МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный технологический институт
(технический университет)»

УТВЕРЖДАЮ
Проректор по учебной
и методической работе
_____ Б.В. Пекаревский
« 21 » мая 2019 г.

.

**Рабочая программа дисциплины**

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки

**09.03.02 Информационные системы и технологии**

Направленность программы бакалавриата

**Информационные системы и технологии**

Квалификация

**Бакалавр**

Форма обучения

**Очная**

Факультет **информационных технологий и управления**

Кафедра **системного анализа и информационных технологий**

Санкт-Петербург

2019

**ЛИСТ СОГЛАСОВАНИЯ**

| Должность разработчика | Подпись | Ученое звание, фамилия, инициалы |
|---|---|---|
| доцент | | доцент, Ананченко И.В. |

Рабочая программа дисциплины «Информационная безопасность» обсуждена на заседании кафедры системного анализа и информационных технологий
протокол от « 25 » 04 2019 № 5
Заведующий кафедрой А.А. Мусаев

Одобрено учебно-методической комиссией факультета информационных технологий и управления
протокол от « 15 » 05 2019 № 9

Председатель В.В. Куркина

СОГЛАСОВАНО

| | | |
|---|---|---|
| Руководитель направления подготовки «Информационные системы и технологии» | | Г.А. Мамаева |
| Директор библиотеки | | Т.Н. Старостенко |
| Начальник методического отдела учебно-методического управления | | Т.И. Богданова |
| Начальник учебно-методического управления | | С.Н. Денисенко |

**СОДЕРЖАНИЕ**



Приложения: 1. Фонд оценочных средств для проведения промежуточной аттестации.

**1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы**

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения (дескрипторы) |
|---|---|---|
| • **ОПК-3** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | **ОПК-3.2** Выбор и обоснование организационно-технических мероприятий по защите информации в информационных системах. | **Знать:** - методологию обоснование организационно-технических мероприятий по защите информации в информационных системах. (ЗН-1). **Уметь:** - проводить организационно-технические мероприятия по защите информации в информационных системах (У-1). **Владеть:** - навыками решения задач организационно-технических мероприятий по защите информации в информационных системах (Н-1). |
| | **ОПК-3.3** Применение методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности. | **Знать:** - принципы и методологию применения методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности (ЗН-2). **Уметь:** - применять методы обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности (У-2). **Владеть:** - навыками решения задач обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности (Н-2). |

## 2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам базовой части (Б1.О.29) и изучается на 4 курсе в 8 семестре.

Изучение данной дисциплины базируется на знании студентами основ математики, информатики и основ алгоритмизации, на знаниях, полученных в процессе изучения дисциплин «Операционные системы», «Информатика», «Алгоритмы и структуры данных», «Программирование на языке С++», «Программирование на языках низкого уровня», «Программирование на языке Python», «Архитектура информационных систем», «Большие данные», «Мультимедиа технологии», «Облачные технологии», «Информационно-коммуникационные системы и сети».

Полученные в процессе изучения дисциплины «Информационная безопасность» знания, умения и навыки могут быть использованы в научно-исследовательской работе бакалавра и при выполнении выпускной квалификационной работы.

## 3. Объем дисциплины

| Вид учебной работы | Всего, академических часов |
|---|---|
| | Очная форма обучения |
| **Общая трудоемкость дисциплины** (зачетных единиц/ академических часов) | 4/ 144 |
| **Контактная работа с преподавателем:** | **52** |
| занятия лекционного типа | **16** |
| занятия семинарского типа, в т.ч. | 32 |
| семинары, практические занятия | **32** |
| лабораторные работы | - |
| курсовое проектирование (КР или КП) | |
| КСР | **4** |
| другие виды контактной работы | |
| **Самостоятельная работа** | 56 |
| **Форма текущего контроля (**Кр, реферат, РГР, эссе) | |
| **Форма промежуточной аттестации** (КР, КП, зачет, экзамен) | **экзамен/36** |

