

Министерство науки и высшего образования Российской Федерации

Читинский институт (филиал)


ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра мировой экономики, предпринимательства и гуманитарных дисциплин

УТВЕРЖДЕН

на заседании кафедры мировой экономики,  
предпринимательства и гуманитарных дисциплин  
28 мая 2024 г. протокол № 9

Заведующий кафедрой  
С.А. Кравцова



**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ  
(ФОНД ОЦЕНОЧНЫХ СРЕДСТВ)  
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ  
Б1.О.20 Защита информации**

Специальность: 38.05.02 Таможенное дело

Специализация: Таможенное дело

Квалификация выпускника: специалист таможенного дела

Чита, 2024 г.

**Структура  
фонда оценочных средств  
по дисциплине «Защита информации»**

№ п/ п	Этапы формирования компетенций	Перечень формируемых компетенций	ЗУНы (З.1, У1, Н1...)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы	Описание показателей и критериев оценивания компетенций на различных этапах формирования, описания шкал оценивания
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы. Наиболее распространенные угрозы. Критерии классификации угроз. Вредоносное программное обеспечение	ОПК-2	З. Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Н. Обладать навыками для решения стандартных задач профессиональной деятельности на основе	Практическая работа №1. Формальные модели безопасности	9-10 баллов – сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 7-8 баллов – сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-6 баллов –

			информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов – студент обнаружил не состоятельность ответов (10)
2	Основные программно-технические меры. Сервисы безопасности. Шифрование, идентификация и аутентификация, контроль целостности	ОПК-2	3. Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Н. Обладать навыками для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением	Практическая работа №2. Методика определения информационных рисков	14-15 баллов – сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов – сформированные, но содержащие отдельные пробелы знаний; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов – общие, но не струк-

			информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		турированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил не состоятельность ответов (15)
3	Основные понятия криптографии. Блочные одноключевые шифры. Шифры поточного шифрования	ОПК-2	3. Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Н. Обладать навыками для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникацион-	Практическая работа №3. Шифрование сообщений методом Вижинера	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержащие отдельные пробелы знаний; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применения навыков; 7-10 баллов — общие, но не структурирован-

			ных технологий и с учетом основных требований информационной безопасности.		ные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятельность ответов (15)
4	Современные симметричные криптосистемы	ОПК-2	3. Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Н. Обладать навыками для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникацион-	Практическая работа №4. Блочное шифрование информации методом гаммирования	14-15 баллов – сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов – сформированные, но содержащие отдельные пробелы знаний; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов – общие, но не структурированные зна-

			ных технологий и с учетом основных требований информационной безопасности.		ния; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов – студент обнаружил несостоятельность ответов (15)
5	Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности	ОПК-2	3. Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Н. Обладать навыками для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	Практическая работа №5. Электронная жеребьевка	14-15 баллов – сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов – сформированные, но содержащие отдельные пробелы знаний; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов – общие, но не структурированные знания; не систематически осуществляемые

			безопасности.		умения; не систематически применяемые навыки; 6 и менее баллов – студент обнаружил несостоятельность ответов (15)
6	Административный уровень информационной безопасности. Политика безопасности. Процедурный уровень информационной безопасности.	ОПК-2	3. Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Н. Обладать навыками для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Практическая работа №6. Шифрование информации методом RSA	14-15 баллов – сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов – сформированные, но содержащие отдельные пробелы знаний; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов – общие, но не структурированные знания; не систематически осуществляемые умения; не система-

					тически применяемые навыки; 6 и менее баллов – студент обнаружил несостоятельность ответов (15)
7	<p>Определение «Цифровой подписи».</p> <p>Характеристика неотказуемости.</p> <p>Классическая схема подписи.</p> <p>Цифровая подпись по алгоритму DSA.</p> <p>Российский алгоритм цифровой подписи по ГОСТ Р34.10-94.</p> <p>Схема слепой подписи</p>	ОПК-2	<p>3. Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. У.</p> <p>Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Н.</p> <p>Обладать навыками для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	Практическая работа №7. Цифровая подпись	<p>14-15 баллов – сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов – сформированные, но содержащие отдельные пробелы знаний; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов – общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и</p>



					менее баллов – студент обнаружил не-состоятельность ответов (15)
8	Итого по текущей аттестации	ОПК-4		Практические работы №1-7	Итого до 100 баллов
9	Промежуточная аттестация	ОПК-2		Тестовое задание для проверки знаний. Задание для проверки умений. Задание для проверки навыков.	Тестовое задание для проверки знаний - 30 баллов. Задание для проверки умений - 35 баллов. Задание для проверки навыков - 35 баллов. Итого до 100 баллов

Министерство науки и высшего образования Российской Федерации  
ЧИТИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)  
ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
Кафедра мировой экономики, предпринимательства и  
гуманитарных дисциплин

**Оценочные средства текущего контроля**

**Практическая работа № 1**  
**«Формальные модели безопасности»**

1. Что такое Профиль защиты? Какова структура Профиля защиты?
2. Что позволяют определить требования адекватности?
3. Что такое задание по безопасности?
4. Какие службы сертификации ИТ-продуктов действуют в РФ?
5. Как произвольную систему ТМД представить системой ХРУ?
6. Для команды  $S(qi0, ai0) = (qi1, ai1, l)$  машины Тьюринга выпишите две представляющие ее команды модели ХРУ.
7. Что такое субъект системы? Что такое объект системы?
8. Каким может являться каждое состояние системы в соответствии с предложенным в модели критерием безопасности?

**Ответы**

1. Профиль защиты — это документ, описывающий требования безопасности к системе. Структура включает разделы, такие как цели безопасности, требования к безопасности и оценка соответствия.
2. Требования адекватности позволяют оценить, насколько система соответствует установленным требованиям безопасности.
3. Задание по безопасности — это документ, который содержит конкретные требования к системе и её безопасности.
4. В РФ действуют такие службы сертификации ИТ-продуктов, как ФСТЭК (Федеральная служба по техническому и экспортному контролю), Роскомнадзор и аккредитованные испытательные лаборатории.
5. Для представления системы ТМД системой ХРУ необходимо перевести команды ТМД в команды ХРУ, используя правила перехода.
6. Для команды  $S(qi0, ai0) = (qi1, ai1, l)$ :  
Команда 1:  

```
move qi0 -> qi1  
move ai0 -> ai1
```

  
Команда 2:  

```
halt
```
7. Субъект системы — это активный компонент, который выполняет действия. Объект системы — это пассивный компонент, на который направлены действия субъекта.
8. Каждое состояние системы может быть безопасным, небезопасным или промежуточным (переходным).

## Практическая работа № 2 «Методика определения информационных рисков»

*Цель работы* – освоить технологию качественной оценки информационного риска по трехфакторной модели.

### *Введение*

Под информационным риском понимают средние ожидаемые потери объекта защиты от реализации угрозы при существовании и использовании уязвимости в системе защиты информации. Таким образом, информационный риск оценивает средний размер ущерба, который может быть нанесен в результате некоторого негативного события.

Методика определения информационных рисков базируется на трехфакторной модели

$$R = P_{\text{уг}} \cdot P_{\text{уз}} \cdot C_{\text{п}}, \quad (1.1)$$

где  $R$  – значение (уровень) информационного риска;  $P_{\text{уг}}$  – вероятность появления угрозы;  $P_{\text{уз}}$  – вероятность использования уязвимости системы защиты информации;  $C_{\text{п}}$  – потери от свершившегося происшествия.

При управлении рисками определяются угрозы, уязвимости, оценивается возможный ущерб и вырабатываются контрмеры.

Оценка рисков осуществляется до и после внедрения контрмер.

Если рассматриваемые факторы оцениваются количественно, то говорят о значении риска (количественное измерение размера ущерба). Если эти факторы оцениваются качественно на основании информации экспертов, то речь идет об уровне информационного риска. В лабораторной работе рассматривается второй подход.

Лабораторная работа состоит из двух частей.

В первой части работы экспертно создается таблица для определения уровня информационного риска от выделенных трех факторов.

Во второй части работы определяется уровень информационного риска конкретной анализируемой ситуации.

