

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ  
по выполнению лабораторных работ  
по дисциплине «Технологии защиты информации в таможенных органах»  
для студентов специальности 38.05.02 «Таможенное дело»

Ставрополь  
2026

Методические указания составлены в соответствии с программой дисциплины «Технологии защиты информации в таможенных органах» для студентов специальности 38.05.02 Таможенное дело и предназначены для оказания помощи студентам при подготовке к лабораторным занятиям.

## СОДЕРЖАНИЕ

Введение.....	4
1 Общие положения.....	6
2 Планы лабораторных занятий.....	9
3 Литература и информационное обеспечение.....	16

## ВВЕДЕНИЕ

Цель освоения дисциплины заключается в изучении студентами методологических и организационно-правовых основ защиты информации в таможенных органах.

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-4. Способен совершать таможенные операции, проводить таможенный контроль и осуществлять иные виды государственного контроля	ИД-4. ПК-4. Применяет информационные системы, таможенные технологии и технические средства при проведении таможенного контроля и осуществлении иных видов государственного контроля, отнесенных к компетенции таможенных органов	Применяет информационные системы, таможенные технологии и технические средства при проведении таможенного контроля

Освоение данного курса определяет следующие задачи:

- изучить методологические основы и практические принципы исследования проблем информационной безопасности и защиты информации в таможенных органах;
- изучить основные методы и системы защиты информации различных направлений обеспечения информационной безопасности в таможенных органах;
- изучить основные методы и модели управления информационной безопасностью и защиты информации в таможенных органах;
- подготовить студентов к применению полученных знаний для анализа моделей объектов и формирования моделей и методов управления и обеспечения информационной безопасности объектов таможенных органов.

Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы представлен в таблице 1.

Таблица 1 – Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

## 1 ОБЩИЕ ПОЛОЖЕНИЯ

Лабораторное занятие является одной из форм проведения групповых занятий со студентами, имеющей своими целями более глубокое усвоение обучаемыми лекционного материала, развитие у них умения целенаправленной работы с научной, учебной литературой для самостоятельного добывания новых знаний, приобретение навыков публичных выступлений, ведения дискуссий и т.д.

Лабораторные занятия предполагают использование различных форм работы: обсуждение теоретических вопросов, решение задач, обсуждение докладов, анализ информации. Лабораторные занятия проводятся с целью углубления и закрепления теоретических знаний, привития навыков анализа обстоятельств дела в конкретно заданной ситуации, что весьма важно для будущей практической деятельности. Они, являясь самостоятельной формой обучения студентов, углубляют знания, полученные на лекциях, способствуют самостоятельной работе с нормативным материалом, опубликованной практикой и литературой.

Занятия проводятся в форме опроса студентов по теоретическим вопросам, обозначенным в планах, а также обсуждения вариантов решения практических заданий (ситуаций), которые были предложены в качестве подготовки к занятию. Готовясь к занятиям, студенты должны изучить:

- материалы лекции по предполагаемой теме, а также план лабораторного занятия;
- соответствующие теме занятия положения нормативно-правовых актов;
- основные положения теории;
- материалы руководящих постановлений таможенных органов; рекомендованную в планах практических занятий базовую, а также дополнительную литературу и методические разработки для студентов, подготовленные кафедрой.

При подготовке к лабораторному занятию студент обязан, изучив действующее законодательство и рекомендованную литературу, письменно изложить в специальной тетради решение задач, заданных преподавателем.

Их изложение не должно сводиться лишь к краткому ответу на вопрос.

Необходимым признается такое обоснование вывода, которое в принципе является доказательным. Для решения таких задач соответственно требуется овладение техникой поиска предписаний, техникой субсумпции, то есть подведения менее общей посылки под общую, толкования закона и его конкретизации.

Лабораторные занятия строятся по следующей схеме:

- вначале преподаватель объявляет тему и задачи занятия;
- производит опрос студентов по теоретическим вопросам, обозначенным в плане занятия, а также проверяет наличие у студентов письменных решений задач. Данные решения обсуждаются в форме дискуссии непосредственно на занятии;
- по окончании занятия подводятся итоги дискуссии и общие итоги.