## 4. Содержание дисциплины

### 4.1. Разделы дисциплины и виды занятий

| № п/п | Наименование раздела дисциплины | Занятия лекционного типа, акад. часы | Занятия семинарского типа, академ. часы | | Самостоятельная работа, акад. часы | Формируемые компетенции | Формируемые индикаторы |
|---|---|---|---|---|---|---|---|
| | | | Семинары и/или практические занятия | Лабораторные работы | | | |
| 1. | Теоретические основы информационной безопасности. | 3 | 6 | | 11 | ОПК-3 | ОПК-3.2<br>ОПК-3.3 |
| 2 | Основы криптографии. Совместное использование симметричных и асимметричных шифров. | 3 | 6 | | 11 | ОПК-3 | ОПК-3.2<br>ОПК-3.3 |
| 3. | Защита информации в IP-сетях. Протоколы SSL и TLS. Протокол защиты электронной почты S/MIME. | 3 | 6 | | 11 | ОПК-3 | ОПК-3.2<br>ОПК-3.3 |
| 4. | Анализ и управление рисками в сфере информационной безопасности. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». | 3 | 6 | | 11 | ОПК-3 | ОПК-3.2<br>ОПК-3.3 |
| 5. | Управление доступом, выявление уязвимостей. Использование сканеров безопасности для получения информации о хостах в сети. Шифрование данных при хранении – файловая система EFS. | 4 | 8 | | 12 | ОПК-3 | ОПК-3.2<br>ОПК-3.3 |

### 4.2. Занятия лекционного типа

| № раздела дисци- | Наименование темы и краткое содержание занятия | Объем, акад. часы | Инновационная форма |
|---|---|---|---|
| 1. | Теоретические основы информационной безопасности. Введение. Базовые понятия. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Модели безопасности. | 3 | ЛВ |
| 2. | Основы криптографии. Основные понятия. Классификация шифров. Симметричные шифры. Схема Фейстеля. Шифр DES. Шифр ГОСТ 28147-89. Шифр Blowfish. Управление криптографическими ключами для симметричных шифров. | 3 | ЛВ |
| 3. | Защита информации в IP-сетях. Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей. Межсетевые экраны. | 3 | ЛВ |
| 4. | Анализ и управление рисками в сфере информационной безопасности. Введение в проблему. Управление рисками. Модель безопасности с полным перекрытием. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001. ГОСТ Р ИСО/МЭК 17799:2005 «Информационная технология. Практические правила управления информационной безопасностью». ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Методики построения систем защиты информации. Модель Lifecycle Security. | 3 | ЛВ |
| 5. | Управление доступом, выявление уязвимостей. Управление доступом к файлам на NTFS. Управление доступом в СУБД SQL SERVER. Выявление уязвимостей с помощью Microsoft Baseline Security analyzer. Использование сканеров безопасности для получения информации о хостах в сети. | 4 | ЛВ |

### 4.3. Занятия семинарского типа

#### 4.3.1. Семинары, практические занятия

| № раздела дисциплины | Наименование темы и краткое содержание занятия | Объем, акад. часы | Инновационная форма |
|---|---|---|---|
| 1 | Модель Харрисона–Рузо–Ульмана. Модель Белла ЛаПадула. Ролевая модель безопасности. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408. | 6 | Слайд-презентация, групповая дискуссия |

| № раздела дисциплины | Наименование темы и краткое содержание занятия | Объем, акад. часы | Инновационная форма |
|---|---|---|---|
| 2 | Асимметричные шифры. Основные понятия. Распределение ключей по схеме Диффи Хеллмана. Криптографическая система RSA. Криптографическая система Эль Гамаля. Совместное использование симметричных и асимметричных шифров. Хэш-функции. Хэш-функции без ключа. Алгоритм SHA-1. | 6 | Слайд-презентация, групповая дискуссия |
| 3 | Защита информации в IP-сетях. Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей. Межсетевые экраны. | 6 | Слайд-презентация, групповая дискуссия |
| 4 | Модель многоуровневой защиты. Методика управления рисками, предлагаемая Майкрософт. Методики и программные продукты для оценки рисков. Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Проведение оценки рисков в соответствии с методикой Майкрософт. | 6 | Слайд-презентация, групповая дискуссия |
| 5 | Встроенный межсетевой экран (Firewall) Windows Server 2008. Использование цифровых сертификатов. Создание центра сертификации (удостоверяющего центра) в Windows Server 2008. Шифрование данных при хранении – файловая система EFS. Использование Microsoft Security Assessment Tool. «Kaspersky Security Center». Установка Kaspersky Security Center. | 8 | Слайд-презентация, групповая дискуссия |

