**Федеральное государственное автономное образовательное учреждение высшего образования**
**«Санкт-Петербургский политехнический университет Петра Великого»**

---

УТВЕРЖДАЮ
Директор ИКНК
_____ Д.П. Зегжда
«17» июня 2024 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## «Защита информации»

| | |
|---|---|
| Разработчик | Высшая школа программной инженерии |
| Направление (специальность) подготовки | 09.03.04 Программная инженерия |
| Наименование ООП | 09.03.04_01 Технология разработки и сопровождения качественного программного продукта |
| Квалификация (степень) выпускника | **бакалавр** |
| Образовательный стандарт | **СУОС** |
| Форма обучения | **Очная** |

СОГЛАСОВАНО
Руководитель ОП
_____ А.В. Петров
«21» мая 2024 г.

Соответствует СУОС
Утверждена протоколом заседания высшей школы "ВШПИ"
от «21» мая 2024 г. № 1

РПД разработали:
Специалист по учебно-методической работе 1 категории Т.А. Вишневская
Старший преподаватель Е.С. Орлов

## 1. Цели и планируемые результаты изучения дисциплины

### Цели освоения дисциплины

Цель изучения дисциплины «Защита информации» – сформировать специалистов, умеющих обоснованно и результативно применять существующие, осваивать и разрабатывать новые средства и методы обеспечения безопасности компьютерной информации.

### Результаты обучения выпускника

| Код | Результат обучения (компетенция) выпускника ООП |
|---|---|
| **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** |
| ИД-1 ОПК-3 | Осуществляет поиск и анализ стандартов в части информационной безопасности для их применения при разработке программного обеспечения |
| ИД-2 ОПК-3 | Формулирует и оценивает риски связанные с информационной безопасностью, возникающие при эксплуатации программных систем |
| **ПК-3** | **Способен решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности** |
| ИД-1 ПК-3 | Осуществляет выбор способов защиты программного обеспечения от несанкционированного доступа |
| ИД-2 ПК-3 | Разрабатывает программное обеспечение с учетом проблем информационной безопасности |

### Планируемые результаты изучения дисциплины

**знания:**

- Знает основные организации являющиеся разработчиками стандартов и источники публикации актуально информации в сфере безопасности
- Знает основные типы рисков связанных с безопасностью возникающих при разработке программного обеспечения
- Знает основные подходы к защите программного обеспечения и пользовательских данных от несанкционированного доступа
- Знает основные проблемы информационной безопасности и меры борьбы с ними

**умения:**

- Умеет выбрать стандарт описывающий область и процессы необходимые для разработки программного обеспечения
- Умеет применять методы оценки рисков в части обеспечения безопасности при разработке программного обеспечения
- Умеет применять основные алгоритмы шифрования данных, обфускации программного кода и разграничения доступа к информации
- Умеет применять при разработке программного обеспечения современные криптографические методы защиты компьютерной информации

**навыки:**

- Владеет основными методами обеспечения безопасности при разработке программных систем
- Владеет методами анализа рисков возникающих при эксплуатации программных систем
- Владеет навыками использования существующих библиотек и фреймворков, реализующих алгоритмы защиты от несанкционированного доступа

## 2. Место дисциплины в структуре ООП

В учебном плане дисциплина «Защита информации» относится к модулю «Модуль цифровых компетенций».

Изучение дисциплины базируется на результатах освоения следующих дисциплин:

- Операционные системы
- Администрирование компьютерных систем

## 3. Распределение трудоёмкости освоения дисциплины по видам учебной работы и формы текущего контроля и промежуточной аттестации

### 3.1. Виды учебной работы

| Виды учебной работы | Трудоемкость по семестрам |
|---|---|
| | Очная форма |
| Лекционные занятия | 50 |
| Практические занятия | 24 |
| Самостоятельная работа | 39 |
| Часы на контроль | 16 |
| Промежуточная аттестация (экзамен) | 11 |
| Промежуточная аттестация (зачет) | 4 |
| **Общая трудоемкость освоения дисциплины** | 144, ач |
| | 4, зет |

### 3.2. Формы текущего контроля и промежуточной аттестации

| Формы текущего контроля и промежуточной аттестации | Количество по семестрам |
|---|---|
| | Очная форма |
| **Текущий контроль** | |
| Расчетно-графические работы, шт. | 1 |
| **Промежуточная аттестация** | |
| Зачеты, шт. | 1 |
| Экзамены, шт. | 1 |