Применительно к отдельным темам занятия, с учетом специфики обсуждаемой темы,

указанная схема может корректироваться. Однако основе занятия, в любом случае, лежит решение практических ситуаций. Их количество определяется преподавателем с учетом всех особенностей изучаемой темы и масштабности ее проблемных вопросов.

Отвечающий на практическом занятии студент обязан кратко изложить содержание практической ситуации.

Лучше всего целенаправленно готовиться к выступлению по определенному вопросу, изучая другие вопросы с целью лучше разобраться в предмете выступления. Темы выступлений (докладов) можно согласовать с преподавателем заранее. Докладчики могут разграничить между собой материал, вопросы, согласовать последовательность выступлений. Чтобы во время выступления чувствовать себя увереннее, следует подготовить опорный конспект в виде развернутого плана, в который можно включить также представляемые в выступлении схемы, определения, формулы, графики и др. На практическом занятии можно сделать не обязательно большое, развернутое выступление, полностью раскрывающее какой-либо вопрос, но и небольшое дополнение, уточнение, задавать вопросы в процессе обсуждения.

Если не удалось выступить на практическом занятии, следует подготовить письменную работу по согласованию с преподавателем. Это может быть:

- словарь терминов,
- графики с комментариями,
- формулы с комментариями и примерами,
- структурно-логические схемы,
- развернутые планы ответов на вопросы темы,
- аннотации статей по теме практического занятия (краткое, не более 1 стр., самостоятельное изложение содержания статьи) и др.

Конспекты лекций, опорные конспекты к выступлениям и другие записи по изучаемому предмету целесообразно группировать по темам и накапливать для подготовки к зачету (экзамену) в специальной папке.

Планирование лабораторных занятий осуществляется с учётом установленного количества часов. Основные этапы планирования и подготовки занятий:

- разработка системы занятий по теме или разделу;
- определение задач и целей занятия;
- определение оптимального объема учебного материала, расчленение на ряд законченных в смысловом отношении блоков, частей;
- разработка структуры занятия, определение его типа и методов обучения. нахождение связей данного материала с другими дисциплинами и использование этих связей при изучении нового материала;
- определение объема и форм самостоятельной работы на занятии. определение форм и методов контроля знаний студентов. определение формы подведения итогов;
- определение самостоятельной работы по данной теме.

При проведении лабораторных занятий преподаватель уделяет внимание формулировкам выводов, способности студентов сравнивать, анализировать, находить несоответствия, оценивает уровень знаний студентов.

При подведении итогов преподаватель знакомит студентов с результатами выполнения заданий, оценивает качество выполненной работы каждым студентом.

Студенты, не подготовившиеся к практическому занятию, равно как и не имеющие письменных решений каких-либо практических ситуаций, заданных преподавателем, должны в отдельном порядке отчитаться за занятие.

После развернутого обсуждения всех наиболее важных вопросов занятия, а также вопросов, касающихся казусов и вариантов его решения, преподаватель подводит итоги дискуссии.

## 2 ПЛАНЫ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Тема 1. Общие положения об информации и защите информации в таможенных органах РФ

Цель: формирование общих представлений об изучаемой дисциплине, об общих положениях об информации и защите информации.

Знания и умения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций или их части:

- знать сущность, виды информации, сбор, хранение, преобразование и передача информации, способы и средства передачи информации, информация и действия с информацией в таможенных органах РФ, цели защиты информации в таможенных органах РФ, виды угроз и методов защиты информации;
- уметь различать и классифицировать информацию;
- владеть навыками работы с нормативно-правовой документацией.

Актуальность темы обусловлена необходимостью приобретения соответствующих компетенций по данной дисциплине.

Теоретическая часть

Развивающиеся информационные технологии быстро внедряются во все сферы человеческого общества. Информация теперь официально определена идеальным объектом, имеющим ценность и стоимость как обычный продукт, стоимость которого обычно во много раз превосходит стоимость компьютерной системы, в которой она хранится и обрабатывается.

В связи с этим необходимо принимать во внимание возможные злонамеренные воздействия со стороны злоумышленников по отношению к информационным системам. Например, нарушитель может пытаться выдать себя за другого пользователя, прослушать канал связи, перехватить и модифицировать информацию, которой обмениваются пользователи системы, расширить свои полномочия для получения доступа к информации, к которой ему представлен только частичный доступ, попытаться разрушить систему. Интенсивное развитие открытых компьютерных сетей привлекает все большее внимание пользователей. Сеть предоставляет злоумышленникам множество возможностей для вторжения во внутренние сети компаний и организаций с целью хищения, искажения или разрушения конфиденциальной информации.

