

TOLBANK

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФГБОУ ВО «СГУ имени Н.Г. Чернышевского»

Факультет компьютерных наук и информационных технологий



Рабочая программа дисциплины  
Техническая защита информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Квалификация выпускника

Специалист по защите информации

Форма обучения

Очная

Саратов,

2017

## **1. Цели освоения дисциплины**

Целями освоения дисциплины «Техническая защита информации» являются: овладение основными знаниями и навыками в области защиты информации от разглашения, несанкционированного доступа и утечки по техническим каналам.

## **2. Место дисциплины в структуре ООП**

Данная учебная дисциплина относится к базовой части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся профессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Операционные системы», «Сети и системы передачи информации», «Организационное и правовое обеспечение информационной безопасности», «Криптографические методы защиты информации».

## **3. Компетенции обучающегося, формируемые в результате освоения дисциплины**

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

- способностью проводить инструментальный мониторинг защищенности компьютерных систем (ПК-12);
- способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации (ПК-19);
- способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций (ПК-20).

В рамках указанных компетенций обучающийся должен

- Знать:
  - угрозы информации в результате разглашения;
  - методы и способы защиты информации от разглашения;
  - угрозы информации в результате несанкционированного доступа;
  - технические средства защиты информации от несанкционированного доступа;
  - технические каналы утечки информации;
  - возможности технических средств перехвата информации;
  - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
  - организацию защиты информации от утечки по техническим каналам на объектах информатизации;
  - основы физической защиты объектов информатизации;

– используемые практические подходы и методики построение комплексных систем защиты информации с использованием технических средств.

• Уметь:

– пользоваться нормативными документами, регламентирующими процедуры по противодействию технической разведке.

• Владеть:

– методами и средствами технической защиты информации;

– методами расчета и инструментального контроля показателей технической защиты информации.

#### 4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Всего часов	Лекции	Лабораторные занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
1	Информация и ее свойства	10	1-4	36	8	8	20	Контрольная работа на 12-й неделе
2	Защита информации от несанкционированного доступа		5-8	36	8	8	20	
3	Защита информации от утечки по техническим каналам		9-12	36	8	8	20	
4	Действующее законодательство в области информационной безопасности		13-16	36	8	8	20	
	Промежуточная аттестация							Экзамен
	ИТОГО			180	32	32	80	36

*Информация и ее свойства:* Виды, источники представления и носители защищаемой информации. Защищаемые свойства информации. Средства и системы обработки информации. Угрозы защищаемой информации. Классификация угроз безопасности информации. Модель угроз

и методики определения актуальности угроз безопасности информации. Правовые, организационные и технические подходы к защите информации.

*Защита информации от несанкционированного доступа и разглашения:* Технические средства защиты информации от разглашения. Защита от несанкционированного доступа в автоматизированных системах. Межсетевые экраны. Средства обнаружения и предотвращения вторжений. Средства анализа защищенности автоматизированных систем. Средства доверенной загрузки. Средства усиленной аутентификации. Средства управления доступом, регистрации и учета. Средства предотвращения утечки информации. Антивирусные средства. Средства защищенной передачи конфиденциальной информации.

*Защита информации от утечки по техническим каналам:* Структура, классификация и основные характеристики технических каналов утечки информации. Классификация технической разведки. Возможности видов технической разведки. Утечка акустической информации. Подавление опасных сигналов акустоэлектрических преобразователей. Энергетическое скрывание акустических информативных сигналов. Скрывание речевой информации в каналах связи. Каналы утечки информации, обрабатываемой в электронных устройствах. Побочные электромагнитные излучения и наводки, защита от информативных полей и сигналов в цепях заземления и электропитания. Обнаружение и локализация закладных устройств, подавление их сигналов.

*Действующее законодательство в области информационной безопасности:* Обзор действующих правовых, нормативных и методических документов в области технической защиты информации.

### **План лабораторных занятий**

На лабораторных занятиях студенты выполняют назначенные задания в оборудованной лаборатории.

<b>№ занятия</b>	<b>Тема</b>	<b>Задания для лабораторного практикума</b>
<b>1</b>	<b>2</b>	<b>3</b>
1-4	Информация и ее свойства	№№ 1–2
5-8	Защита информации от несанкционированного доступа	№№ 3–9
9-12	Защита информации от утечки по техническим каналам	№№ 10–12
13-16	Действующее законодательство в области информационной безопасности	№ 13

### **5. Образовательные технологии, применяемые при освоении дисциплины**

Предусматривается широкое использование в учебном процессе таких образовательных технологий как организационная технология балльно-рейтингового обучения, проектная творческая и научно-исследовательская деятельности. В рамках учебного курса предусмотрены встречи с

представителями компаний-лицензиатов ФСТЭК России и ФСБ России, выступления экспертов и специалистов перед студентами, ознакомительные беседы с представителями потенциальных работодателей.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

Основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья и инвалидов, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

## **6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины**

В рамках самостоятельной работы студенты изучают дополнительную литературу по предмету. При чтении лекций по соответствующим разделам дисциплины даются ссылки на источники, в которых более детально рассматривается материал.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (экзамен). Фонд оценочных средств дисциплины приведён в приложении 1.