## 4. Содержание и результаты обучения

## 4.1 Разделы дисциплины и виды учебной работы

| № раздела | Разделы дисциплины, мероприятия текущего контроля | Очная форма | | |
|---|---|---|---|---|
| | | Лек, ач | Пр, ач | СР, ач |

| | | | | |
|---|---|---|---|---|
| 1. | ВВЕДЕНИЕ В ДИСЦИПЛИНУ ЗАЩИТА ИНФОРМАЦИИ | 1 | 0 | 0 |
| 2. | ИСТОЧНИКИ, РИСКИ И ФОРМЫ АТАК НА ИНФОРМАЦИЮ | | | |
| 2.1. | Угрозы безопасности информационных технологий | 1 | 2 | 2 |
| 2.2. | Модель нарушителя | 1 | 0 | 3 |
| 2.3. | Уязвимости информационных систем и пути нанесения ущерба | 1 | 0 | 4 |
| 3. | ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ | | | |
| 3.1. | Управление рисками | 1 | 0 | 2 |
| 3.2. | Меры противодействия угрозам безопасности | 1 | 2 | 3 |
| 3.3. | Основные принципы построения системы защиты | 1 | 0 | 4 |
| 4. | КРИПТОГРАФИЧЕСКИЕ МОДЕЛИ | | | |
| 4.1. | Шифрсистемы | 2 | 0 | 3 |
| 4.2. | Теоретико-информационная оценка криптостойкости шифрсистем | 2 | 0 | 3 |
| 5. | АЛГОРИТМЫ ШИФРОВАНИЯ | | | |
| 5.1. | Архитектура современных блочных шифров | 2 | 0 | 3 |
| 5.2. | Протоколы шифрования | 2 | 2 | 3 |
| 5.3. | Криптосистемы с открытым ключом | 2 | 2 | 3 |
| 5.4. | Способы контроля целостности сообщения | 2 | 0 | 3 |
| 5.5. | Электронная цифровая подпись | 2 | 0 | 3 |
| 5.6. | Управление криптографическими ключами | 2 | 0 | 2 |
| 6. | МОДЕЛИ БЕЗОПАСНОСТИ ОСНОВНЫХ ОС | | | |
| 6.1. | Механизмы произвольного (дискреционного) разграничения доступа | 1 | 0 | 3 |
| 6.2. | Механизмы принудительного (мандатного) разграничения доступа. Модель TE (Type Enforcement) | 2 | 2 | 2 |
| 6.3. | Механизмы принудительного (мандатного) доступа. Модель Белла — Лападулы. | 2 | 2 | 2 |
| 6.4. | Механизмы создания замкнутой программной среды. | 1 | 1 | 3 |
| 7. | АЛГОРИТМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ | | | |
| 7.1. | Классификация схем аутентификации | 2 | 0 | 0 |
| 7.2. | Реализация механизмов аутентификации в современных ОС | 2 | 2 | 2 |

| | | | | |
|---|---|---|---|---|
| 8. | УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | | | |
| 8.1. | Возникновение уязвимостей в следствии некорректной работы с памятью | 2 | 2 | 2 |
| 8.2. | Атаки на приложения методом внедрения кода (Code Injection) | 2 | 2 | 2 |
| 8.3. | Разрушающие программные средства. | 1 | 0 | 2 |
| 8.4. | Анализ кода на предмет наличия уязвимостей. | 1 | 1 | 3 |
| 9. | МНОГОУРОВНЕВАЯ ЗАЩИТА КОРПОРАТИВНЫХ СЕТЕЙ | | | |
| 9.1. | Уязвимости IP-сетей, сетевых ОС и прикладных сервисов | 2 | 0 | 2 |
| 9.2. | Защищенный транспортный протокол SSL | 2 | 2 | 2 |
| 9.3. | Межсетевые экраны | 2 | 0 | 2 |
| 9.4. | Системы обнаружения вторжений | 2 | 2 | 2 |
| 10. | СТАНДАРТЫ БЕЗОПАСНОСТИ | | | |
| 10.1. | Руководящие документы Гостехкомиссии | 2 | 0 | 0 |
| 10.2. | Международные стандарты | 1 | 0 | 0 |
| **Итого по видам учебной работы:** | | 50 | 24 | 39 |
| Зачеты, ач | | | | 7 |
| Экзамены, ач | | | | 14 |
| **Часы на контроль, ач** | | | | 16 |
| **Промежуточная аттестация (экзамен)** | | 11 | | |
| **Промежуточная аттестация (зачет)** | | 4 | | |
| **Общая трудоёмкость освоения: ач / зет** | | 144 / 4 | | |