### 4.4. Самостоятельная работа обучающихся

| № раздела дисциплины | Перечень вопросов для самостоятельного изучения | Объем, акад. часы | Форма контроля |
|---|---|---|---|
| 1 | Модель Харрисона–Рузо–Ульмана. Модель Белла ЛаПадула. Ролевая модель безопасности. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408. | 11 | Устный опрос №1 |
| 2 | Совместное использование симметричных и асимметричных шифров. Хэш-функции. Хэш-функции без ключа. Алгоритм SHA-1.<br>Хэш-функции с ключом. Инфраструктура открытых ключей. Цифровые сертификаты. | 11 | Устный опрос №2 |
| 3 | Защита информации в IP-сетях. Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей. Межсетевые экраны. | 11 | Устный опрос №3 |

| № раздела дисциплины | Перечень вопросов для самостоятельного изучения | Объем, акад. часы | Форма контроля |
|---|---|---|---|
| 4 | Проведение оценки рисков в соответствии с методикой Майкрософт. Анализ существующих подходов. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель». | 11 | Устный опрос №4 |
| 5 | Развертывание антивирусной защиты: установка агентов администрирования, проверка совместимости. Развертывание антивирусной защиты и управление лицензионными ключами. Конфигурирование сервера администрирования. Работа с вирусными инцидентами. Настройка протокола IPSec в Windows Server 2008. | 12 | Устный опрос №5 |

**5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

Методические указания для обучающихся по организации самостоятельной работы по дисциплине, включая перечень тем самостоятельной работы, формы текущего контроля по дисциплине и требования к их выполнению размещены в электронной информационно-образовательной среде СПбГТИ(ТУ) на сайте: http://media.technolog.edu.ru

**6. Фонд оценочных средств для проведения промежуточной аттестации**

Промежуточная аттестация по дисциплине проводится в виде экзамена.

Экзамен предусматривают выборочную проверку освоения предусмотренных элементов компетенций и комплектуется теоретическими вопросами (для проверки знаний, умений и навыков).

При сдаче экзамена студент получает два вопроса из перечня вопросов, время подготовки студента к ответу - до 30 мин.

Пример варианта вопросов на экзамене:

**Вариант №** 1

1. Модель Белла ЛаПадула. Ролевая модель безопасности.
2. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей.

Фонд оценочных средств по дисциплине представлен в Приложении № 1

Результаты освоения дисциплины считаются достигнутыми, если для всех элементов компетенций достигнут пороговый уровень освоения компетенции на данном этапе – оценка «удовлетворительно».

## 7. Перечень учебных изданий, необходимых для освоения дисциплины

### а) печатные издания:


1. Мельников, В.П. Информационная безопасность и защита информации : Учебное пособие для вузов по спец. «Информационные системы и технологии» / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. - 5-е изд., стер. - М.: Academia, 2011. - 331 с.
2. Платонов, В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : Учебное пособие для вузов по спец. 090102 «Компьютерная безопасность», 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» / В.В. Платонов. - М.: Академия, 2006. - 239 с.
3. Расторгуев, С.П. Основы информационной безопасности : учебное пособие для вузов по спец. «Компьютерная безопасность», «Комплексное обеспечение информационной безопасности автоматизированных систем» и «Информационная безопасность телекоммуникационных систем» / С. П. Расторгуев. - М. : Academia, 2007. - 187 с.