Вопросы для обсуждения

1. Сущность, виды информации
2. Сбор, хранение, преобразование и передача информации
3. Способы и средства передачи информации
4. Информация и действия с информацией в таможенных органах РФ
5. Цели защиты информации в таможенных органах РФ

Контрольные вопросы и задания

1. Выполнить прикладную работу: с помощью справочно-правовой системы Консультант Плюс найти, открыть и ознакомиться с содержанием нормативно-правовых документов, в которых раскрываются теоретические положения.

2. Какие виды информации выделяют?

3. Каковы цели защиты информации в таможенных органах РФ?

4. Каковы основные нормативно-правовые документы о защите информации в таможенных органах РФ?

Рекомендуемый список литературы по теме (№ источника):

– основная: 1-2;

– дополнительная: 1-3;

– интернет-источники: 1-8.

## Тема 2. Угрозы информационной безопасности

Цель: формирование общих представлений об угрозах информационной безопасности.

Знания и умения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций или их части:

– знать классификации угроз информационной безопасности, механизм действия отдельных видов угроз;

– уметь анализировать угрозы информационной безопасности;

– владеть навыками работы с нормативно-правовой документацией, стандартными программными средствами.

Актуальность темы обусловлена необходимостью приобретения соответствующих компетенций по данной дисциплине.

### Теоретическая часть

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации.

Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным. Само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнута открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

### Вопросы для обсуждения

1. Классификации угроз информационной безопасности

## 2. Механизм действия отдельных видов угроз

### Контрольные вопросы и задания

1. Выполнить прикладную работу: 1) с помощью справочно-правовой системы Консультант Плюс найти, открыть и ознакомиться с содержанием нормативно-правовых документов, в которых раскрываются теоретические положения, 2) с помощью стандартного программного обеспечения отразить в виде схемы все актуальные угрозы информационной безопасности в таможенных органах РФ, 3) с помощью стандартного программного обеспечения отразить в виде схемы действие одной на выбор вредоносной программы

2. Какие виды угроз информационной безопасности существуют?

Рекомендуемый список литературы по теме (№ источника):

- основная: 1-2;
- дополнительная: 1-3;
- интернет-источники: 1-8.

## Тема 3. Методы и средства защиты информации

Цель: формирование общих представлений методах и средствах защиты информации.

Знания и умения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций или их части:

- знать принципы информационной безопасности, классификации методов защиты информации, средства защиты информации;
- уметь различать методы и средства защиты информации;
- владеть навыками применения методов защиты информации.

Актуальность темы обусловлена необходимостью приобретения соответствующих компетенций по данной дисциплине

### Теоретическая часть

Методы защиты информации:

- препятствие– метод физического преграждения пути злоумышленнику к защищаемой информации
- управление доступом– метод определения и распределения ресурсов системы санкционированным пользователям
- шифрование- метод защиты информации в коммуникационных каналах путем ее криптографического закрытия. Этот метод защиты широко применяется как для обработки, так и для хранения информации. При передаче информации по коммуникационным каналам большой протяженности этот метод является единственно надежным.

– регламентация– метод защиты информации, создающий специальные условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

– принуждение- такой метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

– побуждение- метод защиты информации, который стимулирует пользователя и персонал системы не нарушать установленных норм (высокая зарплата)

Средства:

– технические реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

– программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

– аппаратно-программные средства защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав системы защиты информации и выполняющих такие (самостоятельно или в комплексе с другими средствами) функции защиты, как: идентификация и аутентификация пользователей, разграничение доступа к ресурсам, регистрация событий, криптографическое закрытие информации, обеспечение отказоустойчивости компонент и системы в целом и т.д.

– организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации специального ПО и аппаратных устройств для обеспечения защиты информации.

Организационные мероприятия охватывают все структурные элементы на всех этапах жизненного цикла защищаемой системы (создание охраняемого периметра, строительство помещений, проектирование системы в целом, монтаж и наладка оборудования, испытания и эксплуатация), а также кадровую политику и подбор персонала.