## 4.2. Содержание разделов и результаты изучения дисциплины

| Раздел дисциплины | Содержание |
|---|---|
| **1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ ЗАЩИТА ИНФОРМАЦИИ** | Введение в дисциплину "Защита информации". Основные виды угроз безопасности. Финансовые потери нарушения информационной безопасности. |
| **2. ИСТОЧНИКИ, РИСКИ И ФОРМЫ АТАК НА ИНФОРМАЦИЮ** | |
| **2.1. Угрозы безопасности информационных технологий** | Обобщенная схема реализации угроз. Классификация преднамеренных угроз. Вид источника угроз. Характер и цель атаки. Пути нанесения ущерба. Используемые уязвимости. |
| **2.2. Модель нарушителя** | Неформальная модель нарушителя : категория , мотивы действия, квалификация, ограничения и предположения. Потенциал нападения. Качественная оценка потенциала нападения. |
| **2.3. Уязвимости информационных систем и пути нанесения ущерба** | Уязвимости и этапы жизненного цикла АС. Уязвимости этапа проектирования и реализации. Уязвимости этапа внедрения и эксплуатации. Уязвимости этапа вывода из эксплуатации. |
| **3. ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ** | |
| **3.1. Управление рисками** | Принцип «разумной достаточности.<br>Оценка вероятности реализации угрозы. Методики управления рисками. Взаимосвязь основных понятий безопасности ИТ |
| **3.2. Меры противодействия угрозам безопасности** | Законы РФ . Информационные ресурсы ограниченного доступа. Права, обязанности и ответственность субъектов.Политика безопасности и программа безопасности.<br>Сервисы и услуги безопасности. Стойкости функции безопасности. Взаимосвязь мер обеспечения информационной безопасности. |
| **3.3. Основные принципы построения системы защиты** | Системы с полным перекрытием. Системность. Комплексность. Достаточность. Непрерывность. Изолированность. Разделение полномочий и персональная ответственность. |
| **4. КРИПТОГРАФИЧЕСКИЕ МОДЕЛИ** | |
| **4.1. Шифрсистемы** | Основные понятия и история криптологии. Классификация криптосистем. Классификация шифрсистем. Простые шифры |
| **4.2. Теоретико-информационная оценка криптостойкости шифрсистем** | Теоретико-информационная оценка криптостойкости шифрсистем Совершенно безопасные системы. Расстояние единственности |

| **5. АЛГОРИТМЫ ШИФРОВАНИЯ** | |
|---|---|
| **5.1. Архитектура современных блочных шифров** | Практическая стойкость шифра. Современные методы и технологии криптоанализа. Итерированные блочные шифры. Выбор основных параметров. Требования к шифрам первого поколения. Сеть Фейстела. |
| **5.2. Протоколы шифрования** | DES, IDEA, AES, ГОСТ 28147-89. Режимы простой замены, гаммирования, гаммирования с обратной связью. Математические модели, особенности и области применения |
| **5.3. Криптосистемы с открытым ключом** | Необратимые преобразования с лазейкой. Система открытого шифрования RSA. Математическая модель. Протокол применения. Анализ криптостойкости. Сравнительный анализ шифрования с секретным ключом и открытого шифрования. Обеспечение имитостойкости |
| **5.4. Способы контроля целостности сообщения** | Хэш-функция. Требования к криптографической хэш-функции. Криптостойкость хэш-функций. Архитектура хэш-функции.. Стандарт функции хэширования ГОСТ Р34.11-94. Основные характеристики и математическая модель. Стандарт функции хэширования SHA-1, 2. Основные характеристики и математическая модель. Протоколы контроля целостности с использованием хэш-функции. Коды аутентификации сообщения. Математическая модель и основные характеристики. HMAC. Математическая модель и основные характеристики. Протокол контроля целостности. Шифрование с контролем целостности. Стандарт блочного шифрования ГОСТ 28147-89, режим выработки имитовставки. Математическая модель и основные характеристики. Протокол контроля целостности. Сравнительный анализ протоколов контроля целостности. Методы защиты от навязывания ранее переданных, задержанных или переадресованных сообщений |
| **5.5. Электронная цифровая подпись** | Модель нарушителя и требования к ЭЦП. ЭЦП RSA, математическая модель, анализ криптостойкости, протокол применения. ЭЦП ElGamal, математическая модель, анализ криптостойкости. Сравнение ЭЦП ElGamal и ЭЦП RSA. ЭЦП DSA, математическая модель, анализ криптостойкости. Математические основы криптографии на эллиптических кривых (ЭК). ЭЦП на ЭК (ГОСТ Р34.10-2001, ECDSA), математическая модель, анализ криптостойкости, протокол применения. Сравнительные характеристики ЭЦП. Хэш-функции в протоколах цифровой подписи |