### б) электронные учебные издания:


1. Тумбинская, М.В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М.В. Тумбинская, М.В. Петровский. - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2019. - 344 с. (ЭБС Лань).
2. Никифоров, С.Н. Методы защиты информации. Шифрование данных : Учебное пособие / С.Н. Никифоров. - 2-е изд., стер. - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2019. - 160 с. (ЭБС Лань).
3. Никифоров, С.Н. Методы защиты информации. Пароли, скрытие, шифрование : Учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2019. - 124 с. (ЭБС Лань).
4. Введение в теоретико-числовые методы криптографии : учебное пособие для вузов по спец. «Криптография» / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2011. - 400 с. - (ЭБС Лань).
5. Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений : Учебное пособие / С.Н. Никифоров. - 2-е изд., стер. - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2019. - 96 с. (ЭБС Лань).
6. Нестеров, С.А. Основы информационной безопасности : Учебное пособие / С.А. Нестеров. - 5-е изд., стер. - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2019. - 324 с. (ЭБС Лань).
7. Панкратова, И.А. Булевы функции в криптографии : Учебное пособие / И.А. Панкратова. - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2019. - 92 с. - (ЭБС Лань).
8. Петренко, В.И. Защита персональных данных в информационных системах. Практикум : учебное пособие / В.И. Петренко, И.В. Мандрица. - Электрон. текстовые дан. - СПб. ; М. ; Краснодар : Лань, 2019. - 108 с. (ЭБС Лань).

## 8. Перечень электронных образовательных ресурсов, необходимых для освоения дисциплины

учебный план, РПД и учебно-методические материалы: http://media.technolog.edu.ru
электронно-библиотечные системы:

«Электронный читальный зал – БиблиоТех» https://technolog.bibliotech.ru/;

«Лань» https://e.lanbook.com/books/.

https://www.youtube.com/watch?v=xDJqRS5d7MQ — «Цифровой двойник» Земли
Проектирование информационных систем
https://www.intuit.ru/studies/courses/1178/330/info
Теория информационных технологий и систем
https://www.intuit.ru/studies/courses/1158/315/info
Теория информационных систем https://www.intuit.ru/studies/courses/507/363/info
Проектирование информационных систем в Microsoft SQL Server 2008 и Visual Studio 2008 https://www.intuit.ru/studies/courses/502/358/info
Управление развитием информационных систем
https://www.intuit.ru/studies/courses/532/388/info
Администрирование ОС Linux http://www.intuit.ru/studies/courses/23/23/info/
Основы работы в ОС Linux http://www.intuit.ru/studies/courses/91/91/info
Операционная система Linux http://www.intuit.ru/studies/courses/37/37/info
Администрирование ОС Unix http://www.intuit.ru/studies/courses/990/299/info
Введение в системное администрирование Unix:
http://www.intuit.ru/studies/courses/1028/253/info
Академия ALT Linux: Операционная система UNIX: Информация
http://www.intuit.ru/studies/courses/22/22/info
LINUX.OGR Community http://www.linux.org/
Astra Linux Common Edition http://astra-linux.com/
UNIX An Open Group Standard http://www.unix.org/

## 9. Методические указания для обучающихся по освоению дисциплины

Все виды занятий по дисциплине «Информационная безопасность» проводятся в соответствии с требованиями следующих СТП:

СТП СПбГТИ 040-02. КС УКДВ. Виды учебных занятий. Лекция. Общие требования;

СТО СПбГТИ 018-2014. КС УКДВ. Виды учебных занятий. Семинары и практические занятия. Общие требования к организации и проведению.

СТП СПбГТИ 048-2009. КС УКДВ. Виды учебных занятий. Самостоятельная планируемая работа студентов. Общие требования к организации и проведению.

Планирование времени, необходимого на изучение данной дисциплины, лучше всего осуществлять на весь семестр, предусматривая при этом регулярное повторение пройденного материала.

Основными условиями правильной организации учебного процесса для студентов является:

плановость в организации учебной работы;

серьезное отношение к изучению материала;

постоянный самоконтроль.

На занятия студент должен приходить, имея знания по уже изученному материалу.

**10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине**

**10.1. Информационные технологии**

В учебном процессе по данной дисциплине предусмотрено использование информационных технологий:

чтение лекций с использованием слайд-презентаций;

взаимодействие с обучающимися посредством ЭИОС.

**10.2. Программное обеспечение**

Программы: ОС Microsoft Windows, ОС Kali Linux, ОС AstraLinux, ОС Ubuntu, MathCAD, Microsoft Office (Microsoft Word, Microsoft Excel, Microsoft Access, Microsoft PowerPoint), интегрированная среда Microsoft Visual Studio Community. VMware Workstation Player. Hyper-V. MS Virtual PC.

