bk* mod *mk*  *x*=*x*0 ¿ mod(*m*1 *m*2 . .. *mk* )*;* ¿ где  имеет решение  *x* = *M M' b* +.. .+ *M M' b ;* числа *Ms* и *Ms* опреде-  0 1 1 1 *k k k*  ляется изусловий *m*1 *m*2. . . *mk* =*Ms ms , M M '* =1 ¿ mod *m* ¿  *s s s*  Рассмотрим наше уравнение  *M* 1=5005 *, M* 2=3003 *, M* 3=2145 *, M* 4=1365 *, M* 5=1155 .  *M'* =1 *, M'* =2 *, M'* =5 *, M'* =1*, M'* =6 .  1 2 3 4 5  *m*1 *m*2. . . *m*5=15015  *x*0=5005∗1∗1+3003∗2∗2+2145∗5∗3+  +1365∗3∗1+1155∗6∗7=101797  *x*=11707 |
| 2.Построить криптосистемуЭль-Гамаляи за- кодируйте число 7 | | | | Числовые значения могут отличаться от тех, которые приве- дены в данном решении  Криптосистема Эль-Гамаля строится следующим образом:   * сначала выбирается большое простое число *p* * выбирается число *g* которое является примитивным для   *Zp*   * выбирается случайное натуральноечисло *x ,* причем   *x*∈ *p*   * вычисляем *y*=*gx* mod *p* |
|  | | | | Для того чтобы зашифровать сообщение *M* надо выполнить следующие действия:   * выбрать случайное натуральное число *k ,* ¿1∈*k*∈ *p*−1*,* ¿   такое что числа *k* и *p*−1 взаимно простые.   * вычислить *a*=*gk* mod *p* и *b*=( *yk M* )mod *p*. |
|  | | | | Пара чисел (*a,b*) и есть шифрованный текст |
|  | | | | Для того чтобы расшифровать сообщение, надо вы- |
|  | | | | *M* = *b* mod *p* .  числить *ax*  Построим криптосистемуЭль-Гамаля и закодируем число  7  Строим криптосистему   * выбираем *p*=13 *; g*=2 *;* выбираемсекретный ключ   *x*=8 . |

|  |  |
| --- | --- |
|  | * вычисляем *y*=28 mod13=9   Для того чтобы зашифровать сообщение *M* =7 надо вы- полнить следующие действия:   * выбрать случайное натуральное число *k* =7 заметим, что числа 7 и 12 взаимно простые. * вычислить *a*=27mod 13=11 и *b*=(97∗7 ) mod 13=11 .   Шифрованный текст – пара чисел (11*,*11) |
| 3. Сформулировать алгоритм установки ЭЦП DSA. Дан текст с хэш значением рав- ным 7. Выполните установку ЭЦП DSA | Числовые значения могут отличаться от тех, которые при- ведены в данном решении  Схема DSA строится следующим образом:   * сначала выбирается большое простое число *p* * выбирается простое число *q* которое является делителем   *p*−1   * выбирается натуральноечисло *t ,* которое 0∈*t* ∈ *p*. .   *p*−1  Если число *t q* =1 mod *p ,* то выбираем другое число  *p*−1  *t* . В противном случае *g*=*t q* mod *p* .   * выбирается натуральноечисло *x ,* которое является сек- ретным ключом причем 1∈ *x*∈ *q* * вычисляем *y*=*gx* mod *p*   Установка подписи:   * проверяем выполняется ли условие для хэш значение *m*   текста *M ,* что 0∈*m*∈*q*   * выбирается натуральноечисло *k ,* ¿(0∈*k* ∈*q*) . ¿ * вычисляем *k*−1 *,* для которого выполняется условие   *k*∗*k*−1=1mod *q*   * вычисляем два числа *r* и *s* по следующим прави- лам:   *r*=(*gk* mod *p*)mod *q* и *s*=*k*−1( *xr*+*m*) mod *q*  Если не выполняются условия 0∈*r* ∈ *q ,* 0∈ *s*∈*q* поме- няйте входные параметры.  Подписью является пара чисел (*r , s* )  Проверка подписи  Предположим, что к нам пришло сообщение *M '* с хэш значением *m'* и подписью (*r' , s'* )   * если хотя бы одно из условий 0∈*r'* ∈*q ,*0∈ *s'* ∈ *q* не вы- полняется, то подпись считается недействительной * *v* =(*s'* )−1mod *q*   вычисляем   * вычисляем:   *'*  *z*1=( *m v* ) mod *q*  *z* =( *r' v* ) mod *q*  2  *u*=(( *gz*1 *y z*2 ) mod *p*) mod *q*   * проверяем условие *r'*=*u* . Если оно выполняется то подпись считается подлинной а сообщение –неизменен- ным.   Дан текст с хэш значением равным 7. Выполните |

|  |  |
| --- | --- |
|  | установку ЭЦП DSA.  Строим схему DSA   * выбираем *p*=23 *, q*=11*, t*=3 * вычисляем *g*=32 mod 23=9 * выбираем *x*=2 * вычисляем *y*=92mod 23=12   Установка подписи:   * выбираем *k* =4 * вычисляем:   *k*−1=3 ,  *r*=(94 mod 23)mod 11=6 ,  *s*=(3∗(2∗6+7 )) mod 11=2  Подписью является пара чисел (6,2) |
| 4. Применяя расширенный алгоритм Евкли- да:   1. найти *d ,x , y* для которых выполняется   *d*=*НОД* (*a , b* )=*ax* +*by ,* гдеa=342; b=612   1. найти *q* для которого выполняется   8*q* mod 101=1 | a) 18=342\*9+612\*(-5), следовательно *d*=18 *, x*=9 *, y*=−5  b) После применении расширенного алгоритма Евклида  *d*=*НОД* (*a , b* )=*ax* +*by ,* где *a*=101*, b*=8 .  Мы получим: 1=*НОД* (101 *,* 8 )=101∗(−3 )+8∗38 *,* возьмем указанное выражение по модулю 101. В результате  (101∗(−3 )+8∗38)mod 101⟶(8∗38)mod 101⟶ *q*=38 |

Критерии оценивания

|  |  |  |
| --- | --- | --- |
| Номер  зада- чи | Критерии | Шкала оценивания |
| 1 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разо- брался в решении задачи |
| 2 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разо- брался в решении задачи |
| 3 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разо- брался в решении задачи |
| 4 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил только однуподзадачу. 3. балла – студент полностью разо- |

|  |  |  |
| --- | --- | --- |
|  |  | брался в решении задачи |

Набранное количество баллов соответствует оценке за выполнение работы:

* менее 4 баллов— оценка «неудовлетворительно»;
* от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
* от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
* 8 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу 8

(проверка ОПК-3)

|  |  |
| --- | --- |
| Задания | Ответы: |
| 1.Постройте аффинную криптоси- стему *f* (*x* )=(*ax* +*b* ) mod *m ,* для русского алфавита. Закодируйте слово «кокос» | Числовые значения могут отличаться от тех, которые приведены в данном решении  Напомним, что аффинная криптосистема определяется тремя натуральными числами *a,b,m*. Шифрование происходит заменой символа с порядковым номером *x* на символ порядко- выйномер которого вычисляется по формуле *f* (*x* )=(*ax* +*b* ) mod*m* . Заметим, что на пару чисел *a* и *m* наложено условие взаимной простоты.  Закодируйте слово «кокос».  Будем рассматривать *f* (*x* )=(5 *x*+2) mod33 . Нам надо закодиро-  вать (11*,*15*,*11*,*15*,*18). В результате получим (24 *,*11*,*24 *,*11*,*26). |
| 2. Взломайте аффинную криптоси- стему *f* (*x* )=(*ax* +*b* ) mod *m ,* для рус- ского алфавита. Известно, что в ис- ходном тексте чаще всего встречают- ся символы с порядковыми номерами  10 и 15, а в шифрованном тексте с по- рядковыми номерами 7 и 12. | Нам надо решить систему  {10 *a*+*b*=7 mod 33 {10 *a*+*b*=12 mod33  15 *a*+*b*=12 mod33 15 *a*+*b*=7 mod 33  или  Ответ *a*=1¿*b*=30 ¿ или *a*=32¿*b*=22 ¿ |
| 3. Выполните операцию умножения байтов в поле *GF*(28 )*,* которая ис- пользуется в алгоритме AES.  *x*7+ *x* +1 и *x*6+ *x*4 + *x*2+ *x* +1 | Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля *GF*(28 ). Поскольку байты оперируют в поле *GF* (28 )*,* то заданы операции сложения и умножения:   * сложение - суть операция поразрядного *XOR* . * умножение- это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена   *ϕ*( *x*) и использованием операции *XOR* при приведении подобных членов. В качестве неприводимого многочлена  *ϕ* ( *x* )=*x*8+ *x*4+ *x*3+ *x*+1 .  Выполняем умножение  ((*x*7+*x*+1)∗(*x*6+*x*4+*x*2+*x*+1))¿mod(*x*8+*x*4+*x*3+*x*+1)=¿=*x*7+*x*6+1. |
| 4. Примените процедуру MixColunmsалгоритма AES к вектору (*e*0 *,b* 4*,*52*,ae* ) , результат запишите в виде четырехбайтового слова | ПроцедураMixColunms, одна из процедур используемых в раунде алгоритма AES.  Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля *GF*(28 ). Поскольку байты оперируют в поле *GF* (28 )*,* то заданы операции сложения и умножения:   * сложение ⊕ - суть операция поразрядного *XOR* .   + умножение- это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена |

|  |  |
| --- | --- |
|  | *ϕ*( *x*) и использованием операции *XOR* при приведении подобных членов. В качестве неприводимого многочлена  *ϕ* ( *x* )=*x*8+ *x*4+ *x*3+ *x*+1 .  Раундовые преобразования работают с четырехбайтовыми сло- вами. Этому слову можно поставить в соответствие многочлен  3 2 8  *a*( *x* )=*a*3 *x* + *a*2 *x* + *a*1 *x*+ *a*0 , где *ai* ∈ *GF* (2 ). Рассмотрим как  будет происходить сложение и умножение четырехбайтовых слов  *a*( *x*) *b*( *x*)*, a*( *x* )=*a x*3+ *a x*2+ *a x*+ *a ,*  и где 3 2 1 0  *b*( *x* )=*b x*3+ *b x*2+*b x*+ *b*  3 2 1 0 :   * сложение   *a*( *x* )+ *b*( *x* )=( *a* ⊕ *b* ) *x*3+( *a* ⊕ *b* )*x*2+(*a* ⊕ *b* ) *x*+( *a* ⊕ *b* )  3 3 2 2 1 1 0 0   * умножение   *с* ( *x* )=*a*( *x* )⊗ *b* (*x* )=*c x*6+ *c x*5 +*c x*4+ *c x*3+*c x*2+*c x*+ *c ,*  6 5 4 3 2 1 0  Для того, чтобы результат умножения был снова представлен в виде четырехбайтового слова, его надо взять по модулю многочле- на *x*4+ 1. Следовательно, в результате получим вектор  *d* ( *x* )=*d x*3 +*d x*2+*d x* +*d*  3 2 1 0  ПроцедураMixColunmsалгоритма AESсостоит из трех операций:   * вектор записывается как многочлен вида   *a*( *x* )=*a x*3+ *a x*2+ *a x*+ *a*  3 2 1 0   * мы должны вычислить *d* ( *x* )=*a*( *x* )⊗ *g*( *x* )*,* где   *g*( *x* )={03}*x*3+{01} *x*2+{01} *x* +{02}.   * записать многочлен виде вектора   Решение   * вектор (*e* 0*, b* 4*,* 52*,ae* ) , записываем как многочлен   *a*( *x* )={*ae*}*x*3+{52}*x*2+{*b* 4 }*x* +{*e* 0}.   * вычисляем *d* ( *x* )=*a*( *x* )⊗ *g*( *x* ) * записываем ответ (*e*0 *, cb ,*19 *,* 9 *a* ) |

Критерии оценивания

|  |  |  |
| --- | --- | --- |
| Номер  зада- чи | Критерии | Шкала оценивания |
| 1 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил одну вычислитель- ную ошибку. 3. балла – студент полностью разо- брался в решении задачи |
| 2 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы | 0 баллов – студент полностью невер- но решил задачу  2 балла – студент полностью разо- брался в решении задачи |
| 3 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную   ошибку. |

|  |  |  |
| --- | --- | --- |
|  |  | 2 балла – студент полностью разо- брался в решении задачи |
| 4 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разо- брался в решении задачи |

Набранное количество баллов соответствует оценке за выполнение работы:

* менее 4 баллов— оценка «неудовлетворительно»;
* от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
* от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
* 8 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу10

(проверка ОПК-3)

|  |  |
| --- | --- |
| Задания | Ответы: |
| 1.Дайте определение хэш-функции | Хэш-функция h — это функция, определенная на битовых строках произвольной длины со значениями в стро- ках битов фиксированной длины.. Хэш-функция h() при- нимает в качестве аргумента сообщение (документ) М произ- вольной длины и возвращает хэш-значение h(M) = Н фикси-  рованной длины. Предполагается, что алгоритм вычисления хэш-значения является эффективным и общедоступным. |
| 2.Укажите, каким условиям должна удовле- творять хэш-функция | Хэш-функция должна удовлетворять целому ряду условий:   * хэш-функция должна быть чувствительна к всевозможным изменениям в тексте М, таким как вставки, выбросы, пере- становки * хэш-функция должна обладать свойством необратимости, то есть задача подбора документа М', который обладал бы требуемым значением хэш-функции, должна быть вычисли- тельно трудная; * вероятность того, что значения хэш-функций двух различ- ных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала   Проиллюстрируем, что условия накладываемые на хеш функцию очень важны Предположим, что есть два пользо- вателя А и В  **условие 1**хэш-функция должна быть чувствительна к все- возможным изменениям в тексте М, таким как вставки, выбросы, перестановки, предположим противное. Тогда фра- зы «Казнить, нельзя помиловать» и «Казнить нельзя, поми- ловать» будут иметь одно хэш-значение и текст можно под- менить.  Для иллюстрации оставшихся условий рассмотрим ЭЦП RSA.  Дано текст *M* и его хэш-значение *h* ( *M* ) . Все парамет- ры, которые используются в криптосистеме RSA.  *S*=*h*( *M* )*d* mod *n*  Установка подписи вычисляем:  Проверка подписи:   * вычисляем *H'* =*Se* mod *n* * вычисляем *h* ( *M* ) |

|  |  |
| --- | --- |
|  | *'*   * проверяем равенство *H* =*h* ( *M* ) . Если оно верно, то   подпись законна.  **условие 2**это условие препятствует криптоаналитику фаб- риковать сообщение с данной подписью, предположим условие не выполняется.  Тогда возможна следующая атака.  - B вычисляет *H'* =*Re* mod *n* с некоторым выбранным наугад целым числом *R* .  *-* Кроме того, B находит прообраз значения *H'* при отображении *h*() , т.е. B определяет *М = h-1 (m').* Теперь B обладает Вашей подписью *R* длясообщения М.  **условие 3** вероятность того, что значения хэш- функций двух различных документов совпадут, должна быть ничтожно мала, предположим противное. Тогда возможна следующая атака   * А выбирает два сообщения *M* и *M ' ,* удовлетво- ряющие соотношению *H'* =*h* ( *M* )=*h* ( *M'* ) * А подписывает *M* и получает ( *M , S*) * Потом А отказывается от своего сообщения, утверждая,   что посылал сообщение *M '* . |
| 3. Основной принцип проектирования хэш- функции. | Основной принцип проектирования хэш-функции заклю- чается в том, что ее значения должны производить лавинный эффект. Другими словами, небольшое изменение в аргумен- те хэш-функции должно очень сильно повлиять на ее значе-  ние. |
| 4.Постройте однонаправленную хэш- функцию используя симметричный блочный алгоритм DES, хэш-значение состоит из *k* бит. | Однонаправленную хэш-функцию можно по- строить, используя симметричный блочный алго- ритмDES, например используя режим «обратная связь по шифру». Последний блок шифротекста можно рассматривать в качестве хэш-значения для текста *M* . |

Критерии оценивания

|  |  |  |
| --- | --- | --- |
| Номер  зада- чи | Критерии | Шкала оценивания |
| 1 | *Владеть навыками:*вычислять хэш значение | 0 баллов – студент полностью невер- но решил задачу  2 балла – студент полностью верно дал определение. |
| 2 | *Владеть навыками:*вычислять хэш значение | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, |

|  |  |  |
| --- | --- | --- |
|  |  | но не привел пояснений к ходу реше- ния.  2 балла – студент полностью разо- брался в решении задачи |
| 3 | *Владеть навыками:*вычислять хэш значение | 0 баллов – студент полностью невер- но решил задачу  2 балла – студент полностью верно дал определение. |
| 4 | *Владеть навыками:*вычислять хэш значение | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния (без схемы шифрования). 3. балла – студент полностью разо- брался в решении задачи |

Набранное количество баллов соответствует оценке за выполнение работы:

* менее 4 баллов— оценка «неудовлетворительно»;
* от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
* от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
* 8 баллов— оценка «отлично», высокий уровень формирования компетенции

Пример заданийдля самостоятельной работык разделу 11

(проверка ОПК-3)

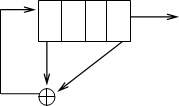
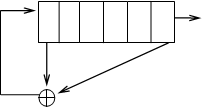
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Задания | Ответы: | | | | | | | |
| 1. Постройтерегистр сдвига с линейной |  | | | | | | | |
| обратной связью с ассоциированным много- |
| членом *x*4+ *x*+1 и выпишем состояние |
| регистра, если он был инициализирован век- |
| тором (1,1,1,1) . |
|  |  | Состояние регистра | | выход | Состояние регистра | | выход |  |
|  | итерация | состояние |  | итерация | состояние |  |  |
|  |  | рег. стало |  | рег. стало |
|  | 0 | 1111 |  | 9 | 0100 | 1 |  |
|  | 1 | 0111 | 1 | 10 | 0010 | 0 |  |
|  | 2 | 1011 | 1 | 11 | 0001 | 0 |  |
|  | 3 | 0101 | 1 | 12 | 1000 | 1 |  |
|  | 4 | 1010 | 1 | 13 | 1100 | 0 |  |
|  | 5 | 1101 | 0 | 14 | 1110 | 0 |  |
|  | 6 | 0110 | 1 | 15 | 1111 | 0 |  |
|  | 7 | 0011 | 0 |  |  |  |  |
|  | 8 | 1001 | 1 |  |  |  |  |
| 2. Постройте10 битную псевдослучайную последовательность с помощью BBS-генера- тора. | Числовые значения могут отличаться от тех, которые при- ведены в данном решении  Напомним, что BBS-генератор строится следующим обра- зом:   * вначале выбираются *p* и *q* - два больших простых числа примерно одинакового размера, причем   *p*≡3mod 4 и *q*≡3 mod 4 .   * вычисляемчисло *n*= *pq* ; * выбираем случайное целое число *x,* что числа *x* и   *n* являются взаимно простыми;   * *x* = *x*2 mod *n*   вычисляем число 0 , которое называется  стартовым числом генератора;   * искомой последовательностью бит длиной *m* будет яв- | | | | | | | |