– морально-этические средства защиты реализуются в виде норм, которые сложились традиционно или складываются по мере распространения ВТ и средств связи в данной стране или обществе. Эти нормы, как правило, не являются обязательными, как законодательные меры, однако несоблюдение их ведет к потере авторитета и престижа организации.

– законодательные – средства защиты определяются законодательными актами страны. В них регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Вопросы для обсуждения:

1. Принципы информационной безопасности
2. Классификации методов защиты информации
3. Средства защиты информации

Контрольные вопросы и задания

1. Выполнить прикладную работу: 1) с помощью справочно-правовой системы Консультант Плюс найти, открыть и ознакомиться с содержанием нормативно-правовых документов, в которых раскрываются теоретические положения, 2) с помощью стандартного программного обеспечения отразить в виде схемы все установленные нормативно методы защиты информации в таможенных органах РФ, 3) с помощью стандартного программного обеспечения отразить в виде схемы действие одного на выбор программного средства защиты информации, применяемого в таможенных органах РФ.

Раскрыть порядок сбора таможенными органами сведений о таможенных платежах, основные информационные источники с соответствующей информацией, публикуемые таможенными органами.

2. Какие методы защиты информации существуют?

3. Какие средства защиты информации существуют?

Рекомендуемый список литературы по теме (№ источника):

- основная: 1-2;
- дополнительная: 1-3;
- интернет-источники: 1-8.

#### Тема 4. Нормативно-правовая база защиты информации в таможенных органах

Цель: формирование общих представлений о системе нормативно-правового регулирования информационной безопасности в таможенных органах РФ.

Знания и умения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций или их части:

- знать нормативно-правовые документы, регламентирующие информационную безопасность в таможенных органах РФ, содержание нормативно-правовых документов;
- уметь правильно толковать положения нормативно-правовых документов;
- владеть навыками работы в справочно-правовых системах.

Актуальность темы обусловлена необходимостью приобретения соответствующих компетенций по данной дисциплине.

#### Теоретическая часть

Нормативно-правовая база защиты информации в таможенных органах РФ представлена следующими документами:

1. Приказ ФТС РФ от 8 октября 2019 г. N 1549 «Об утверждении порядка использования программно-технических и иных средств защиты информации таможенными органами Российской Федерации»

2. ФЗ РФ от 3 августа 2018 г. N 289-ФЗ "О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации" в части защиты информации

3. ФЗ РФ от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"
4. Приказ ФТС России от 10.10.2019 N 1570 "Об утверждении Порядка формирования информационных ресурсов таможенных органов Российской Федерации и доступа к ним"
5. Приказ ФТС России от 17.06.2010 N 1154 "Об утверждении Положения о Единой автоматизированной информационной системе таможенных органов"
6. Приказ ФТС РФ от 05.02.2007 N 154 "Об утверждении Типовых требований по оснащению объектов таможенной инфраструктуры информационно-техническими средствами" в части защиты информации

Вопросы для обсуждения

1. Нормативно-правовые документы, регламентирующие информационную безопасность в таможенных органах РФ

2. Содержание нормативно-правовых документов

Контрольные вопросы и задания

1. Выполнить прикладную работу: 1) с помощью справочно-правовой системы Консультант Плюс найти, открыть и ознакомиться с содержанием нормативно-правовых документов, в которых раскрываются теоретические положения, 2) с помощью стандартного программного обеспечения отразить в виде схемы систему нормативно-правового регулирования защиты информации в таможенных органах РФ, 3) с помощью стандартного программного обеспечения отразить в виде схемы порядок использования программно-технических и иных средств защиты информации таможенными органами Российской Федерации, установленный Приказом ФТС РФ от 8 октября 2019 г. N 1549.

2. Какие документы регулируют защиту информации в таможенных органах РФ?

Рекомендуемый список литературы по теме (№ источника):

- основная: 1-2;
- дополнительная: 1-3;
- интернет-источники: 1-8.

Тема 5. Криптографическая защита информации

Цель: формирование общих представлений о криптографической защите информации.

Знания и умения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций или их части:

- знать средства и методы криптографической защиты информации, элементы криптографической защиты информации;
- уметь применять знания для криптоанализа;
- владеть элементарными навыками криптографии.