### *Создание таблицы для определения уровня информационного риска от трех факторов*

Рассмотрим первую часть лабораторной работы (моделирует работу экспертов). Все три фактора, входящих в формулу (1.1), оцениваются специалистами, ответственными за информационную безопасность в организации. При этом они используют шкалы, которые подготавливают эксперты по всем трем факторам и по информационному риску. В общем случае шкала характеризуется числом уровней, наименованием уровней, а также экспертным описанием каждого уровня или специальной таблицей.

В лабораторной работе для вероятностей  $P_{\text{уг}}$  и  $P_{\text{уз}}$  используется три шкалы (наименования уровней заглавные русские буквы):

ШР3 (3 уровня): низкий (Н), средний (С), высокий (В);

ШР4 (4 уровня): низкий (Н), средний (С), высокий (В), очень высокий (ОВ);

ШР5 (5 уровней): очень низкий (ОН), низкий (Н), средний (С), высокий (В), очень высокий (ОВ).

При этом для вероятности угрозы используются шкалы ШР3 и ШР4, а для вероятности уязвимости используются шкалы ШР4 и ШР5.

Выбор уровней специалистами осуществляются по таблицам, которые устанавливают соответствие между баллами и уровнями. Эти таблицы готовят эксперты.

Для оценки потерь ( $C_n$ ) используется одна 5-и уровневая шкала (ШС5) (необходимо обратить внимание на экспертное описание уровней):

- $N$  (*Negligible*) – очень незначительные потери: воздействием можно пренебречь;

- $Mi$  (*Minor*) - незначительные потери: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно;

- $Mo$  (*Moderate*) - происшествие с умеренными потерями: ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию небольшое и не затрагивает критически важные задачи;

- $S$  (*Serious*) - происшествие с серьезными потерями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, влияет на выполнение критически важных задач;

- $C$  (*Critical*) - происшествие с очень серьезными потерями: происшествие приводит к невозможности решения критически важных задач.

Для информационного риска используется три шкалы (наименования уровней заглавные русские буквы):

ШР3 (3 уровня): низкий риск (НР), средний риск (СР), высокий риск (ВР);

ШР4 (4 уровня): низкий риск (НР), средний риск (СР), высокий риск (ВР), очень высокий риск (ОВР);

ШР5 (5 уровней): очень низкий риск (ОНР), низкий риск (НР), средний риск (СР), высокий риск (ВР), очень высокий риск (ОВР).

Необходимо построить таблицу для определения уровня информационного риска от трех факторов. Таких таблиц получается четыре в зависимости от уровней вероятностей ( $P_{уг}$ ,  $P_{уз}$ ): (3, 3), (3, 4), (4, 4), 4, 5). Число строк в этой таблице зависит от числа уровней вероятностей ( $P_{уг}$ ,  $P_{уз}$ ): а) (3, 3) – 9 строк; (3, 4) – 12 строк; (4, 4) – 16 строк; (4, 5) – 20 строк.

Число столбцов этой таблицы зависит от числа уровней шкалы потерь (ШС5), в нашем случае 5 столбцов. Для примера приведена таблица для уровней (3, 3) (табл. 1.1). Заполнение таблицы 1.1 зависит от числа уровней риска. Это заполнение выполняет студент, исходя из своего варианта. Приведем пример ее заполнения для 3-х уровневых риска (табл. 1.2).

*Таблица для заполнения уровней риска*

Уровень для $P_{уг}$	Уровень для $P_{уз}$	Уровни шкалы потерь (ШС5)				
		$N$	$Mi$	$Mo$	$S$	$C$
Н	Н					
	С					
	В					
С	Н					
	С					
	В					
В	Н					
	С					
	В					

Таблица 1.2

*Таблица для определения уровня риска*

Уровень для $P_{уг}$	Уровень для $P_{уз}$	Уровни шкалы потерь (ШС5)				
		$N$	$Mi$	$Mo$	$S$	$C$
Н	Н	НР	НР	НР	СР	СР
	С	НР	НР	СР	СР	ВР
	В	НР	СР	СР	ВР	ВР
С	Н	НР	НР	СР	СР	ВР
	С	НР	НР	СР	СР	ВР
	В	НР	СР	ВР	ВР	ВР
В	Н	НР	НР	СР	СР	ВР
	С	НР	СР	ВР	ВР	ВР
	В	СР	СР	ВР	ВР	ВР

После создания таблицы 1.2 первая часть лабораторной работы заканчивается.

#### *Определение уровня информационного риска конкретной ситуации*

Рассмотрим вторую часть лабораторной работы.

При определении уровня информационного риска для конкретной ситуации, необходимо оценить вероятности угроз и уязвимостей в зависимости от влияющих факторов. Для этого по угрозам и уязвимостям выделяются косвенные факторы, по которым предлагаются вопросы и несколько фиксированных вариантов ответов, которые «стоят» определенное количество баллов. Итоговая оценка угрозы и уязвимости данного класса определяется путем суммирования баллов.

Далее по таблице соответствия определяется уровень вероятностей угрозы и уязвимости. В варианте лабораторной работы студенту даны суммарные баллы для вероятностей угрозы ( $B_{P_{уг}}$ ) и уязвимости ( $B_{P_{уз}}$ ).

В таблице 1.3 приведено соответствие между значением  $B_{P_{уг}}$  и уровнем вероятности угрозы ( $Y_{P_{уг}}$ ), а в таблице 1.4 приведено соответствие между значением  $B_{P_{уз}}$  и уровнем вероятности уязвимости ( $Y_{P_{уз}}$ ).

Таблица 1.3

*Определение уровней для вероятности угрозы*

Балл для $P_{уг}$	Уровень для $P_{уг}$	Балл для $P_{уг}$	Уровень для $P_{уг}$
$B_{P_{уг}} \leq 12$	Н	$B_{P_{уг}} \leq 15$	Н
$12 < B_{P_{уг}} \leq 24$	С	$15 < B_{P_{уг}} \leq 32$	С
$24 < B_{P_{уг}} \leq 36$	В	$B_{P_{уг}} > 32$	В
$B_{P_{уг}} > 36$	ОВ	-	-

Таблица 1.4

*Определение уровней для вероятности уязвимости*

Балл для $P_{уз}$	Уровень для $P_{уз}$	Балл для $P_{уз}$	Уровень для $P_{уз}$
$B_{P_{уз}} \leq 7$	ОН	$B_{P_{уз}} \leq 10$	Н
$7 < B_{P_{уз}} \leq 16$	Н	$10 < B_{P_{уз}} \leq 21$	С
$16 < B_{P_{уз}} \leq 25$	С	$21 < B_{P_{уз}} \leq 32$	В
$25 < B_{P_{уз}} \leq 34$	В	$B_{P_{уз}} > 32$	ОВ
$B_{P_{уз}} > 34$	ОВ	-	-

*Содержание лабораторной работы*

Исходные данные по варианту лабораторной работы необходимо взять из таблицы 1.5.

1. Ввести последовательно исходные данные для своего варианта.
2. Исходя из числа уровней вероятности угрозы, необходимо ввести их наименования (шкалы ШРЗ или ШР4).
3. Исходя из числа уровней вероятности уязвимости, необходимо ввести их наименования (шкалы ШР4 или ШР5).
4. Исходя из числа уровней риска, необходимо ввести их наименования (шкалы ШР3, ШР4 или ШР5).
5. Если наименования уровней вероятностей введены верно, то на экране появляется таблица 1.1.
6. Далее необходимо сформировать таблицу 1.2. Это осуществляется заполнением таблицы 1.1 уровнями информационного риска.  
Созданием таблицы 1.2 завершается первый этап лабораторной работы.
7. Исходя из значения балла для вероятности угрозы и числа ее уровней, по таблице 1.3 определяется значение уровня этой вероятности –  $Y_{P_{уг}}$ . Этот уровень вводится, а затем проверяется.
8. Исходя из значения балла для вероятности уязвимости и числа ее уровней, по таблице 1.4 определяется значение уровня этой вероятности –  $Y_{P_{уз}}$ . Этот уровень вводится, а затем проверяется.
9. Исходя из значения уровня для потерь и полученных уровней для вероятностей ( $Y_{P_{уг}}$  и  $Y_{P_{уз}}$ ), по таблице 1.2 определяется уровень риска исследуемой ситуации. Этот уровень вводится, а затем проверяется.