|  |  |
| --- | --- |
|  | ляться последовательность  *BBSn, m* ( *x*0 )=*b*0 *b*1 *b*2…*bi*…*bm*−1 *, i*=0 *,*… *, m*−1 *,*  *b x x* =*x*2 mod *n*.  где *i* - младший бит числа *i* , *i*+1 *i*  Постройте 10 битную псевдослучайную последовательность   * Пусть *p*=11*, q*=19 *,* тогда *n*=209. Пусть *x*=2 . * *x* = *x*2 mod *n*⟶   Стартовое число генератора 0  *x* =22 mod 209⟶ *x* =4  0 0 .   * В качестве элементов псевдослучайной последовательно- сти будем брать младший бит в двоичной записи чисел   *x* =*x*2 mod *n*  *i*+1 *i*  В результате получимпоследовательность  *BBS 209 ,10* (4 )=0011010001 |
| 3. Создайте комбинирующий генератор, состоящий из двух регистров сдвига с ли- нейной обратной связью.  Первый регистр с ассоциированным многоч- леном *x*6+*x* +1 *,* он был инициализиро- ван вектором (1,1,1,1,1,1) . Выход регистра  *y*1 .  Второй регистр с ассоциированным многоч- леном *x*4+ *x*+1 он был инициализирован вектором (1,1,1,1) . Выход регистра *y*2 .  В качестве комбинирующей функции возьмем *f* ( *y*1 *, y*2 )= *y*1 ⊕ *y*2  Постройте 7 битную псевдослучайную по- следовательность | Напомним, что комбинирующий генератор проиллюстри- ровать следующей схемой  Решение   * Первыйрегистр  * Второй регистр   В результате получимпоследовательность 0000100 |
| 4. Создайте сжимающий генератор, состоя- щий из двух регистров сдвига с линейной  обратной связью. | Напомним, что сжимающий генератор описывается следу- ющей образом:  Используется 2 регистра с линейной обратной связью. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | состояние рег. стало | *y*1 . | итерация | состояние рег. стало | *y*1 . |
| 0 | 111111 |  | 4 | 101011 | 1 |
| 1 | 011111 | 1 | 5 | 010101 | 1 |
| 2 | 101111 | 1 | 6 | 101010 | 1 |
| 3 | 010111 | 1 | 7 | 110101 | 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | состояние рег. стало | *y*2 . | итерация | состояние рег. стало | *y*2 . |
| 0 | 1111 |  | 4 | 1010 | 1 |
| 1 | 0111 | 1 | 5 | 1101 | 0 |
| 2 | 1011 | 1 | 6 | 0110 | 1 |
| 3 | 0101 | 1 | 7 | 0011 | 0 |

Первый регистр с ассоциированным многоч- леном *x*6+*x* +1 *,* он был инициализиро-



(1,1,1,1,1,1)

Тактовые импульсы поступают на оба LFSR. Предположим, что

*b*=*b*0 *b*1 *b*2 … последовательность с выхода LFSR1.

ван вектором

*bi* .

. Выход регистра

*c*=*c*0 *c*1 *c*2… - последовательность с выхода LFSR2,

Второй регистр с ассоциированным многоч-

*x*4+ *x*+1

Тогда результирующая последовательность

*z*=*z*0 *z*1 *z*2… включает в себя те биты *bi ,* для которых

леном

он был инициализирован

соответствующие биты *ci*=1 . Остальные биты последо-

вектором (1,1,1,1) . Выход регистра *сi* . Постройте 7 битную псевдослучайную по- следовательность

вательности *b*

игнорируются.

Решение

* + Первыйрегистр

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | состояние рег. стало | *bi* | итерация | состояние рег. стало | *bi* |
| 0 | 111111 |  | 5 | 010101 | 1 |
| 1 | 011111 | 1 | 6 | 101010 | 1 |
| 2 | 101111 | 1 | 7 | 110101 | 0 |
| 3 | 010111 | 1 | 8 | 011010 | 1 |
| 4 | 101011 | 1 | 9 | 001101 | 0 |

* + Второй регистр

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | Состояние рег. стало | *ci* | итерация | состояние рег. стало | *ci* |
| 0 | 1111 |  | 5 | 1101 | 0 |
| 1 | 0111 | 1 | 6 | 0110 | 1 |
| 2 | 1011 | 1 | 7 | 0011 | 0 |
| 3 | 0101 | 1 | 8 | 1001 | 1 |
| 4 | 1010 | 1 | 9 | 0100 | 1 |

В результате получимпоследовательность 1111110

Критерии оценивания

|  |  |  |
| --- | --- | --- |
| Номер  зада- чи | Критерии | Шкала оценивания |
| 1 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разо- брался в решении задачи |

|  |  |  |
| --- | --- | --- |
| 2 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разо- брался в решении задачи |
| 3 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разо- брался в решении задачи |
| 4 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разо- брался в решении задачи |

Набранное количество баллов соответствует оценке за выполнение работы:

* менее 4 баллов— оценка «неудовлетворительно»;
* от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
* от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
* 8 баллов— оценка «отлично», высокий уровень формирования компетенции

Типовой вариант контрольной работы

На контрольных работах студентам предлагается следующие типовые задания:

Контрольная работа 1

|  |  |
| --- | --- |
| (проверка ОПК-4) | |
| Задания | Ответы: |
| 1.Задает ли решетку граф | Опр 1. Бинарное отношение « ¿ » на множестве *X* назовемотношением частичного порядка, когда для любых *a , b , c* ∈ *X* выполняются три свойства:  *a*≤*a ;*   * рефлексивность   ( *a*≤*b, b*≤*c* )⟶( *a*≤*c* )   * транзитивность   мметричность (*a*≤*b , b*≤*a*)⟶(*a*=*b*)   * антиси   Опр2. Для *a , b* ∈ *X* элемент *с*=*a*⊕ *b* ∈ *X* называется наименьшей верхней  границей, когда выполняются условия:  *a*≤*c ,b*≤*c*  -   * для *d* ∈ *X* истинно ( *a*≤*d ,b*≤*d* )⟶ (*c*≤*d* )   Опр 3. Для *a , b* ∈ *X* элемент *с*=*a*⊗ *b* ∈ *X* называется наибольшей нижней  границей, когда выполняются условия:  *с*≤*a ,c* ≤*b*  -   * для *d* ∈ *X* истинно ( *d*≤*a ,d* ≤*b* )⟶ (*d*≤*c* )   Опр 4. Пусть *X* − частично упорядоченное множество. ( *X ,*≤)− называет- ся решеткой, когда для любых *a , b* ∈ *X* существуют *a* ⊕ *b* ∈ *X* и *a* ⊗ *b* ∈ *X*  Рассмотрим заданный граф. |

|  |  |
| --- | --- |
|  | В соответствии с определением выполняются все свойства отношения частич- ного порядка на множестве {*a,b, c, d , e, f* } Для каждой пары вершин, соеди-  ненныхв графе путем, существует наименьшая верхняя и наибольшая нижняя граница. Другими словами: *d* ⊕*e*=*a , d* ⊗ *e*=*f ; b* ⊕ *e*=*a , b* ⊗ *e*=*f ;*  *d* ⊕*c*=*a, d* ⊗ *c*=*f ; b* ⊕ *c*=*a , b* ⊗ *c*=*f* .  Следовательно, по Опр4 граф задает решетку. |
| 2.Модель Харрисона- Руззо-Ульмана (ХРУ) Сформулируйте команду передачи субъекту *s'* права readк файлу *f*  его владельцем субъектом  *s* | *CommandGrantFile*( *s , s' , f* )  *IF* ¿ ¿  чтение *read*в *M* [ *s' , f* ]*;*  «внести» право  *endIF*  End. |
| 3. Есть три пользователя  *A , B* и *С* используя протокол DIFFIE- HELLMAN сгенерируйте общий секретный ключ | Числовые значения могут отличаться от тех, которые приведены в данном решении   1. Пользователи *A , B* и *С* выбирают в открытом доступе большое про- стое число *n* и *g* . Пусть *n*=13 и *g*=2 2. Пользователь *A* выбирает случайное большое натуральное число *x* и отправляет пользователю *B* величину *X* =*gx* mod¿*n* ¿ ;   Пусть *x*=5 и *X* =6   1. Пользователь *B* выбирает случайное большое натуральное число *y* и отправляет пользователю *C* величину *Y* =*gy* mod ¿*n* ¿ ;   Пусть *y*=7 и *Y* =11   1. Пользователь *C* выбирает случайное большое натуральное число *z* и отправляет пользователю *A* величину *Z* =*gz* mod ¿*n* ¿ ;   Пусть *z*=3 и *Z* =8   1. Пользователь *A* отправляет пользователю *B* следующую величину   *Z'*=*Zx* mod¿*n* ¿ ; Вычисляем *Z'*=85mod ¿ 13=8 ¿   1. Пользователь *B* отправляет пользователю *С* следующую величину   *X'*= *X y* mod ¿*n* ¿ ; Вычисляем *X'*=67mod ¿ 13=7 ¿   1. Пользователь *C* отправляет пользователю *A* следующую величину   *Y '*=*Y z*mod ¿ *n* ¿ ; Вычисляем *Y '*=113 mod ¿13=5 ¿   1. Пользователь *A* вычисляет величину *k*=*Y* ¿ mod ¿*n* ¿ ; Вычисляем *k*=55mod ¿ 13=5 ¿ 2. Пользователь *B* вычисляет величину ~*k* =*Z*¿ mod ¿*n* ¿ .   Вычисляем ~*k* =87 mod ¿ 13=5 ¿  ~ ¿   1. Пользователь *C* вычисляет величину *k*¯=*X* mod ¿ *n* ¿ .   ~ 3  Вычисляем *k*¯=7 mod ¿13=5 ¿  ~ ~¯  Получили *k* =*k* =*k* =5 |
| 4. Есть два пользователя  *A* и *B* используя протокол MTI сгенери- руйте общий секретный ключ, если известно, что  *n*=17 | Числовые значения могут отличаться от тех, которые приведены в данном решении   1. Пользователи *A* и *B* выбирают в открытом доступе большое простое число *n* и *g* , где *g* образующий элемент мультипликативной группы   *Z*¿ .  *n*  Пусть *n*=17 и *g*=3   1. Пользователи *A* и *B* должны сгенерировать секретные ключи *a ,* |