| | |
|---|---|
| **5.6. Управление криптографическими ключами** | Жизненный цикл ключей и функции управления ключами. Генерация криптографических ключей, криптографические генераторы псевдослучайных последовательностей, генерация больших простых чисел. Управление ключами в криптосистемах с секретным ключом, сравнительный анализ протоколов децентрализованного и централизованного управления ключами. Управление ключами в криптосистемах с открытым ключом. Сертификат открытого ключа. Удостоверяющий центр и его функции. Протоколы сертификации и кросс-сертификации. Юридические аспекты использования ЭЦП. Гибридные криптосистемы на основе открытого шифрования и открытого распределения ключей системы. |
| **6. МОДЕЛИ БЕЗОПАСНОСТИ ОСНОВНЫХ ОС** | |
| **6.1. Механизмы произвольного (дискреционного) разграничения доступа** | Режимы доступа к файлам (UNIX bits), списки контроля доступа (ACL). Права доступа и привелегии. Недостатки модели произвольного доступа. |
| **6.2. Механизмы принудительного (мандатного) разграничения доступа. Модель TE (Type Enforcement)** | Принципы принудительного разграничения доступа. Модель TE (Type Enforcement). Реализация принудительного доступа в ОС Linux - AppArmor, SELinux targeted. |
| **6.3. Механизмы принудительного (мандатного) доступа. Модель Белла — Лападулы.** | Обеспечение контроля над информационными потоками. Метки (уровни безопасности). SELinux MLS/MCS. AstraLinux PARSEC. |
| **6.4. Механизмы создания замкнутой программной среды.** | Необходимость замкнутой программной среды для обеспечения безопасности. Контроль целостности файлов. Linux IMA/EVM. |
| **7. АЛГОРИТМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ** | |
| **7.1. Классификация схем аутентификации** | Аутентификация субъектов. Идентификация и аутентификация. Классификация схем аутентификации. Требования к протоколу аутентификации. Слабая аутентификация (парольная защита). Сильная аутентификация. Аутентификация с нулевой передачей знаний. Протокол Fiat-Shmir, математическая модель, протокол применения, анализ стойкости |
| **7.2. Реализация механизмов аутентификации в современных ОС** | Хранение паролей и аутентификация в операционной системе Windows. Хранение паролей в операционной системе Unix. Аутентификация в веб-сервисах. |
| **8. УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** | |

| | |
|---|---|
| **8.1. Возникновение уязвимостей в следствии некорректной работы с памятью** | Переполнение стека. Переполнение кучи. Уязвимости форматной строки. Эксплуатация уязвимостей некорректной работы с памятью. |
| **8.2. Атаки на приложения методом внедрения кода (Code Injection)** | Атаки методом внедрения комманд (Command Injection). Атаки методом внедрения SQL-запросов (SQL Injection) |
| **8.3. Разрушающие программные средства.** | Классификация вредоносного ПО. Механизмы распространения и маскировки. Методы и организация защиты от вредоносного ПО |
| **8.4. Анализ кода на предмет наличия уязвимостей.** | Методы анализа исходного кода программного обеспечения. Статические и динамические анализаторы. Интеграция анализа кода в CI/CD. |
| **9. МНОГОУРОВНЕВАЯ ЗАЩИТА КОРПОРАТИВНЫХ СЕТЕЙ** | |
| **9.1. Уязвимости IP-сетей, сетевых ОС и прикладных сервисов** | Безопасность компьютерных сетей. Уязвимости IP-сетей, сетевых ОС и прикладных сервисов. Типовые сетевые атаки. Защищенный сетевой протокол IPSec, протоколы (TSP, AH), режимы использования и политика применения. |
| **9.2. Защищенный транспортный протокол SSL** | Стек протокола SSL. Handshake Protocol (протокол рукопожатия). Record Protocol (Протокол записи). Сравнение протоколов IPSec и SSL. |
| **9.3. Межсетевые экраны** | Основные функции. Типы МЭ. Построение и применение правил фильтрации. Конфигурация МЭ. Управление МЭ. |
| **9.4. Системы обнаружения вторжений** | Методы и технологии обнаружения вторжений. Безопасность Java-среды. Сканеры уязвимостей, Назначение и принципы работы |
| **10. СТАНДАРТЫ БЕЗОПАСНОСТИ** | |
| **10.1. Руководящие документы Гостехкомиссии** | Нормативные и технологические стандарты. « Концепция защиты СВТ и АС от несанкционированного доступа(НСД) к информации», «Показатели защищенности от НСД к информации», «Классификация АС и требования по защите информации». |
| **10.2. Международные стандарты** | понятия. ISO/IEC 15408 «Общий критерий оценки безопасности информационных технологий». Концепция документа. Основные понятия, требования безопасности (функциональные и доверия) и их структуризация, уровни доверия, профиль защиты). Принципы применения. |