10. Полученный уровень информационного риска является завершением второго этапа и лабораторной работы в целом.

### Варианты лабораторной работы

Таблица 1.5

№ варианта	Число уровней риска $R$	Число уровней для $P_{уг}$	Число уровней для $P_{уз}$	Балл для $P_{уг}$ (Б_Р <sub>уг</sub> )	Балл для $P_{уз}$ (Б_Р <sub>уз</sub> )	Уровень для потерь
1	5	4	4	15	27	$Mi$
2	5	3	4	27	18	$Mo$
3	5	4	5	8	32	$C$
4	4	4	4	43	28	$S$
5	4	3	4	38	24	$N$
6	4	4	5	19	14	$Mo$
7	5	4	4	27	18	$Mo$
8	5	3	4	15	24	$Mi$
9	5	4	5	8	32	$S$
10	4	4	4	43	28	$C$
11	4	3	4	38	24	$Mo$
12	4	4	5	19	14	$Mi$
13	3	4	4	16	19	$N$
14	3	4	5	32	29	$C$
15	3	4	4	16	19	$Mi$
16	3	4	5	32	29	$S$
17	5	4	5	25	22	$C$
18	5	4	4	17	28	$S$

### Практическая работа №3

#### Шифрование сообщений методом Вижинера

В лабораторной работе используются сообщения, связанные с текстами на рис. 1. В таблице 1 приведены ключи, в таблице 2 - коды букв русского алфавита, в таблице 3 - коды цифр шестнадцатеричной системы счисления.

Таблица 1

Ключи

1	Вагнер	4	Глинка
2	Бородин	5	Моцарт
3	Сальери	6	Берлиоз

Таблица 2

Коды букв

А	Б	В	Г	А	Е	Ё	Ж	З	И	Й
0	1	2	3	4	5	6	7	8	9	10
К	Л	М	Н	О	П	Р	С	Т	У	Ф
11	12	13	14	15	16	17	18	19	20	21
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
22	23	24	25	26	27	28	29	30	31	32

1. Современная государственная политика РФ в области защиты информации сформировалась в начале девяностых годов и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.
2. Хотя сама информация не материальна, но она имеет материальные носители. Говоря о мере информации, выделяют ее количество и объем. Объем данных в сообщении измеряется количеством символов принятого алфавита.
3. Информатика как наука изучает свойства, структуру и функции информационных систем, основы их проектирования, создания, использования и оценки, а также информационные процессы в них происходящие.
4. Под информационной системой понимают систему, организующую, хранящую и преобразующую информацию. В этой системе основным предметом и продуктом труда является информация.
5. Под безопасностью информации понимают свойство передаваемой, накапливаемой, обрабатываемой и хранимой информации, характеризующее ее степень защищенности от дестабилизирующего воздействия внешней среды и внутренних угроз.

Рис. 1. Исходные тексты

Таблица ПЗ

Коды цифр шестнадцатеричной системы счисления

ДСС	ШСС	ДСС	ШСС	ДСС	ШСС	ДСС	ШСС
0000	0	0100	4	1000	6	1100	С
0001	1	0101	5	1001	9	1101	Д
0010	2	1110	6	1010	А	1110	Е
0011	3	0111	7	1011	В	1111	F

Целью работы является получение практических навыков шифрования сообщений с использованием блочных многоалфавитных шифров подстановки.

Задание на лабораторную работу

Лабораторная работа состоит из трех частей:

1. Зашифрование исходного текста по методу Виженера.
2. Расшифровывание шифротекста, полученного на первом этапе.
3. Сравнение и проверка идентичности исходного текста и расшифрованного текста.



Замечание 1. Зашифрование и расшифрование текста в этой лабораторной работе имеет две модификации: а) использование шифровальной таблицы Виженера (ШТВ); б) использование операций сложения и вычитания по модулю 33 (СВМК). Модификация алгоритма заложена в вариант работы (табл. 4).

Замечание 2. При зашифровании текста знаки препинания убираются и все буквы считаются прописными (или заглавными), пробел сохраняется.

Замечание 3. Недостающие буквы последнего блока исходного текста необходимо дополнить буквой из своего варианта.

Замечание 4. При формировании шифротекста его необходимо разбить на блоки с числом символов, равному числу символов ключа. Вывод шифротекста осуществлять поблочно.

Исходные данные

1. Текст, состоящий из 5 абзацев, вариант состоит из одного абзаца.
2. Таблица Виженера и таблица соответствия между буквами и их порядковыми номерами (табл. 2).
3. Номер варианта (табл. 4). Ключ взять из таблицы 1.

Таблица 4

Варианты лабораторной работы				
№	Текст	Ключ	Буква	Модификация
1	1	1	А	ШТВ
2	1	2	Б	ШТВ
3	1	3	В	ШТВ
4	1	4	Г	ШТВ
5	1	5	А	ШТВ
6	1	6	Е	ШТВ
7	2	1	Ж	ШТВ
8	2	2	З	ШТВ
9	2	3	И	ШТВ
10	2	4	Й	ШТВ
11	2	5	К	ШТВ
12	2	6	Л	ШТВ
13	3	1	М	ШТВ
14	3	2	Н	ШТВ
15	3	3	О	ШТВ
16	3	4	П	ШТВ

## Практическая работа № 4

### Блочное шифрование информации методом гаммирования

Цель работы: Освоение принципов шифрования гаммированием, изучение свойств генератора псевдослучайных чисел, программная реализация метода гаммирования.

### Теоретические основы метода гаммирования

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной

гаммы шифра на открытые данные обратимым образом (например, используя операцию сложения по модулю 2). Процесс дешифрования сводится к повторной генерации гаммы шифра при известном ключе и наложении такой же гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей и изменяется случайным образом для каждого шифруемого слова. Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В этом случае простым сложением по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

### **Шифрование данных с помощью датчика псевдослучайных чисел (ПСЧ). Линейные конгруэнтные датчики ПСЧ**

Чтобы получить линейные последовательности элементов гаммы, длина которых не превышает размер шифруемых данных, используют датчики ПСЧ. Одним из хороших конгруэнтных генераторов является линейный конгруэнтный датчик ПСЧ. Он вырабатывает последовательности псевдослучайных чисел  $T(i)$ , описываемые соотношением

$$T(i+1) = (A \cdot T(i) + C) \bmod M, \quad (1)$$

где  $A$  и  $C$  - константы,  $T(0)$  - исходная величина, выбранная в качестве порождающего числа. Очевидно, что эти три величины и образуют ключ.

Такой датчик ПСЧ генерирует псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений  $A$  и  $C$ . Значение  $M$  обычно устанавливается равным  $2^b$ , где  $b$  - длина машинного слова в битах. Необходимо выбирать числа  $A$  и  $C$  так, чтобы период  $M$  был максимальным.

Как показано Д. Кнуттом, линейный конгруэнтный датчик имеет максимальную длину  $M$  тогда, когда  $C$  нечетное и  $A \bmod 4 = 1$ .

В качестве примера использования линейного конгруэнтного датчика ПСЧ рассмотрим процесс шифрования исходного текста «абв». Пусть  $b = 5$ , т.е. для представления буквы исходного текста используется 5 двоичных разрядов. В соответствии с номером в алфавите буква «а» имеет двоичный код 00001; буква «б» имеет двоичный код 00010; буква «в» имеет двоичный код 00011. Исходный текст будет представлен в виде последовательности 00001 00010 00011.