|  |  |
| --- | --- |
|  | 1≤*a*≤*n*−2 *,* и *b,* 1≤*b*≤*n*−2 *,* соответственно, и публикуют свои  *z* =*ga* mod *n z* =*gb* mod *n*  открытые ключи *A* и *B* ;  Пусть Пользователь *A* генерирует число *a*=2 и публикует  *z* =32 mod17=9 *B*  *A* , соответственно пользователь генерирует число  *b*=3 *z* =33 mod 17=10  и публикует *B* ;   1. Пользователь *A* выбирает случайное натуральное число *x* ,   1≤*x*≤*n*−2 и отправляет пользователю *B* величину *X* =*gx* mod¿*n* ¿ ; Пусть пользователь *A* генерирует число *x*=4 и отправляет пользовате- лю *B* величину *X* =34 mod ¿17=13 ¿ ;   1. Пользователь *B* выбирает случайное большое натуральное число *y* ,   1≤ *y* ≤*n*−2 и отправляет пользователю *A* величину *Y* =*gy* mod ¿*n* ¿ ; Пусть пользователь *B* генерирует число *y*=5 и отправляет пользовате- лю величину *Y* =35mod ¿ 17=5 ¿ ;  *A k* =*Y a z x* mod *n*   1. Пользователь вычисляет величину *B* ;   Пусть пользователь *A* на настоящий момент знает величины: *n , g , a , z A , zB , x , X ,Y* . Пользователь *A* вычисляет величину *k* =(*Y a zx* )mod ¿ *n*= ¿ (52104) mod 17= (15∗10000 ) mod 17=15  *B*  ~*k* =*Xb z y* mod *n*.   1. Пользователь *B* вычисляет величину *A*   Пусть пользователь *B* на настоящий момент знает величины:  *n , g ,b , zA , zB , y , X , Y* . Пользователь *B* вычисляет величину  ~*k* =( *Xb z y* ) mod ¿ *n*= ¿ ( 3 5) (2197∗59049) mod¿ 17=15 ¿  *A* 13 9 mod ¿17= ¿  ~*k* =*k* =15  Получили |
| 5. Постройте схему разде-  ления секрета на примере пороговой схемы Шамира (*n,t* )*;* где *n*=5 *,t*=3 .  В качестве конечного поля возьмем *Z*17 | Числовые значения могут отличаться от тех, которые приведены в данном  решении  Схема разделения секрета включает два протокола:  В качестве конечного поля возьмем *Z*17 , а в качестве многочлена,на котором основана схема Шамира (5,3).   * Рассмотрим протокол формирования частичных секретов. Возьмем   *f* ( *x* )=(2 *x*2+2 *x* +2) ¿¿ .  протокол формирования частичных секретов состоит в вычислении *f* (*x* )  *a*1=*f* ( 1)=(2+2+2 ) mod ¿ 17=6 ¿ ;  *a*2=*f* ( 2)=(8+4 +2) mod ¿ 17=14 ¿ ;  *a*3=*f* ( 3 )=(18+6+2 )mod ¿ 17=9 ¿ ;  *a*4=*f* ( 4 )=(32+8+ 2) mod ¿ 17=8 ¿ ;  *a*5=*f* ( 5)=(50+10+2) mod ¿ 17=11 ¿ .   * Рассмотрим протокол восстановления секрета группой пользователей из *t* человек, и найдем секретную информацию *b*0   Чтобы восстановить *f* (*x* ) из трех частичных секретов. Будем считать, что нам дано *a*1=12 *, a*2=5 *, a*3=4 тогда решается система линейных уравнений:  ¿ ¿  Решением будет *b*2=3 *, b*1=1 *, b*0=8 . |
| (проверка ОПК-3) | |

|  |  |
| --- | --- |
| Задания | Ответы: |
| 1.Применяя расширенный алгоритм Евклида:   1. найти *d ,x , y* для   которых выполняется  *d*=*НОД* (*a , b* )=*ax* +*by ,*  где a=512; b=724   1. найти *x* для кото- рого выполняется   8 *x* mod107 | a) 4=*НОД* (512*,* 724 )=512∗(−41 )+724∗29 *,* следовательно  *d*=4 *, x*=−41*, y*=29  b) После применении расширенного алгоритма Евклида  *d*=*НОД* (*a , b* )=*ax* +*by ,* где *a*=107 *, b*=8.  ы получим: 1=*НОД* (107 *,*8)=107∗3+8∗(−40)*,*  М  возьмем указанное выражение по модулю 107. В результате  (107∗3+8∗(−40 ))mod 107⟶(8∗(−40))mod107 ⟶ *q*=−40=67 |
| 2.Построить криптоси- стемуRSAи закодируйте число 7 | Числовые значения могут отличаться от тех, которые приведены в данном решении  Криптосистема RSA строится следующим образом:   * сначала выбираются два больших простых числа *p* и *q* * вычисляем *n*= *pq* и *φ* (*n*)=( *p*−1) (*q*−1) * выбирается открытый ключ натуральное число *e* такой, что 1≤*e*≤*n*−1   и который является взаимно простым с *φ* (*n*)=( *p*−1) (*q*−1)   * вычисляем секретный ключ *d* такой, что 1≤*d* ≤*n*−1 и   *ed*≡1 mod *φ* (*n*)  Для того чтобы зашифровать блок сообщения *M* ¿ (0∈*M* ∈*n* ) ¿ надо выпол- нить следующие действия: *C*=*M e* mod *n*  Для того чтобы расшифровать блок сообщения *C* ¿(0∈*C*∈*n* ) ¿ надо выпол- нить следующие действия: *M* =*Cd* mod *n*  Построим криптосистемуRSA и закодируем число 7 Строим криптосистему   * выбираем *p*=3 и *q*=11*;* * вычисляем *n*=33 и *φ* (*n*)=20 * выбираем *e*=3 * вычисляем *d*=7   Для того чтобы зашифровать сообщение *M* =7 надо выполнить следующие действия:  *C*=*M e* mod *n*=73mod 33=13 |
| 3. Вычислить  *x*≡1 mod 4  {*x*≡3 mod 5  *x*≡2 mod 7 | Напомним процесс вычисления.Пусть задано:  множество натуральных чисел (*m*1 *, m*2 *,*. .. *, mk* ) не равных единице, которые являются попарно взаимно простыми  множество натуральных чисел (*b*1 *, b*2 *,*. .. *, bk* ). Система сравнений  *x*≡*b*1 mod *m*1  {. . .  *x* ≡*bk* mod *mk*  *x*=*x*0¿ mod(*m*1 *m*2. .. *mk* )*;* ¿ где *x* = *M M' b* +.. .+ *M M' b ;*  0 1 1 1 *k k k*  имеет решение  числа *Ms* и *Ms* определяется изусловий *m*1 *m*2. . . *mk* =*Ms ms ,*  *M M '* =1 ¿ mod *m* ¿  *s s s*  Рассмотрим наше уравнение  *M* 1=35 *, M* 2=28 *, M* 3=20 *; M'* =3 *, M'* =2 *, M'* =6 .  1 2 3  *m*1 *m*2 *m*3=140 *;*  *x*0=35∗3∗1+28∗2∗3+20∗6∗2=513  *x*=93 |
| 4. Сформулировать алго- | Числовые значения могут отличаться от тех, которые приведены в данном |

|  |  |
| --- | --- |
| ритм установки ЭЦП DSA. Дан текст с хэш зна- чением равным 5. Выпол- ните установку ЭЦП DSA. К полученным результа- там примените протокол проверки подписи | решении  Схема DSA строится следующим образом:   * сначала выбирается большое простое число *p* * выбирается простое число *q* которое является делителем *p*−1 * выбирается натуральноечисло *t ,* которое 0∈*t* ∈ *p*. . Если число   *p*−1  *t q* =1 mod *p ,* то выбираем другое число *t* . В противном случае  *p*−1  *g*=*t q* mod *p* .   * выбирается натуральноечисло *x,* которое является секретным ключом при- чем 1∈ *x*∈ *q* * вычисляем *y*=*gx* mod *p*   Установка подписи:   * проверяем выполняется ли условие для хэш значение *m* текста *M ,* что   0∈*m*∈*q*   * выбирается натуральноечисло *k ,* ¿ (0∈*k* ∈*q*) . ¿ * вычисляем *k*−1 *,* для которого выполняется условие *k*∗*k*−1=1mod *q* * вычисляем два числа *r* и *s* по следующим правилам:   *r*=(*gk* mod *p*)mod *q* и *s*=*k*−1( *xr*+*m*) mod *q*  Если не выполняются условия 0∈*r* ∈ *q ,* 0∈ *s*∈*q* поменяйте входные па- раметры.  Подписью является пара чисел (*r , s*)  Проверка подписи  Предположим, что к нам пришло сообщение *M '* с хэш значением *m'* и подписью (*r' , s'* )   * если хотя бы одно из условий 0∈*r'* ∈*q ,*0∈ *s'* ∈ *q* не выполняется, то подпись считается недействительной * *v* =(*s'* )−1mod *q*   вычисляем   * вычисляем:   *'*  *z*1=( *m v* ) mod *q*  *z* =( *r' v* ) mod *q*  2  *u*=(( *gz*1 *y z*2 ) mod *p*) mod *q*   * проверяем условие *r'*=*u* . Если оно выполняется то подпись считается подлинной а сообщение –неизмененным.   Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA. Строим схему DSA   * выбираем *p*=23 *, q*=11 *, t*=3 * вычисляем *g*=32 mod 23=9 * выбираем *x*=2 * вычисляем *y*=92mod 23=12   Установка подписи:   * выбираем *k* =4 * вычисляем:   *k*−1=3 ,  *r*=(94 mod 23)mod 11=6 ,  *s*=(3∗(2∗6+5)) mod 11=7 |