Актуальность темы обусловлена необходимостью приобретения соответствующих компетенций по данной дисциплине.

## Теоретическая часть

Криптография представляет собой совокупность методов преобразования данных (шифрования), направленных на то, чтобы сделать эти данные бесполезными для противника. Эти преобразования позволяют решить проблему обеспечения конфиденциальности данных. Для ознакомления с зашифрованной информацией применяется обратный процесс — дешифрование. Для шифрования обычно используется некоторый алгоритм или устройство, реализующее заданный алгоритм, которые могут быть известны широкому кругу лиц. Управление процессом шифрования осуществляется с помощью периодически меняющегося ключа шифрования, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа дешифрования позволяет просто и надежно расшифровать текст. Однако без знания этого ключа процедура дешифрования может быть практически невыполнима даже при известном алгоритме. Ключ шифрования  $K$  — конкретное состояние некоторого параметра (параметров), обеспечивающее выбор одного преобразования из совокупности возможных для используемого метода шифрования.

### Вопросы для обсуждения

1. Средства и методы криптографической защиты информации
2. Элементы криптографической защиты информации

### Контрольные вопросы и задания

1. Выполнить прикладную работу: 1) с помощью справочно-правовой системы Консультант Плюс найти, открыть и ознакомиться с содержанием нормативно-правовых документов, в которых раскрываются теоретические положения, 2) с помощью стандартного программного обеспечения отразить в виде схемы организацию криптографической защиты информации в таможенных органах РФ, 3) с помощью стандартного программного обеспечения либо открытых ресурсов сети Интернет разработать алгоритм шифрования сведений электронных документов, хранящихся на рабочем компьютере.

2. Какие методы криптографии существуют?

Рекомендуемый список литературы по теме (№ источника):

- основная: 1-2;
- дополнительная: 1-3;
- интернет-источники: 1-8

### 3 ЛИТЕРАТУРА И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

#### Основная литература

1. Макрусев, В. В. Управление таможенным делом : учебник для вузов / В. В. Макрусев, М. В. Бойкова, Е. О. Любкина ; под общей редакцией В. В. Макрусева. — Москва : Издательство Юрайт, 2026. — 547 с. — (Высшее образование). — ISBN 978-5-534-17516-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589311>.
2. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588515>.

#### Дополнительная литература

1. Международная информационная безопасность: теория и практика : Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583236>.
2. Информационное право : учебник для вузов / под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2025. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567645>.
3. Попова, Л. И. Технологии таможенного контроля : учебник для вузов / Л. И. Попова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 247 с. — (Высшее образование). — ISBN 978-5-534-17976-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561660>.

#### Интернет-ресурсы

1. База данных «Цифровая библиотека IPRsmart (IRPsmart ONE)» [сайт]. Режим доступа: <https://www.iprbookshop.ru>.
2. Научная электронная библиотека «ELIBRARY.RU» [сайт]. Режим доступа: <https://elibrary.ru>.
3. Научная электронная библиотека «КиберЛенинка» [сайт]. Режим доступа: <https://cyberleninka.ru>.

4. Некоммерческая интернет-версия Консультант Плюс [сайт]. Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=home>.
5. Официальный сайт библиотеки ФГАОУ ВО СКФУ [сайт]. Режим доступа: <http://catalog.ncstu.ru/catalog> –.
6. Университетская библиотека ONLINE [сайт]. Режим доступа: <https://biblioclub.ru>.
7. Федеральная таможенная служба [сайт]. Режим доступа: <https://customs.gov.ru>.
8. Электронно-библиотечная система Лань [сайт]. Режим доступа: <https://e.lanbook.com>.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ  
по организации и проведению самостоятельной работы  
по дисциплине «Технологии защиты информации в таможенных органах»  
для студентов специальности 38.05.02 «Таможенное дело»

Ставрополь  
2026



Методические указания составлены в соответствии с программой дисциплины «Технологии защиты информации в таможенных органах» для студентов специальности 38.05.02 Таможенное дело и предназначены для оказания помощи студентам при выполнении самостоятельной работы.

## ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	4
1 ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ.....	5
2 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ТЕОРЕТИЧЕСКОГО МАТЕРИАЛА....	7
2.1 Общие положения.....	7
2.2 Вопросы для собеседования.....	8
2.3 Критерии оценки результатов самостоятельного изучения литературы в ходе собеседования....	9
3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОМУ РЕШЕНИЮ ЗАДАЧ, ВЫПОЛНЕНИЮ ТЕСТОВЫХ ЗАДАНИЙ.....	11
3.1 Общие положения.....	11
3.2 Комплект задач и тестовых заданий.....	11
3.3 Критерии оценки решения задач (тестовых заданий).....	13
4 ЛИТЕРАТУРА И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ.....	15

## ВВЕДЕНИЕ

Важное место с точки зрения реализации цели и задач дисциплины «Технологии защиты информации в таможенных органах» отводится самостоятельной работе студентов (далее – СРС).

СРС является планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (возможно частичное непосредственное участие преподавателя при сохранении ведущей роли студентов).

СРС начинается с первого дня занятий по дисциплине и заканчивается с её окончанием. Её надо уметь правильно организовать, чтобы добиться желаемых результатов. Каковы главные принципы организации самостоятельной работы? Во-первых, целенаправленность, сознательная активность в овладении знаниями и навыками самостоятельной работы. Во-вторых, систематичность в работе, умение работать постоянно, упорно, систематически.

Самостоятельная работа требует определенных навыков, умения. Наибольшую пользу она приносит тогда, когда студент занимается систематически, проявляет трудолюбие и упорство. На основе самостоятельно приобретенных знаний формируются твердые убеждения студента и умение отстаивать их.

Цель настоящих методических указаний – определить назначение СРС и её роль в изучении дисциплины; конкретизировать формы и виды СРС; объяснить критерии оценивания СРС.

## 1 ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Целью самостоятельной работы студентов (далее – СРС) по дисциплине «Технологии защиты информации в таможенных органах» является овладение фундаментальными знаниями, профессиональными умениями и навыками по дисциплине, опытом творческой, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем.

Задачами СРС являются:

- систематизация и закрепление полученных в рамках аудиторной работы теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий, для эффективной подготовки к промежуточной аттестации.

Дисциплина «Технологии защиты информации в таможенных органах» относится к части, формируемой участниками образовательных отношений.

Технологическая карта самостоятельной работы обучающихся представлена в таблице 1.

Таблица 1 - План-график выполнения самостоятельной работы

Код оцениваемой компетенции, индикатора (ов)	Этап формирования компетенции (№ темы)	Вид деятельности студентов	Средства и технологии оценки	Наименование оценочного средства
ИД-2. ОПК-2 ИД-2. ОПК-6 ИД-4. ПК-4	1-5	Самостоятельное изучение теоретического материала	Собеседование	Вопросы для собеседования
ИД-2. ОПК-2 ИД-2. ОПК-6 ИД-4. ПК-4	1-5	Самостоятельное решение задач, выполнение тестовых заданий	Проверка решений	Комплект задач и тестовых заданий

## 2 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ТЕОРЕТИЧЕСКОГО МАТЕРИАЛА

### 2.1 Общие положения

При изучении дисциплины большую и важную роль играет самостоятельная индивидуальная работа с литературой. Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь.

Успешность самостоятельного чтения литературы во многом зависит от умения правильно работать с литературой, работать над текстом.

При работе с текстом целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом. Т.е. не запоминать, а понять общий смысл прочитанного содержания. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом.

Чтение становится более продуктивным, когда сопровождается записями. Основные виды систематизированной записи прочитанного следующие:

1. Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;
2. Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;
3. Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;
4. Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;
5. Конспектирование – краткое и последовательное изложение содержания прочитанного.

Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи.

Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта. При составлении конспекта рекомендуется придерживаться следующих правил:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова.  
При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

## 2.2 Вопросы для собеседования

Тема 1. Общие положения об информации и защите информации в таможенных органах РФ

1. Сущность, виды информации

2. Сбор, хранение, преобразование и передача информации

3. Способы и средства передачи информации

4. Информация и действия с информацией в таможенных органах РФ

5. Цели защиты информации в таможенных органах РФ

Рекомендуемый список литературы по теме (№ источника):

– основная: 1-2;

– дополнительная: 1-3;

– интернет-источники: 1-8.

Тема 2. Угрозы информационной безопасности

1. Классификации угроз информационной безопасности

2. Механизм действия отдельных видов угроз

Рекомендуемый список литературы по теме (№ источника):

– основная: 1-2;

– дополнительная: 1-3;

– интернет-источники: 1-8.