Для формирования гаммы шифра выберем параметры датчика ПСЧ:  $A=5$ ;  $C=3$ ;  $T(0)=7$ ;  $M=2^b$ ;  $b=5$ ;  $M=2^5=32$ . Сформируем три псевдослучайных числа:

$$T(1) = (5 \cdot 7 + 3) \bmod 32 = 6 \text{ (00110);}$$

$$T(2) = (5 \cdot 6 + 3) \bmod 32 = 1 \text{ (00001)};$$

$$T(3) = (5 \cdot 1 + 3) \bmod 32 = 8 \text{ (01000)}.$$

Полученная гамма шифра 00110 00001 01000. Зашифрованный текст получается путем наложения гаммы шифра на исходный текст (путем сложения по модулю 2):

$$\begin{array}{r} 00001 \ 00010 \ 00011 \\ 00110 \ 00001 \ 01000 \\ \hline 00111 \ 00011 \ 01011 \end{array}$$

что соответствует шифрограмме «жвк», «ж» (седьмая буква в алфавите) имеет код 00111, «в» (третья буква в алфавите) имеет код 00011, «к» (одиннадцатая буква в алфавите) имеет код 01011.

Дешифрование производится путем наложения той же гаммы на зашифрованный текст с помощью операции сложения по модулю 2:

$$\begin{array}{r} 00111 \ 00011 \ 01011 \\ 00110 \ 00001 \ 01000 \\ \hline 00001 \ 00010 \ 00011 \end{array}$$

В результате получаем исходный текст «абв».

### Метод гаммирования с обратной связью

Значение зашифрованного символа зависит не только от гаммы, но и от предыдущих символов.

Для получения сегмента гаммы можно использовать контрольную сумму определенного участка шифруемых данных. Процесс шифрования в этом случае представляется следующими шагами:

1. Генерация сегмента гаммы  $H(1)$  и наложение его на соответствующий участок шифруемых данных.
2. Подсчет контрольной суммы участка, соответствующего сегменту гаммы  $H(1)$ .
3. Генерация с учетом контрольной суммы уже зашифрованного участка данных следующего сегмента гамм  $H(2)$ .
4. Подсчет контрольной суммы участка данных, соответствующего сегменту данных  $H(2)$  и т.д.

Под контрольной суммой понимают функцию  $f(t(1), \dots, t(n))$ , где  $t(i)$  -  $i$ -е слово шифруемых данных.

Зашифруем исходный текст «абв», представленный в виде последовательности 00001 00010 00011. Пусть  $A=5$ ;  $C=3$ ;  $b=5$ ;  $M=32$ ;  $T(0)=7$ . Тогда  $T(1)=(5 \cdot 7 + 3) \bmod 32 = 6 \text{ (00110)}$ .

В качестве контрольной суммы участка данных, выберем количество единиц на этом участке. Тогда сегменту  $H(1)$  соответствует участок 00001, количество единиц равно 1.

$$T(2)=(5 \cdot 1 + 3) \bmod 32 = 8 \text{ (01000)}.$$

Контрольная сумма следующего участка (00010) равна 1.

$$T(3)=(5 \cdot 1 + 3) \bmod 32 = 8 \text{ (01000)}.$$

Полученная шифрограмма:

$$00001 \ 00010 \ 00011$$

00110 01000 01000

00111 01010 01011

что соответствует тексту «жик».

### Задание на практическую работу

1. Выбрать в таблице параметры генератора ПСЧ: А, С, Т(0), b.
2. Разработать программу шифрования и дешифрования текста.
3. Произвести шифрование исходного текста, получить шифrogramму, осуществить ее дешифрование и сравнение с исходным текстом.
4. Произвести изменение одного или несколько параметров генератора случайных чисел, осуществить получение шифrogramмы и сравнение ее с предыдущим вариантом.

### Варианты индивидуальных заданий

Таблица 1

#### Генераторы ПСЧ

№ вариан-та	Вид генератора ПСЧ	Количество разрядов <i>b</i>
1	Линейные конгруэнтные датчики ПСЧ	6
2	Гаммирование с обратной связью	7
3	Линейные конгруэнтные датчики ПСЧ	8
4	Гаммирование с обратной связью	6
5	Линейные конгруэнтные датчики ПСЧ	7
6	Гаммирование с обратной связью	8
7	Линейные конгруэнтные датчики ПСЧ	6
8	Гаммирование с обратной связью	7
9	Линейные конгруэнтные датчики ПСЧ	8
10	Гаммирование с обратной связью	6
11	Линейные конгруэнтные датчики ПСЧ	7
12	Гаммирование с обратной связью	8
13	Линейные конгруэнтные датчики ПСЧ	6
14	Гаммирование с обратной связью	7
15	Линейные конгруэнтные датчики ПСЧ	8

### Практическая работа №5 «Электронная жеребьевка»

Цель работы: изучить принципы организации и проведения электронной жеребьевки, а также научиться применять методы защиты информации при проведении жеребьевки в цифровом формате.

Задачи:

1. Изучить основные понятия и принципы проведения жеребьевки.
2. Ознакомиться с методами и технологиями проведения электронной жеребьевки.

3. Разработать алгоритм проведения электронной жеребьёвки с использованием криптографических методов защиты информации.

4. Реализовать алгоритм проведения электронной жеребьёвки в программной среде (например, используя язык программирования Python или специализированные программные продукты).

5. Проанализировать возможные угрозы безопасности при проведении электронной жеребьёвки и разработать меры по их предотвращению.

Порядок выполнения работы:

1. Изучить теоретические основы проведения жеребьёвки и её виды.

2. Выбрать метод проведения электронной жеребьёвки (например, с использованием генератора случайных чисел, блокчейн-технологии и т. д.).

3. Разработать алгоритм проведения жеребьёвки, включая этапы регистрации участников, генерации случайных чисел, определения победителей и верификации результатов.

4. Реализовать алгоритм в программной среде.

5. Протестировать алгоритм на наличие уязвимостей и возможных угроз безопасности.

6. Разработать меры по защите информации при проведении жеребьёвки (например, использование криптографических алгоритмов, аутентификации участников и т. п.).

7. Оформить отчёт, включающий в себя:

- цель и задачи работы;
- краткое описание выбранного метода проведения жеребьёвки;
- алгоритм проведения жеребьёвки;
- результаты тестирования алгоритма;
- меры по защите информации;
- выводы.

## **Практическая работа № 6**

### **«Шифрование сообщений криптосистемой *RSA*»**

*Цель работы* – ознакомиться с технологией асимметричного шифрования на примере алгоритма RSA.

*Задание на практическую работу*

Студент вводит в систему свой вариант (табл. 8.1). Параметры  $p$  и  $q$  описаны в формуле (8.1);  $e$  – открытый ключ; буква – вставляемая в конце исходного текста при необходимости буква; текст – номер исходного текста (рис. 8.1).

*Варианты лабораторной работы*

Таблица 8.1

№	$p$	$q$	$e$	Буква	Текст
1	67	53	2005	А	1
2	53	67	2501	Б	1
3	67	53	1999	В	2
4	53	67	2503	Г	2
5	67	53	1999	Д	3
6	53	67	2503	Е	3
7	67	53	2005	Ж	4
8	53	67	2501	З	4
9	83	53	1999	И	5
10	53	83	2505	Й	5
11	83	53	1999	К	4
12	53	83	2505	Л	4
13	83	53	2003	М	3
14	53	83	2505	Н	3
15	83	53	2003	О	2
16	53	83	2505	П	2
17	79	41	1999	Р	1
18	41	79	2501	С	1
19	79	41	1999	Т	2
20	41	79	2501	У	2
21	79	41	2003	Ф	3
22	41	79	2503	Х	3
23	79	41	2003	Ц	4
24	41	79	2503	Ч	4
25	67	53	2017	А	5
26	53	67	2507	Б	5
27	67	53	2021	В	4
28	53	67	2521	Г	4
29	67	53	2027	Д	3
30	53	67	2537	Е	3
31	67	53	2033	Ж	2
32	53	67	2543	З	2

### *Исходные тексты*

1. Современная государственная политика РФ в области защиты информации сформировалась в начале девяностых годов и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

2. Хотя сама информация не материальна, но она имеет материальные носители. Говоря о мере информации, выделяют ее количество и объем. Объем данных в сообщении измеряется количеством символов принятого алфавита.

3. Информатика как наука изучает свойства, структуру и функции информационных систем, основы их проектирования, создания, использования и оценки, а также информационные процессы в них происходящие.

4. Под информационной системой понимают систему, организующую, хранящую и преобразующую информацию. В этой системе основным предметом и продуктом труда является информация.