|  |  |
| --- | --- |
|  | Подписью является пара чисел (6,7)  Проверка подписи  Дано *m'* =5 *;* ¿ ¿   * условие 0∈6∈11*,* ¿ 0∈7∈11 ¿ выполняется * вычисляем:   *v* =(*s'* )−1mod *q*=7−1 mod 11=8  *z* =( *m' v* ) mod *q*=(5∗8) mod 11=7  1  *z* =( *r' v* ) mod *q*=(6∗8) mod 11=4  2  *u*=(( *gz*1 *y z*2 ) mod *p*) mod *q*=((97 ¿ 124) mod 23) mod 11=6  Условие *r'* =*u* выполнено, подпись подлинная. |
| 5. Построить рюкзачную криптосистему и закоди- ровать элементы множе- ства, которые состоят из двоичных векторов (000,010,011,111) | Числовые значения могут отличаться от тех, которые приведены в данном решении  Напомним описание рюкзачной криптосистемы.  Создание криптосистемы:   * выбираем сверхрастущий вектор *A*=(*a*1 *,* . .. *, an* ) - это секретная информа- ция   *n*  *m*>∑ *ai*   * выбираем *m* и *t ,* такие что *i*=1 и *НОД* (*m ,t* )=1 - это секрет-   ная информация   * вычисляем *t*−1 *,* такое что *t*∗*t*−1=1mod *m* - это секретная информация * строим вектор *B*=(*b*1 *,* .. . *,bn*) *,* где *bi*=*tai* mod *m*.   . Вектор *B* - это  открытая информация и используется, как ключ зашифрования.  Шифрование  *B*=(*b*1 *,* .. . *,bn*) *,* двоичныйвектор *X* =(*x*1 *,*. . .*, xn*).  Дано: вектор   * шифр вычисляем *C*=*B*∗*X*   Дешифрование  *A*=(*a*1 *,* . .. *, an* )*,* числа *C , t*−1 *, m*.  Дано: вектор  −1)   * вычисляем *α*=(*C*∗*t* mod *m* * решаем задачу о рюкзаке ( *A , α*)   Рассмотрим предложенное задание Создание криптосистемы:   * выберем *A*=(1,3,5 )*, m*=11 *,t*=5 *, t*−1=9 - это секретный ключ * вычислим *B*=(5,4,3) .   Шифрование  Дано: вектор *B*=(5,4,3) *,* двоичныевектора *x*1=(0,0,0 )*; x*2=(0,1,0) *;*  *x*3=(0,1,1)*; x*4=(1,1,1) .  получилишифр *c*1=0 *;c*2=4 *;c*3=7 *; c*4=12 |

Критерии оценивания

|  |  |  |
| --- | --- | --- |
| Номер зада-  чи | Критерии | Шкала оценивания |
| ОПК-4 | | |
| 1 | Владеть навыками: построение модели информационной безопасности | 0 баллов – студент полностью не вер- но решил задачу |

|  |  |  |
| --- | --- | --- |
|  |  | 1. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 2. балла – студент полностью разо- брался в решении задачи |
| 2 | Владеть навыками: построение модели информационной безопасности | 0 баллов – студент полностью не вер- но решил задачу  2 балла – студент полностью разо-  брался в решении задачи |
| 3 | Уметь: выполнять передачу или генерацию ключей. | 1. баллов – студент полностью не вер- но решил задачу 2. балл – студент верно решил задачу, но была допущена вычислительная ошибка. 3. балла – студент полностью разо- брался в решении задачи |
| 4 | Уметь: выполнять передачу или генерацию ключей. | 1. баллов – студент полностью не вер- но решил задачу 2. балл – студент верно решил задачу, но была допущена вычислительная ошибка. 3. балла – студент полностью разо- брался в решении задачи |
| 5 | Уметь: выполнять передачу или генерацию ключей. | 1. баллов – студент полностью не вер- но решил задачу 2. балл – студент верно рассмотре- лодин протокол формирование или восстановление секрета. 3. балла – студент полностью разо- брался в решении задачи |
| (проверка ОПК-3) | | |
| 1 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил одну подзадачу. 3. балла – студент полностью разо- брался в решении задачи |
| 2 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разо- брался в решении задачи |
| 3 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разо- брался в решении задачи |
| 4 | *Уметь:* реализовывать некоторые криптографические алгоритмы.  *Владеть навыками:*создавать ЭЦП. | 1. баллов – студент полностью невер- но решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разо- брался в решении задачи |
| 5 | *Уметь:* реализовывать некоторые криптографические | 0 баллов – студент полностью невер- |

|  |  |  |
| --- | --- | --- |
|  | алгоритмы. | но решил задачу |
| *Владеть навыками:*создавать ЭЦП. | 1 балл – студент верно решил задачу, |
|  | но не привел пояснений к ходу реше- |
|  | ния. |
|  | 2 балла – студент полностью разо- |
|  | брался в решении задачи |

Максимальное количество баллов по ОПК-4 -10 баллов Максимальное количество баллов по ОПК-3 -10 баллов

Набранное количество баллов соответствует оценки за контрольную работу: Рассмотрим формирование компетенций ОПК-4 и ОПК-3:

-менее 4 баллов компетенция не сформирована;

-от 4 до 6 баллов — пороговый уровень формирования компетенции;

* от 7 до 8 баллов —продвинутый уровень формирования компетенции;
* от 9 до 10 баллов —высокий уровень формирования компетенции.

Рассмотрим формирование оценки:

-менее 4 баллов по ОПК-4 или менее 4 баллов по ОПК-3 – оценка «неудовлетворительно»;

-от 4 до 6 баллов одна компетенция и от 4 до 8 баллов другая компетенция - оценка «удовлетвори-

тельно»;

-от 4 до 6 баллов одна компетенция и от 9 до 10 баллов другая компетенция или от 7 до 8 баллов

одна компетенция и от 7 до 10 баллов другая компетенция - оценка «хорошо»;

-от 9 до 10 баллов одна компетенция и от 9 до 10 баллов другая компетенция - оценка «отлично».

Контрольная работа 2

|  |  |
| --- | --- |
| (проверка ОПК-4) | |
| Задания | Ответы: |
| 1.Постройте аффинную криптосистему, для рус- ского алфавита. Закоди- руйте слово «золото» | Числовые значения могут отличаться от тех, которые приведены в данном решении  Напомним, что аффинная криптосистема определяется тремя нату- ральными числами *a, b,m*. Шифрование происходит заменой символа с по- рядковым номером *x* на символ порядковыйномер которого вычисляется по формуле *f* (*x* )=(*ax* +*b* ) mod *m* . Заметим, что на пару чисел *a* и *m* наложено условие взаимной простоты.  Закодируйте слово «золото».  Будем рассматривать *f* (*x* )=(7 *x*+5) mod33 . Нам надо закодировать  (8*,*15 *,*12*,*15*,*19 *,*15). В результате получим (28 *,*11 *,*23*,*11*,*6*,*11) или фраза «брьр- лр» |
| 2. Взломайте аффинную криптосистему  *f* (*x* )=(*ax* +*b* ) mod *m ,* дл я русского алфавита. Из- вестно, что в исходном тексте чаще всего встре- чаются символы с поряд- ковыми номерами 10 и 14, а в шифрованном тексте с порядковыми номерами 8  и 17. | Нам надо решить систему  {10 *a*+*b*=8 mod 33 {10 *a*+*b*=17 mod 33  14 *a*+*b*=17 mod 33 14 *a*+*b*=8 mod 33  или  Ответ *a*=27¿*b*=2 ¿ или *a*=6¿*b*=23 ¿ |
| 3. Выполните операцию | Алгоритм оперирует байтами, которые рассматриваются как элементы конеч- ного поля *GF*(28 ). Поскольку байты оперируют в поле *GF*(28 )*,* то заданы операции сложения и умножения:   * сложение - суть операция поразрядного *XOR* . * умножение- это операция умножения многочленов со взятием результата   по модулю некоторого неприводимого многочлена *ϕ*( *x*) и использованием операции *XOR* при приведении подобных членов. В качестве неприво- |
| умножения байтов в поле |
| *GF*(28 )*,* которая ис- |
| пользуется в алгоритме |
| AES. |
| *x*4+ *x*+1 и |
| *x*4+ *x*2 +1 |

LFSR

Состояние регистра

**итерация состоя-**

**ние**

Выход

**рег. стало** 8 4 3

димог0о многочле1н1а1

*ϕ* ( *x* )=*x*

+ *x* +*x*

+ *x*+1 .

Решен1ие

011 1

(( *x*4+ *x*+1)∗( *x*4+01*x*2+1))¿ m1 od( *x*8+ *x*4+ *x*3+ *x*+1 )=*x*6+ *x*5+ *x*4+*x*2. ¿

2

1

4

. Закодируйте с помощью

криптосистемы Хилла,

Напом3ним крипто0с1и0стему Хи1лла:

Все ар4ифметическ00и1е операци0и выполняются по модулю *n*=26 . Выбирает-

для английского алфавита.

*d*×*d M*

Зашифровать слово

ся цел5ое число

*d*1≥002 .

Оно у1казывает размерность используемых матриц.