## 5. Образовательные технологии

В преподавании курса используются преимущественно традиционные образовательные технологии: – лекции, –практические занятия.

## 6. Лабораторный практикум

Не предусмотрено

## 7. Практические занятия

| № раздела | Наименование практических занятий (семинаров) | Трудоемкость, ач |
|---|---|---|
| | | Очная форма |
| 1. | Анализ уязвимостей | 2 |
| 2. | Шифрование и дешифрование информации, обмен ключами | 3 |
| 3. | Создание и использование цифровых сертификатов | 2 |
| 4. | Создание удостоверяющего центра (центра сертификации) | 4 |
| 5. | Администрирование разрешений на файл и папки | 2 |
| 6. | Настройка принудительного разграничения доступа средствами AppArmor | 2 |
| 7. | Настройка принудительного разграничения доступа в ОС AstraLinux | 3 |
| 8. | Настройка межсетевого экрана | 2 |
| 9. | Настройка поддержки SSL/TLS для веб-приложения. | 2 |
| 10. | Методики и программные продукты для оценки рисков. | 2 |
| | **Итого часов** | 24 |

## 8. Организация и учебно-методическое обеспечение самостоятельной работы

СРС направлена на закрепление и углубление освоения учебного материала, развитие практических умений. СРС включает следующие виды самостоятельной работы студентов:

– работа с лекционным материалом, с рекомендованной учебной литературой;

– подготовка к практическим работам;

– подготовка к экзаменам.

Творческая проблемно-ориентированная самостоятельная работа студентов (ТСРС) направлена на развитие комплекса интеллектуальных универсальных (общекультурных) и профессиональных умений, повышение творческого потенциала студентов. ТСРС включает:

– поиск, обработка и презентация информации по печатным и электронным источникам информации по заданной проблеме дисциплины.

– выполнение курсового проекта.

Примерное распределение времени самостоятельной работы студентов

| Вид самостоятельной работы | Примерная трудоемкость, ач |
|---|---|
| | Очная форма |
| **Текущая СР** | |
| работа с лекционным материалом, с учебной литературой | 10 |
| опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях) | 4 |
| самостоятельное изучение разделов дисциплины | 6 |
| выполнение домашних заданий, домашних контрольных работ | 0 |
| подготовка к лабораторным работам, к практическим и семинарским занятиям | 10 |
| подготовка к контрольным работам, коллоквиумам | 0 |
| **Итого текущей СР:** | 30 |
| **Творческая проблемно-ориентированная СР** | |
| выполнение расчётно-графических работ | 0 |
| выполнение курсового проекта или курсовой работы | 30 |
| поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме | 10 |
| работа над междисциплинарным проектом | 0 |
| исследовательская работа, участие в конференциях, семинарах, олимпиадах | 0 |
| анализ данных по заданной теме, выполнение расчётов, составление схем и моделей на основе собранных данных | 0 |
| **Итого творческой СР:** | 40 |
| **Общая трудоемкость СР:** | 39 |

## 9. Учебно-методическое обеспечение дисциплины

### 9.1. Адрес сайта курса

https://dl.spbstu.ru/course/view.php?id=4065

### 9.2. Рекомендуемая литература

**Основная литература**

| № | Автор, название, место издания, издательство, год (годы) издания | Год изд. | Источник |
|---|---|---|---|
| 1 | Стельмашонок Е.В. Концепция обеспечения информационной безопасности корпоративных бизнес - процессов // Научно-технические ведомости СПбГТУ. 2005. №4(42) URL: http://elib.spbstu.ru/dl/local/ntv/2005/4(42)/24.pdf | 2005 | ЭБ СПбПУ |
| 2 | Столлингс В. Криптография и защита сетей: Москва: Вильямс, 2001. | 2001 | ИБК СПбПУ |