5. Под безопасностью информации понимают свойство передаваемой, накапливаемой, обрабатываемой и хранимой информации, характеризующее ее степень защищенности от дестабилизирующего воздействия внешней среды и внутренних угроз.

## **Практическая работа №7**

### **Цифровая подпись**

*Цель работы* – изучить принципы работы с цифровыми подписями и научиться применять их для обеспечения подлинности и целостности электронных документов.

Порядок выполнения работы:

1. Изучить теоретические основы работы цифровых подписей и их применения.

2. Выбрать алгоритм создания и проверки цифровой подписи (например, RSA, Elliptic Curve Cryptography – ECC и др.).

3. Реализовать алгоритм создания цифровой подписи для заданного электронного документа.

4. Реализовать алгоритм проверки цифровой подписи для заданного документа.

5. Протестировать алгоритмы на различных примерах электронных документов.

6. Разработать рекомендации по применению цифровых подписей для защиты информации при проведении электронной жеребьевки, включая этапы регистрации участников, генерации случайных чисел, определения победителей и верификации результатов.

7. Оформить отчет.

## Оценочные средства промежуточного контроля

### Билеты к зачету в 1-м семестре на 3-м курсе

Министерство науки и высшего образования  
Российской Федерации  
Федеральное государственное  
бюджетное  
образовательное учреждение  
высшего образования  
**«БАЙКАЛЬСКИЙ ГОСУДАР-  
СТВЕННЫЙ УНИВЕРСИТЕТ»**  
(ФГБОУ ВО «БГУ»)

Специальность – **38.05.02 Таможенное дело**  
Специализация – **Таможенное дело**  
Кафедра мировой экономики, предпри-  
нимательства и гуманитарных дисциплин  
Дисциплина – **«Защита информации»**

### БИЛЕТ ДЛЯ ЗАЧЁТА № 1

1. Тест (30 баллов).
2. Определите к какому типу по ограничению доступа относится информация, представленная в вашем варианте задания и объясните какие нормативно-правовые документы устанавливают этот статус. (35 баллов).
3. Определить необходимые меры защиты, регламентированные нормативно-методическими документами произвести выбор необходимых средств защиты для ситуаций, описанных в варианте задания. (35 баллов).

Составитель	_____	О.В. Гладких
Заведующий кафедрой	_____	С.А. Кравцова

### Образцы тестов, заданий

#### ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

*ОПК-2 Способен осуществлять сбор, обработку, анализ данных для решения профессиональных задач, информирования органов государственной власти и общества на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*

Знать сущность профессиональной деятельности, построенной на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Актуальность информационной безопасности.
2. Анализ защищенности и обнаружение атак.
3. Анализ защищенности информационной системы.
4. Анализ угроз информационной безопасности компьютерных систем.
5. Грифы ограничения доступа к документам.



6. Защита государственной тайны.
7. Защита коммерческой тайны.
8. Защита компьютерных систем от воздействия вредоносных программ.
9. Защита от СПАМА.
10. Защита персональных данных.

## ВОПРОСЫ ДЛЯ ПРОВЕРКИ УМЕНИЙ

*ОПК-2 Способен осуществлять сбор, обработку, анализ данных для решения профессиональных задач, информирования органов государственной власти и общества на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.*

Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Задача № 1. Определите к какому типу по ограничению доступа относится информация, представленная в вашем варианте задания и объясните какие нормативно-правовые документы устанавливают этот статус.

Задача № 2. Установите правовой статус информации со ссылкой на нормативные документы и определите какие свойства информационной безопасности следует поддерживать.

## ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ

*ОПК-2 Способен осуществлять сбор, обработку, анализ данных для решения профессиональных задач, информирования органов государственной власти и общества на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.*

Обладать навыками для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Задание № 1. В соответствии с методическими документами ФСТЭК определить параметры защищенности информации для ситуаций, представленных в варианте задания.

Задание № 2. Определить необходимые меры защиты, регламентированные нормативно-методическими документами произвести выбор необходимых средств защиты для ситуаций, описанных в варианте задания.

## Ответ 1

Для обеспечения защиты информации в новой информационной системе управления внутренними бизнес-процессами в крупной компании необходимо учесть следующие параметры защищённости в соответствии с методическими документами ФСТЭК:

**1. Уровень защиты от несанкционированного доступа:**

- Реализация многофакторной аутентификации для доступа к системе.
- Разграничение прав доступа на основе ролей и обязанностей пользователей.
- Использование шифрованных каналов передачи данных.
- Мониторинг и регистрация всех попыток доступа к системе для последующего анализа.
- Внедрение системы обнаружения и предотвращения вторжений (IDS/IPS).

**2. Целостность данных:**

- Применение алгоритмов хеширования и цифровых подписей для проверки целостности передаваемых и хранимых данных.
- Регулярное резервное копирование данных с использованием надёжных методов хранения (например, географически распределённых хранилищ).
- Механизмы контроля версий и аудита изменений данных.
- Шифрование данных для предотвращения их несанкционированного изменения.

**3. Возможность восстановления системы после сбоев:**

- Разработка и внедрение плана восстановления работоспособности системы (DRP) с учётом различных сценариев сбоев (например, аппаратные отказы, сетевые проблемы, DDoS-атаки).
- Автоматическое переключение на резервные серверы или каналы связи.
- Тестирование плана восстановления работоспособности системы на регулярной основе.
- Хранение резервных копий в надёжных и защищённых местах.

**4. Защита конфиденциальной информации:**

- Классификация информации по уровням конфиденциальности и применение соответствующих мер защиты.
- Внедрение средств криптографической защиты для передачи и хранения конфиденциальных данных.
- Обучение сотрудников правилам работы с конфиденциальной информацией и мерам по её защите.
- Проведение регулярных проверок соответствия системы требованиям ФСТЭК и других регуляторных органов.

**5. Соответствие требованиям методических документов ФСТЭК:**

- Анализ и оценка рисков информационной безопасности с учётом специфики компании и её бизнес-процессов.
- Разработка и внедрение политик информационной безопасности, соответствующих требованиям ФСТЭК.
- Проведение сертификационных и аттестационных мероприятий для подтверждения соответствия системы требованиям безопасности.

## **Ответ 2**

Для обеспечения защиты информации в новой информационной системе управления внутренними бизнес-процессами необходимо учесть ряд мер и выбрать соответствующие средства защиты. Вот как это может выглядеть:

**1. Уровень защиты от несанкционированного доступа:**

- **Многофакторная аутентификация:** использование аппаратных токенов, биометрических данных, одноразовых паролей и других методов для подтверждения личности пользователя. Средства: двухфакторная аутентификация (например, Google Authenticator, RSA SecurID).
- **Разграничение прав доступа:** системы управления доступом, такие как Microsoft Active Directory, Oracle Identity Management.
- **Шифрованные каналы передачи данных:** протоколы SSL/TLS для веб-трафика, IPsec для VPN-соединений.
- **Мониторинг и регистрация попыток доступа:** системы SIEM (Security Information and Event Management), например, Splunk, ArcSight.
- **Система обнаружения и предотвращения вторжений (IDS/IPS):** решения типа Snort, Suricata, Cisco IPS.

## 2. Целостность данных:

- **Алгоритмы хеширования и цифровые подписи:** использование SHA-2, RSA, ECDSA для проверки целостности данных. Средства: OpenSSL, Java Cryptography Architecture.
- **Резервное копирование данных:** системы резервного копирования и восстановления данных, например, Veeam Backup & Replication, Veritas Backup Exec.
- **Механизмы контроля версий:** системы управления версиями, такие как Git, SVN.
- **Шифрование данных:** инструменты шифрования, например, VeraCrypt, BitLocker для шифрования дисков, а также библиотеки и фреймворки для шифрования данных в приложениях (например, библиотеки openssl в языках программирования).

## 3. Возможность восстановления системы после сбоев:

- **План восстановления работоспособности системы (DRP):** разработка и тестирование DRP с использованием инструментов для управления инцидентами, таких как ServiceNow, BMC Atrium.
- **Автоматическое переключение на резервные серверы:** использование решений для балансировки нагрузки и отказоустойчивости, например, Cisco Catalyst, F5 Big-IP.
- **Тестирование плана восстановления:** регулярное тестирование DRP с помощью инструментов для тестирования катастрофоустойчивости, таких как TestComplete, Tricentis.