«HELP»

Пуст 6 еперь *M*110

0

квадра ая матрица. Элементами матрицы

ь т

7

ляют

яв ся целые

−

111

числа

тн

0

о 25.

от 0 д

Отметим, что матрица *M* должна быть не-

вырожденной.матрица *M* является секретным ключом.

Шифрование происходит блоками по *d* символов, оно выполняется с помо- щью формулы *MP*=*C* mod *n ,* где *P*− блок исходного текста, а *C*− блок шифра.

Решение

* + Пустьбудет

*M*= 3 3

2 5

( )

1 ( ) ( )

*P* = *H* 7=

*P* = *L* = 11

* + *E* 4 и

2 ( ) ( )

*P* 15

*MP* = 7 = *H* =*C*

*1* 1( ) ( )

* Процессшифрования 8 *I* и

*MP* =( 0 )=(*A* )=*C*

*2*

19

*T*

2

В результате получим слово «HIAT»

(проверка ОПК-3)

Задания 1.Постройте регистр сдвига с линейной обрат- ной связью с ассоцииро- ванным многочленом

*x*3+ *x* +1 и выпишем

состояние регистра, если он был инициализирован вектором (111) .

Ответы:

вектор инициализации регистр сдвига

(1,1,1)

1. Постройте 10 битную псевдослучайную после- довательность с помощью RSA-генератора.

Числовые значения могут отличаться от тех, которые приведены в данном решении

Напомним, что RSA-генератор строится следующим образом:

* выбираем *p* и *q* - два больших простых числа примерно одинакового размера *p*≠*q* ;
* вычисляем число *n*= *pq* и число *ϕ* ( *n* )=( *p*−1)( *q*−1 ) ;
* выбираем случайное натуральное число *e* , которое являются взаимно простыми с *ϕ* ( *n* ) ;
* выбираем в качестве стартового числа генератора случайное натуральное число *x*0 ¿ (1∈ *x*0∈ *n*) ¿ ;
* искомой последовательностью бит длиной *m* будет являться последо- вательность

*RSAn , m* (*x*0 )=*b*0 *b*1 *b*2 …*bi* …*bm*−1 *, i* =0 *,*…*, m*−1 *,* где *bi* - младший бит

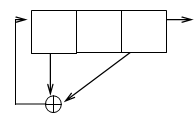
*i*

числа

*xi* ,

*xi*+1

=*xe* mod *n*.



Построим 10 битную псевдослучайную последовательность

|  |  |
| --- | --- |
|  | * Пусть *p*=3 *,* а *q*=11 . * Вычислим *n*= *pq*=33 и *ϕ* (*n* )=( *p*−1)( *q*−1 )=20 . * В качестве *e* возьмем число 3. * В качестве стартового числа генератора *x*0=14 . * В качестве элементов псевдослучайной последовательности будем брать   *x* =*xe* mod *n*.  младший бит в двоичной записи чисел *i*+1 *i*  В результате получили последовательность *RSA33 ,10* (14 )=0100010001 . |
| 3. Создайте комбиниру- ющий генератор, состоя- щий из двух регистров сдвига с линейной обрат- ной связью.  Первый регистр с ассоци- ированным многочленом *x*6+ *x* +1 *,* он был инициализирован векто- ром (1,1,1,1,1,1) . Выход  регистра *y*1 .  Второй регистр с ассоции- рованным многочленом *x*3+ *x* +1 он был инициализирован векто- ром (1,1,1) . Выход  регистра *y*2 .  В качестве комбиниру- ющей функции возьмем  *f* ( *y*1 *, y*2 )= *y*1 *y*2 Постройте 7 битную псев- дослучайную последо- вательность | Напомним, что комбинирующий генератор проиллюстрировать следующей схемой  Решение   * Первыйрегистр  * Второй регистр   В результате получимпоследовательность 1110100 |
| 4. Создайте сжимающий генератор, состоящий из двух регистров сдвига с линейной обратной свя- зью.  Первый регистр с ассоци- ированным многочленом *x*6+ *x* +1 *,* он был инициализирован векто- ром (1,1,1,1,1,1) . Выход  регистра *bi* . | Напомним, что сжимающий генератор описывается следующей образом:  Используется 2 регистра с линейной обратной связью. Тактовые импульсы поступают на оба LFSR. Предположим, что  *b*=*b*0 *b*1 *b*2 … последовательность с выхода LFSR1.  *c*=*c*0 *c*1 *c*2… - последовательность с выхода LFSR2,  Тогда результирующая последовательность *z*=*z*0 *z*1 *z*2… включает в себя те биты *bi ,* для которых соответствующие биты *ci*=1 . Остальные биты последовательности *b* игнорируются.  Решение |

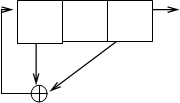
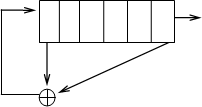
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | состояние рег. стало | *y*1 . | итерация | состояние рег. стало | *y*1 . |
| 0 | 111111 |  | 4 | 101011 | 1 |
| 1 | 011111 | 1 | 5 | 010101 | 1 |
| 2 | 101111 | 1 | 6 | 101010 | 1 |
| 3 | 010111 | 1 | 7 | 110101 | 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | состояние рег. стало | *y*2 . | итерация | состояние рег. стало | *y*2 . |
| 0 | 111 |  | 4 | 001 | 0 |
| 1 | 011 | 1 | 5 | 100 | 1 |
| 2 | 101 | 1 | 6 | 110 | 0 |
| 3 | 010 | 1 | 7 | 111 | 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | состояние рег. стало | *bi* | итерация | состояние рег. стало | *bi* |
| 0 | 111111 |  | 5 | 010101 | 1 |
| 1 | 011111 | 1 | 6 | 101010 | 1 |
| 2 | 101111 | 1 | 7 | 110101 | 0 |
| 3 | 010111 | 1 | 8 | 011010 | 1 |
| 4 | 101011 | 1 | 9 | 001101 | 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Состояние регистра | | выход | Состояние регистра | | выход |
| итерация | состояние рег. стало | *ci* . | итерация | состояние рег. стало | *сi* . |
| 0 | 111 |  | 5 | 100 | 1 |
| 1 | 011 | 1 | 6 | 110 | 0 |
| 2 | 101 | 1 | 7 | 111 | 0 |
| 3 | 010 | 1 | 8 | 011 | 1 |
| 4 | 001 | 0 | 9 | 101 | 1 |

Критерии оценивания



* Первыйрегистр
* Второй регистр

В результате получимпоследовательность 111110

Постройте 6 битную псев- дослучайную последо-

вательность

*сi* .

регистра

. Выход

(1,1,1)

ром

был векто-

он инициализирован

многочленом

рованным

*x*3+ *x* +1

Второй регистр с ассоции-

|  |  |  |
| --- | --- | --- |
| Номер задачи | Критерии | Шкала оценивания |
| ОПК-4 | | |
| 1 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы | 1. баллов – студент полностью неверно решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил одну вычислитель- ную ошибку. 3. балла – студент полностью разобрал-   ся в решении задачи |
| 2 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы | 0 баллов – студент полностью неверно решил задачу  2 балла – студент полностью разобрал-  ся в решении задачи |
| 3 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы | 1. баллов – студент полностью неверно решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 3. балла – студент полностью разобрал-   ся в решении задачи |
| 4 | *Уметь*: реализовывать некоторые криптографиче- | 0 баллов – студент полностью неверно |

|  |  |  |
| --- | --- | --- |
|  | ские алгоритмы | решил задачу   1. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния или допустил вычислительную ошибку. 2. балла – студент полностью разобрал-   ся в решении задачи |
| ОПК-3 | | |
| 1 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью неверно решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разобрал- ся в решении задачи |
| 2 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью неверно решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разобрал- ся в решении задачи |
| 3 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью неверно решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разобрал- ся в решении задачи |
| 4 | *Уметь*: реализовывать некоторые криптографиче- ские алгоритмы. | 1. баллов – студент полностью неверно решил задачу 2. балл – студент верно решил задачу, но не привел пояснений к ходу реше- ния. 3. балла – студент полностью разобрал- ся в решении задачи |

Максимальное количество баллов по ОПК-4 -8 баллов Максимальное количество баллов по ОПК-3 -8 баллов

Набранное количество баллов соответствует оценки за контрольную работу: Рассмотрим формирование компетенций ОПК-4 и ОПК-3:

-менее 4 баллов компетенция не сформирована;

-от 4 до 5 баллов — пороговый уровень формирования компетенции;

* от 6 до 7 баллов — продвинутый уровень формирования компетенции;
* 8 баллов — высокий уровень формирования компетенции.

Рассмотрим формирование оценки:

-менее 4 баллов по ОПК-4 или менее 4 баллов по ОПК-3 – оценка «неудовлетворительно»;

-от 4 до 5 баллов одна компетенция и от 4 до 7 баллов другая компетенция - оценка «удовлетвори-

тельно»;

-от 4 до 5 баллов одна компетенция и 8 баллов другая компетенция или от 6 до 7 баллов одна

компетенция и от 6 до 8 баллов другая компетенция - оценка «хорошо»;

-8 баллов одна компетенция и 8 баллов другая компетенция - оценка «отлично».

Тест для самопроверки по результатам освоения дисциплины.

(проверка ОПК-3)

**Вопрос 1**Вычислите *НОД* (315 *,*123)

Выберите ответ 1) 3.

2) 6

3) 12

*x x*=1mod5¿¿¿¿{

**2**Найдите для которого выполняется

**Вопрос**

Выберите ответ 1) 3.