Тема 3. Методы и средства защиты информации

1. Принципы информационной безопасности

2. Классификации методов защиты информации

3. Средства защиты информации

Рекомендуемый список литературы по теме (№ источника):

– основная: 1-2;

– дополнительная: 1-3;

– интернет-источники: 1-8.

Тема 4. Нормативно-правовая база защиты информации в таможенных органах

1. Нормативно-правовые документы, регламентирующие информационную безопасность в таможенных органах РФ

## 2. Содержание нормативно-правовых документов

Рекомендуемый список литературы по теме (№ источника):

- основная: 1-2;
- дополнительная: 1-3;
- интернет-источники: 1-8.

## Тема 5. Криптографическая защита информации

### 1. Средства и методы криптографической защиты информации

### 2. Элементы криптографической защиты информации

Рекомендуемый список литературы по теме (№ источника):

- основная: 1-2;
- дополнительная: 1-3;
- интернет-источники: 1-8.

## 2.3 Критерии оценки результатов самостоятельного изучения литературы в ходе собеседования

Для оценки результатов самостоятельного изучения литературы со студентами проводится собеседование по выданным для собеседования вопросам. Собеседование проводится в устной форме в специально установленное преподавателем для этого время. Во время собеседования выясняется уровень подготовки студента по обсуждаемой теме, объем специальной литературы, с которой он ознакомился, обсуждение вопросов, не до конца понятых студентами.

Оценка «отлично» выставляется студенту, если он обстоятельно с достаточной полнотой излагает соответствующую тему; дает правильные формулировки, точные определения, понятия терминов; может обосновать свой ответ, привести необходимые примеры; правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания студентом данного материала.

Оценка «хорошо» выставляется студенту, если: задание изложено неполно, но правильно; при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя; даются правильные формулировки, точные определения, понятия терминов; студент может обосновать свой ответ, привести необходимые примеры; правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания студентом данного материала.

Оценку «удовлетворительно» студент получает, если: неполно, но правильно изложено задание; при изложении была допущена одна существенная ошибка; знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий; излагает выполнение задания недостаточно логично и последовательно; затрудняется при ответах на вопросы преподавателя.

Оценку «неудовлетворительно» студент получает, если: неполно изложено задание; при изложении были допущены существенные ошибки, т.е. если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы СРС.

### 3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОМУ РЕШЕНИЮ ЗАДАЧ, ВЫПОЛНЕНИЮ ТЕСТОВЫХ ЗАДАНИЙ

#### 3.1 Общие положения

Цель самостоятельного решения задач и выполнения тестовых заданий - закрепление знаний по основным теоретическим положениям дисциплины и формирование навыков и умений по применению этих знаний, необходимых в будущей учебной и практической деятельности.

Данный вид СРС способствует формированию у студентов системного мышления, а также навыков использования специальной и справочной литературы для решения практических вопросов.

Задания выполняются на основе изучения материалов лекций и практических занятий, а также соответствующей литературы. Данный вид СРС предполагает самостоятельную систематизацию информации и мыслительный поиск решения проблемы.

Перед выполнением заданий студенту необходимо:

- изучить материал задания в материалах лекционных и практических занятий по дисциплине, источниках литературы;
- ознакомиться со статистическими данными, публикуемыми в периодической печати и в статистических сборниках;
- ознакомиться со статьями периодической печати, освещающими вопросы задания.

Ответ на задание должен быть написан грамотно и разборчивым почерком. Они должны быть конкретными, точными. Выполненная работа сдается на проверку преподавателю в срок, который устанавливается преподавателем, ведущим практические занятия по дисциплине.

Без проверки могут быть возвращены работы, выполненные небрежно, неразборчивым почерком. Если работа выполнена с ошибками, работа возвращается студенту для повторного выполнения или доработки. Повторную работу студент должен предоставить на кафедру вместе с незначительной работой. После получения допуска работы к собеседованию студент должен пройти собеседование у преподавателя, который проверял данную работу.