## 4. Защита конфиденциальной информации:

- **Классификация информации:** системы управления классификацией информации, например, IBM Security QRadar SIEM.
- **Средства криптографической защиты:** инструменты для шифрования данных, такие как TLS-шифрование для передачи данных, BitLocker для защиты хранимых данных.
- **Обучение сотрудников:** проведение тренингов и семинаров по информационной безопасности с использованием платформ для дистанционного обучения (например, Moodle, Zoom для онлайн-семинаров).
- **Регулярные проверки соответствия:** использование инструментов для аудита и мониторинга соответствия требованиям регуляторов, например, OpenSCAP, Nessus.

## 5. Соответствие требованиям методических документов ФСТЭК:

- **Анализ и оценка рисков:** использование методов и инструментов для анализа рисков, например, CRAMM, OCTAVE.
- **Разработка и внедрение политик информационной безопасности:** инструменты для создания и управления политиками безопасности, например, IBM Security QRadar SIEM, Microsoft Group Policy.
- **Сертификационные и аттестационные мероприятия:** использование инструментов для проведения сертификационных и аттестационных испытаний, например, специализированных программных комплексов для тестирования на соответствие требованиям безопасности.

### *Тестовые задания*

№	Характеристика задания	Варианты ответов	Ключ
1.	<p><i>Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Как называется процесс преобразования данных в нечитабельный формат для защиты информации?</p>	Ваш ответ: ____	Шифрование
2.	<p><i>Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Какой термин описывает слабое место в системе, которое может быть использовано злоумышленником?</p>	Ваш ответ: ____	Уязвимость
3.	<p><i>Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Какой термин описывает событие, угрожающее безопасности информации?</p>	Ваш ответ: ____	Инцидент
4.	<p><i>Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Как называется документ, определяющий правила и процедуры по обеспечению безопасности информации?</p>	Ваш ответ: ____	Политика
5.	<p><i>Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Какой тип шифрования ис-</p>	Ваш ответ: ____	Симметричное

	пользует один ключ для шифрования и дешифрования?		
6.	<i>Прочитайте текст и запишите развернутый обоснованный ответ</i>  Какой метод аутентификации использует два различных фактора для подтверждения личности?	Ваш ответ: ____	Двухфакторная
7.	<i>Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа</i>  Какой из следующих терминов описывает слабое место в системе, которое может быть использовано злоумышленником?	1. Уязвимость 2. Риск 3. Инцидент 4. Политика безопасности  Ваш ответ: ____	1
8.	<i>Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа</i>  Какой из следующих методов используется для оценки и анализа системы безопасности?	1. Аудит безопасности 2. Шифрование 3. Резервное копирование 4. Аутентификация  Ваш ответ: ____	1
9.	<i>Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа</i>  Какой из следующих методов аутентификации является наиболее безопасным?	1. Пароль 2. Двухфакторная аутентификация 3. Ответ на секретный вопрос 4. Биометрическая аутентификация  Ваш ответ: ____	2
10.	<i>Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа</i>  Какой из следующих инструментов используется для защиты сети от несанкционированного доступа?	1. Антивирус 2. Файрвол 3. Шифратор 4. Резервное копирование  Ваш ответ: ____	2
11.	<i>Прочитайте текст, выберите</i>	1. Асимметричное шифрование	2

	<p>те правильный ответ и запишите аргументы, обосновывающие выбор ответа</p> <p>Какой из следующих типов шифрования использует один ключ для шифрования и дешифрования?</p>	<p>2. Симметричное шифрование</p> <p>3. Хеширование</p> <p>4. Потокное шифрование</p> <p>Ваш ответ: _____</p>						
12.	<p>Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа</p> <p>Какой из следующих терминов описывает событие, угрожающее безопасности информации?</p>	<p>1. Инцидент безопасности</p> <p>2. Уязвимость</p> <p>3. Риск</p> <p>4. Политика безопасности</p> <p>Ваш ответ: _____</p>	1					
13.	<p>Прочитайте текст и установите последовательность</p> <p>Установите правильную последовательность этапов процесса защиты информации:</p>	<p>1. Оценка рисков</p> <p>2. Разработка политики безопасности</p> <p>3. Реализация мер защиты</p> <p>4. Мониторинг и аудит</p> <p>5. Обучение сотрудников</p> <p>Запишите соответствующую последовательность цифр слева направо:</p> <table><tr><td></td><td></td><td></td><td></td><td></td></tr></table>						21354
14.	<p>Прочитайте текст и установите последовательность</p> <p>Установите правильную последовательность действий при реагировании на инциденты безопасности:</p>	<p>1. Уведомление заинтересованных сторон</p> <p>2. Идентификация инцидента</p> <p>3. Анализ инцидента</p> <p>4. Устранение последствий</p> <p>5. Документирование инцидента</p> <p>Запишите соответствующую последовательность цифр слева направо:</p> <table><tr><td></td><td></td><td></td><td></td><td></td></tr></table>						23415
15.	<p>Прочитайте текст и установите последовательность</p> <p>Расположите этапы процесса криптографической защиты информации в порядке их выполнения:</p>	<p>1. выбор алгоритма шифрования;</p> <p>2. проверка целостности зашифрованных данных;</p> <p>3. генерация ключа;</p> <p>4. шифрование данных.</p> <p>Запишите соответствующую последовательность цифр слева направо:</p> <table><tr><td></td><td></td><td></td><td></td></tr></table>					1342	
16.	<p>Прочитайте текст и установите последовательность</p>	<p>1. мониторинг и аудит информационной системы;</p> <p>2. определение угроз информационной безопасности;</p>	2431					

	<p>Установите последовательность этапов при организации защиты информации в таможенной службе:</p>	<p>3. внедрение технических средств защиты;</p> <p>4. разработка политики информационной безопасности.</p> <p>Запишите соответствующую последовательность цифр слева направо:</p> <table border="1"> <tr> <td></td><td></td><td></td><td></td> </tr> </table>																									
17.	<p><i>Прочитайте текст и установите последовательность</i></p> <p>Установите правильную последовательность действий при управлении доступом к информации:</p>	<p>1. Определение уровней доступа</p> <p>2. Отзыв доступа</p> <p>3. Авторизация доступа</p> <p>4. Мониторинг доступа</p> <p>5. Аутентификация пользователей</p> <p>Запишите соответствующую последовательность цифр слева направо:</p> <table border="1"> <tr> <td></td><td></td><td></td><td></td> </tr> </table>					15342																				
18.	<p><i>Прочитайте текст и установите последовательность</i></p> <p>Установите правильную последовательность действий при создании резервной копии данных:</p>	<p>1. Определение данных для резервирования</p> <p>2. Проверка целостности резервной копии</p> <p>3. Проведение резервного копирования</p> <p>4. Выбор метода резервирования</p> <p>5. Хранение резервной копии</p> <p>Запишите соответствующую последовательность цифр слева направо:</p> <table border="1"> <tr> <td></td><td></td><td></td><td></td> </tr> </table>					14325																				
19.	<p><i>Прочитайте текст и установите соответствие</i></p> <p>Установите соответствие между терминами и их определениями</p>	<p>К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:</p> <table border="1"> <thead> <tr> <th colspan="2">Термин</th><th colspan="2">Определение</th></tr> </thead> <tbody> <tr> <td>А</td><td>Шифрование</td><td>1</td><td>Процесс проверки подлинности пользователя или системы</td></tr> <tr> <td>Б</td><td>Аутентификация</td><td>2</td><td>Процесс защиты данных путем преобразования их в нечитабельный формат</td></tr> <tr> <td>В</td><td>Авторизация</td><td>3</td><td>Процесс предоставления прав доступа к ресурсам после аутентификации</td></tr> <tr> <td>Г</td><td>Резервное копирование</td><td>4</td><td>Процесс создания копий данных для их восстановления в случае потери</td></tr> <tr> <td></td><td></td><td>5</td><td>Событие, которое</td></tr> </tbody> </table>	Термин		Определение		А	Шифрование	1	Процесс проверки подлинности пользователя или системы	Б	Аутентификация	2	Процесс защиты данных путем преобразования их в нечитабельный формат	В	Авторизация	3	Процесс предоставления прав доступа к ресурсам после аутентификации	Г	Резервное копирование	4	Процесс создания копий данных для их восстановления в случае потери			5	Событие, которое	A2Б1В3Г 4
Термин		Определение																									
А	Шифрование	1	Процесс проверки подлинности пользователя или системы																								
Б	Аутентификация	2	Процесс защиты данных путем преобразования их в нечитабельный формат																								
В	Авторизация	3	Процесс предоставления прав доступа к ресурсам после аутентификации																								
Г	Резервное копирование	4	Процесс создания копий данных для их восстановления в случае потери																								
		5	Событие, которое																								