**10.3. Базы данных и информационно справочные системы**

Справочно-поисковая система «Консультант-Плюс»

**11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.**

Для ведения лекционных и практических занятий используется компьютерный класс, оснащенный объединенными в сеть персональными компьютерами, оборудованием и техническими средствами обучения на необходимое количество посадочных мест. При проведении занятий используется аудитория, оборудованная при необходимости проектором для отображения презентаций. Кроме того, при проведении лекций и практических занятий необходим компьютер с установленным на нем браузером и программным обеспечением для демонстрации презентаций (Power Point и др.). Для самостоятельной работы с медиаматериалами каждому студенту требуется персональный компьютер или планшет, широкополосный доступ в сеть Интернет, браузер последней версии, устройство для воспроизведения звука (динамики, колонки, наушники и др.)

**12. Особенности освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья.**

Для инвалидов и лиц с ограниченными возможностями учебные процесс осуществляется в соответствии с Положением об организации учебного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья СПбГТИ(ТУ), утвержденным ректором 28.08.2014г.

Приложение № 1
к рабочей программе дисциплины

**Фонд оценочных средств**
**для проведения промежуточной аттестации по**
**дисциплине «Информационная безопасность»**

## 1. Перечень компетенций и этапов их формирования.

| Индекс компетенции | Содержание | Этап формирования |
|---|---|---|
| ОПК-3 | **Способен решать стандартные задачи профессиональной деятельности на основе информационной** и библиографической культуры **с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности** | промежуточный |

**2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкала оценивания**

| Код и наименование индикатора достижения компетенции | Показатели сформированности (дескрипторы) | Критерий оценивания | УРОВНИ СФОРМИРОВАННОСТИ (описание выраженности дескрипторов) | | |
|---|---|---|---|---|---|
| | | | «удовлетворительно» (пороговый) | «хорошо» (средний) | «отлично» (высокий) |
| ОПК-3.2 Выбор и обоснование организационно-технических мероприятий по защите информации в информационных системах. | **Правильно определяет** методологию обоснование организационно-технических мероприятий по защите информации в информационных системах. (ЗН-1) | Ответы на вопросы №1 - 41 к экзамену | Затрудняется в четком определении методологии обоснования организационно-технических мероприятий по защите информации в информационных системах. | Определяет основные принципы и методологию организационно-технических мероприятий по защите информации в информационных системах. | Демонстрирует глубокие знания принципов и методологии обоснования организационно-технических мероприятий по защите информации в информационных системах. |
| | **Демонстрирует** навыки, как проводить организационно-технические мероприятия по защите информации в информационных системах (У-1) | Ответы на вопросы №1 - 41 к экзамену | Демонстрирует слабые навыки проведения организационно-технических мероприятий по защите информации в информационных системах. | Демонстрирует с ошибками проведение организационно-технических мероприятий по защите информации в информационных системах | Демонстрирует хорошие навыки проведения организационно-технических мероприятий по защите информации в информационных системах |
| | **Перечисляет и приводит примеры** решения задач организационно-технических мероприятий по защите информации в информационных системах (Н-1) | Ответы на вопросы №1 – 41 к экзамену | Затрудняется с решением задач организационно-технических мероприятий по защите информации в информационных системах. | Справляется с решением типовых задач организационно-технических мероприятий по защите информации в информационных системах. | Демонстрирует хорошие навыки и умения решения задач организационно-технических мероприятий по защите информации в информационных системах. |