#### 3.2 Комплект задач и тестовых заданий

Основные объекты информационной безопасности:

- а) компьютерные сети, базы данных
- б) транспортно-логистические системы
- в) психологическое состояние пользователей
- г) бизнес-ориентированные коммерческие системы

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- а) Сотрудники
- б) Хакеры
- в) Конкуренты
- г) Контрагенты

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- а) владельцы данных
- б) пользователи
- в) администраторы
- г) руководство

К правовым методам, обеспечивающим информационную безопасность, относятся:

- а) разработка аппаратных средств обеспечения правовых данных
- б) разработка и установка во всех компьютерных правовых сетях журналов учета действий
- в) разработка и конкретизация правовых нормативных актов обеспечения безопасности
- г) криптографический метод

Защита информации от утечки — это деятельность по предотвращению:

- а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
- б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
- в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
- г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа

Какой документ является основным в вопросе регулирования защиты информации в таможенных органах РФ?

- а) Приказ ФТС РФ №1549
- б) Федеральный закон РФ №289-ФЗ
- в) Приказ ФТС РФ №1570
- г) Приказ ФТС РФ №1154

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяют на:

- а) правовые (законодательные);
- б) организационно-административные;
- в) аппаратно-программные

г) интеллектуальные

Наиболее известными продуктами, на базе которых разворачивается инфраструктура открытых ключей, являются следующие:

- а) Entrust/PKI фирмы Entrust Technologies.
- б) Baltimore UniCERT фирмы Baltimore Technologies LTD.
- в) BT TrustWise Onsite фирмы VeriSign Inc
- г) AltaSoft Inc

К техническим средствам борьбы с компьютерными вирусами относят:

- а) запреты на самостоятельную установку нового ПО
- б) привлечение к уголовной или административной ответственности
- в) применение антивирусных мониторов и сканеров
- г) применение программных и аппаратных средств, не допускающих возможность

заражения объектов компьютерной системы

Совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника – это:

- а) криптография
- б) криптоанализ
- в) дешифрование
- г) закрытый текст

Программно-аппаратный комплекс, который стоит между сетью внутренней и сетью внешней, предназначенный для фильтрации данных и предотвращения проникновения во внутреннюю сеть вредоносных программ — это:

- а) Firewall
- б) Брандмауэр
- в) межсетевой экран
- г) VPN

### 3.3 Критерии оценки решения задач (тестовых заданий)

Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, причем не затрудняется с ответом при видоизменении задач, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения задач.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, правильно применяет теоретические положения при решении задач, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, испытывает затруднения (допускает неточности,

недостаточно правильные формулировки, нарушения логической последовательности) при решении задач.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает задачи.

## 4 ЛИТЕРАТУРА И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

### Основная литература

3. 1. Макрусев, В. В. Управление таможенным делом : учебник для вузов / В. В. Макрусев, М. В. Бойкова, Е. О. Любкина ; под общей редакцией В. В. Макрусева. — Москва : Издательство Юрайт, 2026. — 547 с. — (Высшее образование). — ISBN 978-5-534-17516-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589311>.
4. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588515>.

### Дополнительная литература

4. Международная информационная безопасность: теория и практика : Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583236>.
5. Информационное право : учебник для вузов / под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2025. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567645>.
6. Попова, Л. И. Технологии таможенного контроля : учебник для вузов / Л. И. Попова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 247 с. — (Высшее образование). — ISBN 978-5-534-17976-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561660>.

### Интернет-ресурсы

1. База данных «Цифровая библиотека IPRsmart (IRPsmart ONE)» [сайт]. Режим доступа: <https://www.iprbookshop.ru>.
2. Научная электронная библиотека «ELIBRARY.RU» [сайт]. Режим доступа: <https://elibrary.ru>.

3. Научная электронная библиотека «КиберЛенинка» [сайт]. Режим доступа: <https://cyberleninka.ru>.
4. Некоммерческая интернет-версия Консультант Плюс [сайт]. Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=home>.
5. Официальный сайт библиотеки ФГАОУ ВО СКФУ [сайт]. Режим доступа: <http://catalog.ncstu.ru/catalog> –.
6. Университетская библиотека ONLINE [сайт]. Режим доступа: <https://biblioclub.ru>.
7. Федеральная таможенная служба [сайт]. Режим доступа: <https://customs.gov.ru>.
8. Электронно-библиотечная система Лань [сайт]. Режим доступа: <https://e.lanbook.com>.