		<table><tr><td></td><td></td><td></td><td>может угрожать без опасности информации</td></tr><tr><td colspan="4">Запишите выбранные цифры под соответствующими буквами:</td></tr><tr><td>A</td><td>Б</td><td>В</td><td>Г</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>				может угрожать без опасности информации	Запишите выбранные цифры под соответствующими буквами:				A	Б	В	Г																			
			может угрожать без опасности информации																														
Запишите выбранные цифры под соответствующими буквами:																																	
A	Б	В	Г																														
20.Прочитайте текст и установите соответствие	Установите соответствие между стандартами и их описаниями	<p>К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:</p> <table><tr><th colspan="2">Стандарт</th><th colspan="2">Описание</th></tr><tr><td>A</td><td>ISO/IEC 27001</td><td>1</td><td>Стандарт для защиты персональных данных в Европе</td></tr><tr><td>Б</td><td>NIST SP 800-53</td><td>2</td><td>Стандарт для защиты информации в здравоохранении</td></tr><tr><td>В</td><td>GDPR</td><td>3</td><td>Стандарт для защиты платежной информации</td></tr><tr><td>Г</td><td>PCI DSS</td><td>4</td><td>Рекомендации по управлению безопасностью информации</td></tr><tr><td></td><td></td><td>5</td><td>Стандарт для систем управления информационной безопасностью</td></tr></table> <p>Запишите выбранные цифры под соответствующими буквами:</p> <table><tr><td>A</td><td>Б</td><td>В</td></tr><tr><td></td><td></td><td></td></tr></table>	Стандарт		Описание		A	ISO/IEC 27001	1	Стандарт для защиты персональных данных в Европе	Б	NIST SP 800-53	2	Стандарт для защиты информации в здравоохранении	В	GDPR	3	Стандарт для защиты платежной информации	Г	PCI DSS	4	Рекомендации по управлению безопасностью информации			5	Стандарт для систем управления информационной безопасностью	A	Б	В				A5Б4В1Г 3
Стандарт		Описание																															
A	ISO/IEC 27001	1	Стандарт для защиты персональных данных в Европе																														
Б	NIST SP 800-53	2	Стандарт для защиты информации в здравоохранении																														
В	GDPR	3	Стандарт для защиты платежной информации																														
Г	PCI DSS	4	Рекомендации по управлению безопасностью информации																														
		5	Стандарт для систем управления информационной безопасностью																														
A	Б	В																															
21.Прочитайте текст и установите соответствие	Установите соответствие между методами защиты информации и их описаниями	<p>К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:</p> <table><tr><th colspan="2">Метод</th><th colspan="2">Описание</th></tr><tr><td>A</td><td>Антивирус</td><td>1</td><td>Процесс проверки подлинности пользователя</td></tr><tr><td>Б</td><td>Шифрование</td><td>2</td><td>Программа для защиты от вредоносного ПО</td></tr><tr><td>В</td><td>Аутентификация</td><td>3</td><td>Защита сети от не санкционированного</td></tr></table>	Метод		Описание		A	Антивирус	1	Процесс проверки подлинности пользователя	Б	Шифрование	2	Программа для защиты от вредоносного ПО	В	Аутентификация	3	Защита сети от не санкционированного	A2Б5В1Г 4														
Метод		Описание																															
A	Антивирус	1	Процесс проверки подлинности пользователя																														
Б	Шифрование	2	Программа для защиты от вредоносного ПО																														
В	Аутентификация	3	Защита сети от не санкционированного																														



		<table> <tr> <td></td><td></td><td></td><td>доступа</td></tr> <tr> <td>Г</td><td>Резервное копирование</td><td>4</td><td>Процесс создания копий данных для восстановления</td></tr> <tr> <td></td><td></td><td>5</td><td>Процесс преобразования данных в табельный формат</td></tr> </table> <p>Запишите выбранные цифры под соответствующими буквами:</p> <table> <tr> <td>А</td><td>Б</td><td>В</td><td>Г</td></tr> <tr> <td></td><td></td><td></td><td></td></tr> </table>				доступа	Г	Резервное копирование	4	Процесс создания копий данных для восстановления			5	Процесс преобразования данных в табельный формат	А	Б	В	Г																	
			доступа																																
Г	Резервное копирование	4	Процесс создания копий данных для восстановления																																
		5	Процесс преобразования данных в табельный формат																																
А	Б	В	Г																																
22.Прочитайте текст и установите соответствие	<p>Установите соответствие между типами атак и их описаниями</p>	<p>К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:</p> <table> <tr> <th colspan="2">Тип атаки</th><th colspan="2">Описание</th></tr> <tr> <td>А</td><td>Фишинг</td><td>1</td><td>Атака, направленная на перегрузку сервера</td></tr> <tr> <td>Б</td><td>DDoS-атака</td><td>2</td><td>Использование поддельных сообщений для получения конфиденциальной информации</td></tr> <tr> <td>В</td><td>Вредоносное ПО</td><td>3</td><td>Программное обеспечение, предназначенное для нанесения вреда системе</td></tr> <tr> <td>Г</td><td>Социальная инженерия</td><td>4</td><td>Метод, использующий манипуляции для обмана пользователей</td></tr> <tr> <td></td><td></td><td>5</td><td>Вставка вредоносного кода в запросы к базе данных</td></tr> </table> <p>Запишите выбранные цифры под соответствующими буквами:</p> <table> <tr> <td>А</td><td>Б</td><td>В</td><td>Г</td></tr> <tr> <td></td><td></td><td></td><td></td></tr> </table>	Тип атаки		Описание		А	Фишинг	1	Атака, направленная на перегрузку сервера	Б	DDoS-атака	2	Использование поддельных сообщений для получения конфиденциальной информации	В	Вредоносное ПО	3	Программное обеспечение, предназначенное для нанесения вреда системе	Г	Социальная инженерия	4	Метод, использующий манипуляции для обмана пользователей			5	Вставка вредоносного кода в запросы к базе данных	А	Б	В	Г					<p>A2Б1В3Г 4</p>
Тип атаки		Описание																																	
А	Фишинг	1	Атака, направленная на перегрузку сервера																																
Б	DDoS-атака	2	Использование поддельных сообщений для получения конфиденциальной информации																																
В	Вредоносное ПО	3	Программное обеспечение, предназначенное для нанесения вреда системе																																
Г	Социальная инженерия	4	Метод, использующий манипуляции для обмана пользователей																																
		5	Вставка вредоносного кода в запросы к базе данных																																
А	Б	В	Г																																
23.Прочитайте текст и установите соответствие	<p>Установите соответствие между терминами и их характеристиками</p>	<p>К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:</p> <table> <tr> <th colspan="2">Термин</th><th colspan="2"></th></tr> <tr> <td>А</td><td>Уязвимость</td><td>1</td><td>Оценка и анализ системы безопасности</td></tr> <tr> <td>Б</td><td>Риск</td><td>2</td><td>Слабое место в системе, которое может быть использовано злоумышленником</td></tr> <tr> <td>В</td><td>Инцидент</td><td>3</td><td>Вероятность возникновения угрозы</td></tr> <tr> <td>Г</td><td>Политика безопасности</td><td>4</td><td>Событие, угрожающее безопасности</td></tr> </table>	Термин				А	Уязвимость	1	Оценка и анализ системы безопасности	Б	Риск	2	Слабое место в системе, которое может быть использовано злоумышленником	В	Инцидент	3	Вероятность возникновения угрозы	Г	Политика безопасности	4	Событие, угрожающее безопасности	<p>A2Б3В4Г 5</p>												
Термин																																			
А	Уязвимость	1	Оценка и анализ системы безопасности																																
Б	Риск	2	Слабое место в системе, которое может быть использовано злоумышленником																																
В	Инцидент	3	Вероятность возникновения угрозы																																
Г	Политика безопасности	4	Событие, угрожающее безопасности																																