| | | | | | |
|---|---|---|---|---|---|
| ПК-3.3 Применение методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности. | **Правильно определяет** применение методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности (ЗН-2) | Ответы на вопросы №1 - 41 к экзамену | Затрудняется в определении методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности. | Определяет основные принципы и методологию организационно-технических мероприятий по защите информации в информационных системах. | Демонстрирует глубокие знания принципов и методологии обоснования организационно-технических мероприятий по защите информации в информационных системах. |
| | **Демонстрирует** навыки применения методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности (У-2) | Ответы на вопросы №1 - 41 к экзамену | Демонстрирует слабые навыки проводить организационно-технические мероприятия по защите информации в информационных системах. | Демонстрирует с ошибками навыки проводить организационно-технические мероприятия по защите информации в информационных системах | Демонстрирует хорошие навыки проведения организационно-технических мероприятий по защите информации в информационных системах |
| | **Перечисляет и приводит примеры** решения задач обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности (Н-2) | Ответы на вопросы №1 - 41 к экзамену | Затрудняется с решением задач организационно-технических мероприятий по защите информации в информационных системах. | Справляется с решением типовых задач организационно-технических мероприятий по защите информации в информационных системах. | Демонстрирует хорошие навыки и умения решения задач организационно-технических мероприятий по защите информации в информационных системах. |

Шкала оценивания соответствует СТО СПбГТИ(ТУ):

По дисциплине промежуточная аттестация проводится в форме экзамена, шкала оценивания – балльная («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

**3. Типовые контрольные задания для проведения промежуточной аттестации**

**а) Вопросы для оценки знаний, умений и навыков, сформированных у студента по компетенции ПК-3:**

1. Теоретические основы информационной безопасности. Базовые понятия.
2. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом.
3. Защита от несанкционированного доступа. Модели безопасности.
4. Основы криптографии. Основные понятия. Классификация шифров.
5. Симметричные шифры. Схема Фейстеля. Шифр DES.
6. Шифр ГОСТ 28147-89. Шифр Blowfish. Управление криптографическими ключами для симметричных шифров.
7. Защита информации в IP-сетях.
8. Протокол защиты электронной почты S/MIME.
9. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей.
10. Межсетевые экраны.
11. Анализ и управление рисками в сфере информационной безопасности.
12. Управление рисками. Модель безопасности с полным перекрытием.
13. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001.
14. ГОСТ Р ИСО/МЭК 17799:2005 «Информационная технология. Практические правила управления информационной безопасностью».
15. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
16. Методики построения систем защиты информации. Модель Lifecycle Security.
17. Управление доступом, выявление уязвимостей. Управление доступом к файлам на NTFS.
18. Управление доступом в СУБД SQL SERVER.
19. Выявление уязвимостей с помощью Microsoft Baseline Security analyzer.
20. Использование сканеров безопасности для получения информации о хостах в сети.
21. Модель Харрисона–Рузо–Ульмана. Модель Белла ЛаПадула.
22. Ролевая модель безопасности.
23. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.
24. Асимметричные шифры.
25. Распределение ключей по схеме Диффи Хеллмана.
26. Криптографическая система RSA.
27. Криптографическая система Эль Гамаля.
28. Совместное использование симметричных и асимметричных шифров. Хэш-функции. Хэш-функции без ключа. Алгоритм SHA-1.
29. Защита информации в IP-сетях.
30. Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS.
31. Протоколы IPSec и распределение ключей. Межсетевые экраны.
32. Модель многоуровневой защиты. Методика управления рисками, предлагаемая Майкрософт.
33. Методики и программные продукты для оценки рисков. Методика CRAMM.
34. Методика FRAP. Методика OCTAVE.
35. Методика RiskWatch. Проведение оценки рисков в соответствии с методикой Майкрософт.
36. Встроенный межсетевой экран (Firewall) Windows Server.

37. Использование цифровых сертификатов.
38. Создание центра сертификации (удостоверяющего центра) в Windows Server.
39. Шифрование данных при хранении – файловая система EFS.
40. Использование Microsoft Security Assessment Tool.
41. «Kaspersky Security Center». Установка Kaspersky Security Center.

При сдаче экзамена, студент получает два вопроса сформированных на основе перечня, приведенного выше.

Время подготовки студента к устному ответу на вопросы - до 30 мин.

**5. Методические материалы для определения процедур оценивания знаний, умений и навыков, характеризующих этапы формирования компетенций.**

Промежуточная аттестация по дисциплине проводится в соответствии с требованиями СТП СТО СПбГТИ(ТУ) 016-2015. КС УКДВ Порядок проведения зачетов и экзаменов.