**Дополнительная литература**

| № | Автор, название, место издания, издательство, год (годы) издания | Год изд. | Источник |
|---|---|---|---|
| 1 | Нестеров С.А. Информационная безопасность и защита информации, 2011. URL: http://elib.spbstu.ru/dl/2451.pdf | 2011 | ЭБ СПбПУ |

**Ресурсы Интернета**

1. НОУ ИНТУИТ Курсы по теме Безопасность: https://www.intuit.ru/studies/courses
2. . Габидулин Э.М. и др. Защита информации Учебное пособие , МФТИ,2017: http://permsite.ru/files/2017/12/information_security_Z3WChDA.pdf

### 9.3. Технические средства обеспечения дисциплины

Программные требования: На компьютерах лаборатории должна быть установлены система виртуализации VirtualBox, виртуальные машины с ОС Debian Linux, CentOS Linux, AstraLinux SE.

## 10. Материально-техническое обеспечение дисциплины

Для успешного проведения курса необходимо использование локальной сети с сервером на 8-10 рабочих мест

## 11. Критерии оценивания и оценочные средства

### 11.1. Критерии оценивания

Для дисциплины «Защита информации» предусмотрены следующие формы аттестации: зачёт, экзамен. Дисциплина реализуется с применением системы индивидуальных достижений.

**Текущий контроль успеваемости**

Максимальное значение персонального суммарного результата обучения (ПСРО) по приведенной шкале - 100 баллов
Максимальное количество баллов приведенной шкалы по результатам прохождения двух точек контроля - 80 баллов.

Подробное описание правил проведения текущего контроля с указанием баллов по каждому контрольному мероприятию и критериев выставления оценки размещается в СДО в навигационном курсе дисциплины.

**Промежуточная аттестация по дисциплине**

Максимальное количество баллов по результатам проведения аттестационного испытания в период промежуточной аттестации – 20 баллов приведенной шкалы.

Промежуточная аттестация по дисциплине проводится в соответствии с расписанием.

*Промежуточная аттестация по дисциплине проводится по расписанию зачетов и экзаменов. Портфолио, представляемое на промежуточную аттестацию, включает работы, выполненные в течение семестра и размещенные в личном кабинете обучающегося в ЭИОС.*

*Получение оценок «зачтено» за все предусмотренные программой задания, размещенные в личном кабинете обучающегося в ЭИОС, является основанием проведения промежуточной аттестации по дисциплине.*

*Экзамен проводится в режиме устного собеседования.*

Результаты промежуточной аттестации, определяются на основе баллов, набранных в рамках применения, СИД

| Баллы по приведенной шкале в рамках применения СИД (ПСРО+ ПА) | Оценка по результатам промежуточной аттестации |
|---|---|
| | Экзамен/диф.зачет/зачет |
| 0 - 60 баллов | Неудовлетворительно/не зачтено |
| 61 - 75 баллов | Удовлетворительно/зачтено |
| 76 - 89 баллов | Хорошо/зачтено |
| 90 и более | Отлично/зачтено |

**11.2. Оценочные средства**

Оценочные средства по дисциплине представлены в фонде оценочных средств, который является неотъемлемой частью основной образовательной программы и размещается в электронной информационно-образовательной среде СПбПУ на портале etk.spbstu.ru

## 12. Методические рекомендации по организации изучения дисциплины

В соответствии с учебными планами дисциплина «Защита информации» включает следующие виды занятий:

1) лекции

2) практические занятия;

3) курсовое проектирование.

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических задач. Практические занятия направлены на закрепление лекционного материала.

Курсовые проекты призваны укрепить понимание принципов, изложенных в лекциях, и предоставить студенту возможность глубже понять как работают сервисы и механизмы безопасности в современных автоматизированных системах, а также почувствовать, что они способны не только понять, но а какой-то мере реализовать возможности защиты.

При выборе предлагаемых слушателям тем проектов следует рассматривать задачи, возникающие в самых различных отраслях и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете.

Проекты могут быть трех типов:

- исследовательские проекты;

- проекты по программной реализации сервисов и механизмов защиты на разных вычислительных платформах;

- проекты по изучению/реферированию дополнительной литературы.

Про результатам работы над проектом должен быть представлен отчет, содержащий

1. Титульный лист с указанием темы и автора
2. Наличие обязательных разделов:
    1. Обоснование выбора темы и цель работы
    2. Выводы
    3. Библиографию, в том числе электронные ресурсы. Большинство ссылок должны быть за последние три года.

## 13. Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.