2) 16

3) 12

**Вопрос 3**Алгоритмы шифрования с открытым ключом – это система

Выберите ответ

* 1. в которых ключ расшифрования трудно найти даже при известном ключе шифрования
  2. в которых ключ расшифрования легко находится по ключу шифрования
  3. в которых ключ расшифрования совпадает с ключом шифрования

**Вопрос 4**Закодируйте вектор *X* =(0,1,1) с помощью рюкзачной криптосистемы, которая является криптосистемой с открытым ключом.

Дано секретный ключ рюкзачной криптосистемы:

* + вектор *A*=(1,3,5 ) , которыйявляетсязакрытым;
  + число *m*=11 , котороеявляетсямодулем;
  + число *t* =5 ,котороеявляетсямножителем.

Выберите ответ 1) 7.

2) 16

3) 12

**Вопрос 5**Зашифруйтечисло 5 криптосистемой RSA,если задано

* + простые числа *p*=3 и *q*=7 ;
  + ключ шифрования (открытый ключ) *e*=5 .

Выберите ответ

1) 17

2) 2

3) 25

**Вопрос 6**В какой криптосистеме алгоритм шифрования блока *X* задается форму- лой *C*=*Xe* mod *n ,* где

* + *n*− это число, которое получается из формулы *n*= *p*∗*q ,* здесь *p* и *q*

простые числа;

* + *e*− это открытый ключ шифрования, который удовлетворяет условию

*НОД* (*e , ϕ*(*n* ))=1 *,* где *ϕ*(*n* )=( *p*−1)∗(*q*−1).

1. Криптосистема RSA
2. Криптосистема RC6
3. криптосистема AES

**Вопрос 7**Постройте 6 битную псевдослучайную последовательность RSA. Дано:

* Пусть *p*=3 *,* а *q*=7 .
* В качестве *e* возьмем число 5.
* В качестве стартового числа генератора *x*0=5.
* В качестве элементов псевдослучайной последовательности будем брать младший бит в двоичной записи чисел *xi*+1

1. В результатеполучилипоследовательность *RSA21, 6* (5 )=111111 .
2. В результатеполучилипоследовательность *RSA21, 6* (5 )=111110 .
3. В результатеполучилипоследовательность *RSA21, 6* (5 )=100101 .

**Вопрос 7**КриптосистемаRSA - это.

1. Криптосистема открытого ключа (ассиметричная криптосистема)
2. Симметричная криптосистема
3. Криптосистема вида квадрат

Правильныеответы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Вопрос №** | Вариант ответа |  | **Вопрос №** | Вариант ответа |
| **1** | 1 |  | **5** | 1 |
| **2** | 2 |  | **6** | 1 |
| **3** | 1 |  | **7** | 1 |
| **4** | 1 |  | **8** | 1 |

Каждый правильный ответ оценивается в 1 балл.

Набранное количество баллов 8 соответствует формированию проверяемой компе- тенции на высоком уровне, 6-7 баллов – на продвинутом уровне, 4-5 баллов – на по- роговом уровне, менее 4 баллов – ниже порогового уровня.

Список заданий к зачету

На зачете проверяется сформированность знаний, умений и навыков в соответствии с компетенциямиОПК-4 (вопросы 1–8) и ОПК-3 (вопросы 9–16).

Зачет проводится в устной форме и выставляется по итогам ответов, данных сту- дентом на два вопроса из списка. Список вопросов к зачету заранее доступен для студен- тов.

1. Определение информации, данных, знаний. Определение безопасности. Несанкционированный до- ступ.
2. Информационные системы. Доступность, целостность, конфиденциальность. Основные понятия об угрозах.
3. Каналы утечки информации, их классификация.
4. Каналы утечки информации технических средств обработки, хранения и передачи информации.- Каналы утечки речевой информации. Каналы утечки информации при её передаче по каналам связи.
5. Технические каналы утечки видовой информации. Каналы утечки информации, создаваемые ата- ками извне и внутри корпоративных систем ИКТ
6. Модели разграничения доступа по принципу предоставления прав. Модели дискретного доступа. Вероятностные модели.
7. Информационные модели. Модель мандатного доступа. Модель Бела-Лападулы, игровая модель. Матрица доступов.
8. Аутентикация, авторизация, пароли, токены, "рукопожатие". Протоколы аутентификации без пере- дачи секретной информации, одноразовые ключи.
9. Доказательство с нулевым знанием.
10. Асимметричные шифры, шифры с открытым ключом.
11. Электронные цифровые подписи. Трудоемкость дешифрования. Рюкзачная криптосистема.
12. Алгоритм RSA.
13. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Алгоритм Эль-Гамаля. Алгоритм Рабина.
14. Введение в защиту ПО. Угрозы безопасности ПО. Примеры уязвимостей ПО. Разрушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО.
15. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО. Компьютерные вирусы и антивирусные программы.
16. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Информационная безопасность распределенных систем. Рекомендации X.800

**Описание процедуры выставления оценивания сформированности компе- тенций**(для ответа на теоретический вопрос)

Результат определяется оценками «отлично» (высокий уровень), «хорошо» (продви- нутый уровень), «удовлетворительно» (пороговый уровень), «неудовлетворительно» (компетенция не сформирована).

Для оценивания ответов (по каждой компетенции):

Оценка «отлично»:

* студент ответил на вопрос правильно и полно. Оценка «хорошо»:
* студент ответил на вопрос правильно, но недостаточно полно (не менее 70% от полного).

Оценка «удовлетворительно»:

* студент ответил на вопрос с 1 ошибкой или 1-2 недочетами и неполно (не менее 70% от полного ответа).

Оценка «неудовлетворительно»:

* студент ответил на вопрос неправильно (больше 1 ошибки или 2 недочетов) или неполно (менее 70% от полного).

Критерии оценивания

Оценка **«зачтено»** выставляется студенту, который:

* + прочно усвоил предусмотренный программный материал;
  + правильно, аргументировано ответил на все вопросы, с приведением примеров;
  + показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов.

Дополнительным условием получения оценки «зачтено» могут стать хорошие успе- хи при выполнении самостоятельных и контрольной работы, систематическая активная работа на практических занятиях.

Оценка **«не зачтено»** Выставляется студенту, который не справился с 50% вопросов и заданий, в ответах на другие вопросы допустил существенные ошибки. Не может ответить на дополнительные вопросы, предложенные преподавателем. Целостного представления о взаимосвязях, компонентах дисциплины у студента нет.

Список заданий к экзамену

На экзамене проверяется сформированность знаний, умений и навыков в соответ- ствии с компетенциямиОПК-4 (вопросы 1–9) и ОПК-3 (вопросы 10–21).

Экзамен проводится в устной форме и выставляется по итогам ответов, данных студентом на два теоретических и один практический вопрос. Список теоретических вопросов к экзамену заранее доступен для студентов. В билете присутствует один практи- ческий вопрос, аналогичный рассмотренным в курсе.

Список вопросов к экзамену:

1. Определение информации, данных, знаний. Определение безопасности. Несанкционированный до- ступ.
2. Информационные системы. Доступность, целостность, конфиденциальность. Основные понятия об угрозах
3. Модели разграничения доступа по принципу предоставления прав. Модели дискретного доступа. Вероятностные модели.
4. Информационные модели. Модель мандатного доступа. Модель Бела-Лападулы, игровая модель. Матрица доступов.
5. Критерий адекватности защиты. Оранжева книга. Документы Гостехкомиссии РФ. Информацион- ная безопасность распределенных систем. Рекомендации X.800 .
6. Юридические вопросы информационной безопасности
7. Угрозы безопасности ПО. Примеры уязвимостей ПО. Разрушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО.
8. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО. Компьютерные вирусы и антивирусные программы
9. Шифрование. Трудоемкость дешифрования. Cимметричные шифры. Схема Фейстеля, SP-сеть. Режимы шифрования. Некоторые исторические алгоритмы (алгоритмы Цезаря, Вижнера).
10. Алгоритмы AES, Гост 28147-89, DES,
11. Serpent, Mars,IDEA
12. Каналы утечки информации технических средств обработки, хранения и передачи информа- ции. Каналы утечки речевой информации.
13. Каналы утечки информации при её передаче по каналам связи. Технические каналы утечки видовой информации. Каналы утечки информации, создаваемые атаками извне и внутри корпоративных систем ИКТ
14. Асимметричные шифры, шифры с открытым ключом.Идея открытых ключей и преимуще- ства их. Алгоритм Рабина. Алгоритм RSA. Алгоритм Эль-Гамаля
15. Электронные цифровые подписи. ЭЦП RSA, ЭЦП DSA, ЭЦП Гост
16. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Решить *y*=*ax* mod *p*
17. Генераторы случайных и псевдослучайных чисел, их использование при аутентификации. Криптографические ГПСЧ, их свойства.
18. Генератор LFSR, и его модификации. Взлом LFSR.
19. Виды поточных шифров. Алгоритмы А5, RC4, Flash, Wake
20. Аутентикация, авторизация, пароли.
21. Хэш-функции MD5, SHA1.

**Описание процедуры выставления оценивания сформированности компе- тенций** (для ответа на теоретический вопрос)

Результат определяется оценками «отлично» (высокий уровень), «хорошо» (продви- нутый уровень), «удовлетворительно» (пороговый уровень), «неудовлетворительно» (компетенция не сформирована).

Для оценивания ответов (по каждой компетенции):

Оценка «отлично»:

* студент ответил на вопрос правильно и полно. Оценка «хорошо»:
* студент ответил на вопрос правильно, но недостаточно полно (не менее 70% от полного).

Оценка «удовлетворительно»:

* студент ответил на вопрос с 1 ошибкой или 1-2 недочетами и неполно (не менее 70% от полного ответа).

Оценка «неудовлетворительно»:

* студент ответил на вопрос неправильно (больше 1 ошибки или 2 недочетов) или неполно (менее 70% от полного).