## **7. Данные для учета успеваемости студентов в БАРС**

Таблица 1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции и	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
10	10	30	0	10	0	10	40	100

### **Программа оценивания учебной деятельности студента**

#### **10 семестр**

#### **Лекции**

Оценивается посещаемость, активность, умение выделить главную мысль и др. – от 0 до 10 баллов.

#### **Лабораторные занятия**

Оценивается самостоятельность при выполнении работы, грамотность в оформлении, правильность выполнения – от 0 до 30 баллов.

#### **Практические занятия**

Не предусмотрены.

**Самостоятельная работа**

Оценивается качество подготовки к лабораторным занятиям – от 0 до 10 баллов.

**Автоматизированное тестирование**

Не предусмотрено.

**Другие виды учебной деятельности**

Контрольная работа – от 0 до 10 баллов.

**Промежуточная аттестация**

Промежуточная аттестация представляет собой теоретический экзамен, проводимый в устной форме с предварительной подготовкой студента к ответу.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 25 до 30 баллов;

ответ на «хорошо» оценивается от 20 до 24 баллов;

ответ на «удовлетворительно» оценивается от 15 до 19 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 14 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за десятый семестр по дисциплине «Техническая защита информации» составляет 100 баллов.

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Техническая защита информации» в оценку (экзамен):

90–100 баллов	«отлично»
70–89 баллов	«хорошо»
40–69 баллов	«удовлетворительно»
0–39баллов	«неудовлетворительно»

## 8. Учебно-методическое и информационное обеспечение дисциплины

### а) основная литература:

1) Юрин, И. Ю. Теоретические и практические основы защиты информации [Электронный ресурс]: учеб. пособие / И. Ю. Юрин. Саратов, 2012. 32 с. URL: [http://library.sgu.ru/uch\\_lit/620.pdf](http://library.sgu.ru/uch_lit/620.pdf) (дата обращения: 02.01.2017). Загл. с экрана. Яз.рус.

### б) дополнительная литература:

1) Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки [Текст] : учеб.пособие / Ю. К. Меньшаков ; худож. М. Гуров ; Рос.гос. гуманитар. ун-т. - Москва : Рос.гос. гуманитар. ун-т, 2002. - 398, [2] с. : ил. - Библиогр.: с. 396-399. - ISBN 5-7281-0487-8 (в пер.),

2) Титов, А. А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие / Титов А. А. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 197 с. - Б. ц. URL: <http://www.iprbookshop.ru/13931> (дата обращения: 02.01.2017). Загл. с экрана. Яз.рус.

3) Ярочкин, В. И. Информационная безопасность [Текст] : учеб.для вузов / В. И. Ярочкин. - 5-е изд. - Москва : Акад. Проект, 2008. - 542, [2] с. : рис., табл. - (Gaudeamus). - Библиогр.: с. 534-539. - ISBN 978-5-8291-0987-5 (в пер.).

## 9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения лабораторных занятий необходимы: лаборатория с компьютерной техникой на базе операционных систем «Windows», дистрибутивы средств защиты (пользование в течение разрешенного свободного периода действия лицензии), технические средства:

- 1) Зонд-монитор СРМ 700.
- 2) Нелинейный локатор «КАТРАН».
- 3) САЗ «Шатёр-4»
- 4) Генератор шума «Гром ЗИ-4».
- 5) Программно-аппаратный комплекс «Аккорд NT/2000».
- 6) Программно-аппаратный комплекс «Соболь».
- 7) Программно-аппаратный комплекс «ESMART Access».
- 8) Биометрическая защита EyeDOptiMouse.
- 9) Программный комплекс «SecretNet».

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Ассистент кафедры теоретических основ компьютерной безопасности и криптографии



Н.Н. Бондарев

Программа разработана в 2012 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «25» мая 2012 года, протокол № 18).

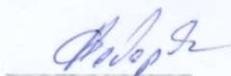
Программа актуализирована в 2017 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «09» января 2017 года, протокол № 10).

Заведующий кафедрой теоретических основ компьютерной безопасности и криптографии, профессор, к.ф.-м.н.



В.Н. Салий

Декан факультета компьютерных наук и информационных технологий, к.ф.-м.н., доцент



А.Г. Федорова