		5	Документ, определяющий правила												
		Запишите выбранные цифры под соответствующими буквами:													
		А	Б В Г												
24.Прочитайте текст и установите соответствие	К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:	A1Б3В2Г4													
Установите соответствие между типами шифрования и их описаниями	<table><tr><th>Тип шифрования</th><th>Описание</th></tr><tr><td>А Симметричное шифрование</td><td>1 Использует один ключ для шифрования и дешифрования</td></tr><tr><td>Б Асимметричное шифрование</td><td>2 Преобразует данные в фиксированную длину</td></tr><tr><td>В Хеширование</td><td>3 Использует пару ключей (открытый и закрытый)</td></tr><tr><td>Г Шифрование на основе блоков</td><td>4 Шифрует данные по блокам фиксированного размера</td></tr><tr><td></td><td>5 Шифрует данные по одному биту или байту</td></tr></table>	Тип шифрования	Описание	А Симметричное шифрование	1 Использует один ключ для шифрования и дешифрования	Б Асимметричное шифрование	2 Преобразует данные в фиксированную длину	В Хеширование	3 Использует пару ключей (открытый и закрытый)	Г Шифрование на основе блоков	4 Шифрует данные по блокам фиксированного размера		5 Шифрует данные по одному биту или байту		
Тип шифрования	Описание														
А Симметричное шифрование	1 Использует один ключ для шифрования и дешифрования														
Б Асимметричное шифрование	2 Преобразует данные в фиксированную длину														
В Хеширование	3 Использует пару ключей (открытый и закрытый)														
Г Шифрование на основе блоков	4 Шифрует данные по блокам фиксированного размера														
	5 Шифрует данные по одному биту или байту														
	Запишите выбранные цифры под соответствующими буквами:														
		А	Б В Г												
25.Прочитайте текст, выберите один или несколько правильных вариантов ответов и запишите аргументы, обосновывающие выбор ответов	<ol style="list-style-type: none"><li>1. Антивирус</li><li>2. Файрвол</li><li>3. IDS (Система обнаружения вторжений)</li><li>4. VPN (Виртуальная частная сеть)</li><li>5. Резервное копирование</li></ol>	124													
Какие из следующих инструментов используются для защиты сети от несанкционированного доступа?															
26.Прочитайте текст, выберите один или несколько правильных вариантов ответов	<ol style="list-style-type: none"><li>1. Идентификация инцидента</li><li>2. Устранение последствий</li><li>3. Документирование инцидента</li></ol>	123													

	<p><i>и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Какие из следующих действий являются частью процесса реагирования на инциденты безопасности?</p>	<p>4. Обучение сотрудников</p> <p>5. Оценка рисков</p>	
27.	<p><i>Прочитайте текст, выберите один или несколько правильных вариантов ответов и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Какие из следующих аспектов относятся к управлению рисками в области безопасности информации?</p>	<p>1. Идентификация рисков</p> <p>2. Оценка рисков</p> <p>3. Разработка стратегии управления рисками</p> <p>4. Реализация мер защиты</p>	1234
28.	<p><i>Прочитайте текст, выберите один или несколько правильных вариантов ответов и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Какие из следующих аспектов относятся к управлению доступом к информации?</p>	<p>1. Аутентификация пользователей</p> <p>2. Авторизация доступа</p> <p>3. Мониторинг активности пользователей</p> <p>4. Шифрование данных</p> <p>5. Резервное копирование данных</p>	123
29.	<p><i>Прочитайте текст, выберите один или несколько правильных вариантов ответов и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Какие из следующих действий могут помочь в обеспечении физической безопасности информации? (Выберите все подходящие варианты)</p>	<p>1. Использование замков и систем контроля доступа</p> <p>2. Установка видеонаблюдения</p> <p>3. Шифрование данных</p> <p>4. Обучение сотрудников по вопросам безопасности</p> <p>5. Регулярные проверки помещений</p>	1245
30.	<p><i>Прочитайте текст, выберите один или несколько правильных вариантов ответов и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Какие из следующих методов</p>	<p>1. Антивирусные программы</p> <p>2. Файрволы</p> <p>3. Регулярные обновления программного обеспечения</p> <p>4. Использование сложных паролей</p> <p>5. Обучение пользователей</p>	1235

	могут использоваться для защиты от вредоносного ПО?		
--	---	--	--

**Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Система критериев оценки определяет оценку успеваемости по каждому заданию (вопросу) экзаменационного билета или заданию для зачета с использованием интервальной шкалы баллов, применяемой в привязке к рейтинговой 100-балльной системе.

**ОЦЕНКА ОТВЕТА НА ТЕОРЕТИЧЕСКИЙ ВОПРОС В УСТНОЙ ИЛИ ПИСЬМЕННОЙ ФОРМЕ:**

Оценка «отлично» / «зачтено» (91-100 баллов) выставляется при соблюдении следующих условий: Ответ отличается глубиной и полнотой, свободным владением понятийно-категориальным (терминологическим) аппаратом изученной дисциплины. Отражает знание не только основной, но и дополнительной литературы. Приведены примеры, отражающие умение связать теорию с практикой. Ответ изложен логически последовательно, грамотно и корректно.

Оценка «хорошо» / «зачтено» (76-90 баллов) выставляется при соблюдении следующих условий: Ответ отличается полнотой, владением понятийно-категориальным (терминологическим) аппаратом изученной дисциплины, но в ответе могут присутствовать неточности. Отражает знание основной литературы. Приведены примеры, отражающие умение связать теорию с практикой. Ответ изложен логически последовательно, грамотно и корректно, но недостаточно аргументирован.

Оценка «удовлетворительно» / «зачтено» (61-75 баллов) выставляется при соблюдении следующих условий: В ответе отражено знание понятийно-категориального (терминологического) аппарата изучаемой дисциплины, но присутствуют отдельные ошибки и неточности. Ответ характеризуется недостаточным знанием рекомендованной литературы. Примеры, отражающие умение связать теорию с практикой, тривиальны, либо отсутствуют. Ответ неполный, носит фрагментарный, непоследовательный характер.

Оценка «неудовлетворительно» / «не зачтено» (0-60 баллов) выставляется при соблюдении следующих условий: Ответ характеризуется незнанием, либо фрагментарным представлением о понятийно-категориальном аппарате дисциплины, содержит множество ошибок. Примеры и иллюстрации отсутствуют. Ответ логически непоследователен.

**ОЦЕНКА ВЫПОЛНЕНИЯ ТЕСТОВОГО ЗАДАНИЯ**

**Подсчитывается доля набранных баллов в максимальной сумме баллов за все задания теста:**

– Каждый правильный ответ на тестовый вопрос (тип выборочный, одинарный, множественный, открытый) оценивается в  $m$  баллов (число  $m$  определяется путем деления максимального количества баллов за выполнение теста в структуре экзаменационного билета/задания на количество тестовых заданий);

– Каждый частично правильный ответ на тестовый вопрос (тип выборочный, множественный, открытый) оценивается в  $m/2$  баллов независимо от соотношения правильно/неправильно выбранных вариантов (число  $m$  определяется путем деления максимального количества баллов за выполнение теста в структуре экзаменационного билета/задания на количество тестовых заданий);

– Каждый неправильный ответ на тестовый вопрос (тип выборочный, одинарный) оценивается в 0 баллов.

Оценка «отлично»/ «зачтено» (91-100 баллов) выставляется, если доля набранных баллов составляет 91-100%.

Оценка «хорошо»/ «зачтено» (76-90 баллов), если доля набранных баллов составляет 76-90%.

Оценка «удовлетворительно»/ «зачтено» (61-75 баллов), если доля набранных баллов составляет 61-75%.

Оценка «неудовлетворительно»/ «не зачтено» (0-60 баллов), если доля набранных баллов составляет не более 60%.