Критерии оценивания экзамена:

*«2» - плохо:*

Теоретический вопрос: студент не раскрыл теоретический вопрос, на заданные эк- заменаторами вопросы не смог дать удовлетворительный ответ.

Практический вопрос: студент не понял смысла текста (задачи), не смог выполнить задания. На заданные экзаменатором вопросы ответил неудовлетворительно, не проде- монстрировал сформированность требующихся для выполнения заданий знаний и умений. Или студент понял отдельные детали текста, но не его основной смысл, задания выполнил неправильно, на заданные экзаменатором вопросы ответил неудовлетворительно, не продемонстрировал сформированность требующихся для выполнения заданий умений.

*«3» - удовлетворительно:*

Теоретический вопрос: студент смог с помощью дополнительных вопросов вос- произвести основные положения темы, но не сумел привести соответствующие примеры или аргументы, подтверждающие те или иные положения.

Практический вопрос: студент понял смысл текста (задачи), но смог выполнить за- дание лишь после дополнительных вопросов, предложенных экзаменатором. При этом на поставленные экзаменатором вопросы не вполне ответил правильно и полно, но под- твердил ответами понимание вопросов и продемонстрировал отдельные требующиеся для выполнения заданий знания и умения.

*«4» - хорошо:*

Теоретический вопрос: студент (не допуская ошибок) правильно изложил теорети- ческий вопрос, но недостаточно полно или допустил незначительные неточности, не иска- жающие суть понятий, теоретических положений, правовых и моральных норм. Примеры, приведенные учеником, воспроизводили материал учебников. На заданные экзаменатором уточняющие вопросы ответил правильно.

Практический вопрос: студент понял смысл текста (задачи), предложенные задания выполнил правильно, но недостаточно полно. На заданные экзаменатором вопросы отве- тил правильно. Проявил необходимый уровень всех требующихся для выполнения зада- ний знаний и умений.

*«5» - отлично:*

Теоретический вопрос: студент полно и правильно изложил теоретический вопрос, привел собственные примеры, правильно раскрывающие те или иные положения, сделал обоснованный вывод;

Практический вопрос: студент понял смысл текста (задачи), полно и правильно вы- полнил предложенные задания, проявил высокий уровень всех требующихся для выполне- ния заданий знаний и умений.

1. Перечень компетенций, этапы их формирования, описание показателей и крите- риев оценивания компетенцийна различных этапах их формирования, описание

**шкалы оценивания**

* 1. Шкала оцениваниясформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дис- циплины осуществляется по следующейтрехуровневой шкале:

*Пороговый уровень* - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков,полученных сту- дентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

*Продвинутый уровень* - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

*Высокий уровень* - предполагает способность студента использовать потенциал ин- тегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятель- ного поиска новых подходов в их решении путем комбинирования и использования из- вестных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

1. Методические рекомендации преподавателюпо процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирова-

**ния компетенций**

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом дея- тельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разде- ле «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

* 1. Критерии оценивания степени овладения знаниями¸ умениями,навыкамии (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

* + - владение основным объемом знаний по программе дисциплины;
    - знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без суще- ственных ошибок;
    - владение инструментарием дисциплины, умение его использовать в реше- нии стандартных (типовых) задач;
    - способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
    - усвоение основной литературы, рекомендованной рабочей программой дис- циплины;
    - знаниебазовыхтеорий,концепцийинаправлений по изучаемой дисциплине;
    - самостоятельная работа на практических и лабораторных занятиях, пери- одическое участие в групповых обсуждениях, достаточный уровень культу- ры исполнения заданий.

Продвинутый уровень (общие характеристики):

* + - достаточно полные и систематизированные знания в объёме программы дис- циплины;
    - использование основной терминологии данной области знаний, стилистиче- ски грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
    - владение инструментарием дисциплины, умение его использовать в реше- нии учебных и профессиональных задач;
    - способность самостоятельно решать сложные задачи (проблемы) врамках рабочей программы дисциплины;
    - усвоение основной и дополнительной литературы, рекомендованной рабо- чей программой дисциплины;
    - умение ориентироватьсявбазовых теориях,концепцияхинаправлениях по изучаемой дисциплине и давать им сравнительную оценку;
    - самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

* + - систематизированные,глубокиеиполныезнанияповсемразделам дисциплины;
    - точное использование терминологии данной области знаний,стилистически грамотное, логически правильное изложение ответа на вопросы, умение де- лать обоснованные выводы;
    - безупречное владение инструментарием дисциплины, умение его использо- вать в постановке и решениинаучных и профессиональных задач;
    - способность самостоятельно и творчески решать сложные задачи (про- блемы) врамках рабочей программы дисциплины;
    - полное и глубокое усвоение основной и дополнительной литературы, ре- комендованной рабочей программой дисциплины;
    - умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
    - активная самостоятельнаяработанапрактических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
  1. Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в тече- ние нескольких семестров, оценка может выставляться не только по окончании ее освое- ния, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетвори- тельно», «неудовлетворительно», «зачтено», «незачтено») определяетсярабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полно- стью или частично формируемая данной дисциплиной) сформирована на высоком уровне. Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полно-

стью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компе- тенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформиро- вананиже, чем на пороговом уровне.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полно- стью или частично формируемая данной дисциплиной) сформирована не ниже, чем на по- роговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформировананиже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины

**«Информационная безопасность» Методические указания для студентов по освоению дисциплины**

Основной формой изложения учебного материала по дисциплине **«Информацион- ная безопасность»** являются лекции и практические занятия. Для успешного освоения дисциплины очень важно рассмотрение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий.

Задачи разбираются на лекциях и лабораторных занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Для решения всех за- дач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, лаборатор- ных занятиях или из учебной литературы. Большое внимание должно быть уделено вы- полнению домашней работы. В качестве заданий для самостоятельной работы дома сту- дентам предлагаются задания, аналогичные разобранным на лекциях и лабораторных за- нятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач. Для проверки и контроля усвоения теоретического материала, периодически проводятся контрольные работы.

Освоить вопросы, излагаемые в процессе изучения дисциплины «Математические методы защиты информации» самостоятельно студенту крайне сложно. Это связано со сложностью изучаемого материала и большим объемом курса. Поэтому посещение всех аудиторных занятий является совершенно необходимым. Без упорных и регулярных заня- тий в течение семестра сдать экзамен по итогам изучения дисциплины студенту практиче- ски невозможно.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы особенно рекомендуется использовать учебную ли- тературу.

Также для подбора учебной литературы рекомендуется использовать широкий спектр интернет-ресурсов:

1. Электронно-библиотечная система «Университетская библиотека online» ([www.biblioclub.ru](http://www.biblioclub.ru/) ) - электронная библиотека, обеспечивающая доступ к наиболее вос- требованным материалам-первоисточникам, учебной, научной и художественной литера- туре ведущих издательств (\*регистрация в электронной библиотеке – только в сети уни- верситета. После регистрации работа с системой возможна с любой точки доступа в Internet.).
2. Информационная система "Единое окно доступа к образовательным ресурсам" ([http://window.edu.ru/library).](http://window.edu.ru/library))

Целью создания информационной системы "Единое окно доступа к образователь- ным ресурсам" (ИС "Единое окно ") является обеспечение свободного доступа к ин- тегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования.

Информационная система "Единое окно доступа к образовательным ресурсам" со- здана по заказу Федерального агентства по образованию в 2005-2008 гг. Головной разра- ботчик проекта - Федеральное государственное автономное учреждение Государственный научно-исследовательский институт информационных технологий и телекоммуникаций (ФГАУ ГНИИ ИТТ "Информика") [www.informika.ru.](http://www.informika.ru/)

ИС "Единое окно" объединяет в единое информационное пространство электрон- ные ресурсы свободного доступа для всех уровней образования в России. Разделы этой системы:

* Электронная библиотека– является крупнейшим в российском сегменте Интерне- та хранилищем полнотекстовых версий учебных, учебно-методических и научных матери- алов с открытым доступом. Библиотека содержит более 30 000 материалов, источниками которых являются более трехсот российских вузов и других образовательных и научных учреждений. Основу наполнения библиотеки составляют электронные версии учебно- методических материалов, подготовленные в вузах, прошедшие рецензирование и ре- комендованные к использованию советами факультетов, учебно-методическими комисси- ями и другими вузовскими структурами, осуществляющими контроль учебно-методиче- ской деятельности.

-Интегральный каталог образовательных интернет-ресурсов содержит представлен- ные в стандартизованной форме метаданные внешних ресурсов, а также содержит описа- ния полнотекстовых публикаций электронной библиотеки. Общий объем каталога пре- вышает 56 000 метаописаний (из них около 25 000 - внешние ресурсы). Расширенный поиск в "Каталоге" осуществляется по названию, автору, аннотации, ключевым словам с возможной фильтрацией по тематике, предмету, типу материала, уровню образования и аудитории.

* Избранное. В разделе представлены подборки наиболее содержательных и полез- ных, по мнению редакции, интернет-ресурсов для общего и профессионального образова- ния.

-Библиотеки вузов. Разделсодержит подборки сайтов вузовских библиотек, элек- тронных каталогов библиотек вузов и полнотекстовых электронных библиотек вузов.

Для самостоятельного подбора литературыв библиотеке ЯрГУ рекомендуется ис- пользовать:

1. Личный кабинет (<http://lib.uniyar.ac.ru/opac/bk_login.php)дает> возможность по- лучения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб.и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Автори- зация», и заполнить представленные поля информации.
2. Электронная библиотека учебных материалов ЯрГУ (<http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)> содержит более 2500 полных тек-

стов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

1. Электронная картотека «Книгообеспеченность» (<http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php)>раскрывает учебный фонд на-

учной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книго- обеспеченности дисциплин основной и дополнительной литературой, а также цикла дис- циплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.