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

« 20 » мая 2019 г.

**Рабочая программа дисциплины**

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Направления подготовки**

**09.03.01 Информатика и вычислительная техника**
Направленности программы бакалавриата
Автоматизированные системы обработки информации и управления
Системы автоматизированного проектирования

**09.03.03 Прикладная информатика**
Направленность программы бакалавриата
Прикладная информатика в химии

Квалификация

**Бакалавр**

Форма обучения

**Очная**

Факультет **информационных технологий и управления**

Кафедра **систем автоматизированного проектирования и управления**

Санкт-Петербург
2019

**Б1.О.17**

**ЛИСТ СОГЛАСОВАНИЯ**

| Должность разработчика | Подпись | Ученое звание, инициалы, фамилия |
|---|---|---|
| Доцент | | Г.В. Кузнецова |

Рабочая программа дисциплины «Информационная безопасность» обсуждена на заседании кафедры систем автоматизированного проектирования и управления
протокол от «18» апреля 2019 № 9

Заведующий кафедрой, д.т.н, профессор Т.Б. Чистякова

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

Председатель, к.т.н., доцент В.В. Куркина

СОГЛАСОВАНО

| | | |
|---|---|---|
| Руководитель направления подготовки «Информатика и вычислительная техника» | | профессор Т.Б. Чистякова |
| Руководитель направления подготовки «Прикладная информатика» | | доцент И.В. Новожилова |
| Директор библиотеки | | Т.Н. Старостенко |
| Начальник методического отдела учебно-методического управления | | Т.И. Богданова |
| Начальник УМУ | | С.Н.Денисенко |

**Содержание**

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

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

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения (дескрипторы) |
|---|---|---|
| ОПК-3<br>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-3.4<br>Выбор и обоснование организационно-технических мероприятий по защите информации в информационных системах | **знать** виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты, (ЗН-1)<br>**уметь** выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; (У-1)<br>**владеть** навыками работы с различными источниками информации (В-1) |
| | ОПК-3.5<br>Применение методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности | **знать** организационные, технические и программные методы и модели защиты (ЗН-2)<br>**уметь** применять методы защиты компьютерной информации при использовании и проектировании ИС в различных областях; (У-2)<br>**владеть** навыками работы с программно- инструментальными средствами (В-2) |
| ОПК-4<br>Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью | ОПК-4.1<br>Применение правовых основ защиты компьютерной информации, а также стандартов, норм и правил на различных стадиях жизненного цикла информационной системы | **знать** требования информационных систем и методы обеспечения информационной безопасности; (ЗН-3)<br>**уметь** проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе (У-3)<br>**владеть** навыками эксплуатирования и сопровождения информационных систем и сервисов (В-3) |

## 2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам обязательной части (Б1.О.17) и изучается на 4 курсе в 8 семестре.

Дисциплина базируется на знаниях, полученных студентами в курсах « «Операционные системы», «Разработка программных систем», «Вычислительные системы, сети и телекоммуникации», «Базы данных», «Правовые основы информатики».

Полученные в процессе изучения дисциплины «Информационная безопасность» знания, умения и навыки могут быть использованы при прохождении преддипломной практики, а также 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:** | **76** |
| занятия лекционного типа | 36 |
| занятия семинарского типа, в т.ч. | 36 |
| семинары, практические занятия | 36 |
| лабораторные работы | – |
| курсовое проектирование (КР или КП) | – |
| КСР | 4 |
| другие виды контактной работы (контроль) | |
| **Самостоятельная работа** | **32** |
| **Форма текущего контроля (**Кр, реферат, РГР, эссе) | Тестирование |
| **Форма промежуточной аттестации** (КР, КП , зачет, экзамен) | Экзамен (36) |

## 4 Содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

### 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 | Основы информационной безопасности. Основные понятия защиты информации. | 4 | 4 | | 4 | ОПК-3 | ОПК-3.4, ОПК-3.5 |
| 2 | Классификация средств защиты. Службы и механизмы обеспечения безопасности. | 4 | 2 | | 4 | ОПК-3 | ОПК-3.4, ОПК-3.5 |
| 3 | Идентификация и аутентификация. Управление доступом. | 4 | 4 | | 4 | ОПК-3 | ОПК-3.4, ОПК-3.5 |
| 4 | Основы криптографии. | 8 | 12 | | 6 | ОПК-3 | ОПК-3.4, ОПК-3.5 |
| 5 | Политики безопасности. | 4 | 2 | | 2 | ОПК-3; ОПК-4 | ОПК-3.4, ОПК-3.5, ОПК-4.1 |
| 6 | Стандарты безопасности. | 4 | 2 | | 4 | ОПК-3 | ОПК-3.4, ОПК-3.5 |
| 7 | Методы защиты программ от внешних воздействий. | 2 | 6 | | 4 | ОПК-3; ОПК-4 | ОПК-3.4, ОПК-3.5, ОПК-4.1 |
| 8 | Вопросы организации информационной безопасности на предприятии. | 6 | 4 | | 4 | ОПК-3; ОПК-4 | ОПК-3.4, ОПК-3.5, ОПК-4.1 |
| | Итого | 36 | 36 | | 32 | | |

### 4.2. Занятия лекционного типа

| № раздела-дисциплины | Наименование темы и краткое содержание занятия | Объем, акад. часы | Инновационная форма |
|---|---|---|---|
| 1. | Основные понятия и определения. Источники и риски функционирования информационных систем. Угрозы, атаки и уязвимости компьютерных систем. Основные задачи обеспечения безопасности информации. Законодательство РФ в области защиты информации. | 4 | |
| 2 | Классификация средств защиты. Службы и механизмы обеспечения безопасности.<br>Информация ограниченного доступа: институт тайны. | 4 | |
| 3 | Идентификация и аутентификация. Основные понятия и концепции. Биометрия. Управление доступом. | 4 | |
| 4 | Основы криптографии. Основные понятия и определения. Криптографические алгоритмы. Симметричные и ассиметричные алгоритмы.<br>Контроль целостности информации. Функции хеширования. Электронная подпись. | 8 | |
| 5 | Формальные модели безопасности. Политика безопасности. Основные модели и критерии защищенности. | 4 | |
| 6 | Стандарты безопасности. Роль и задачи стандартов. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. | 4 | |
| 7 | Методы защиты программ от внешних воздействий.<br>Антивирусная защита | 2 | |
| 8 | Организация информационной безопасности на предприятии. Правовые, организационные и технические мероприятия. Конфиденциальное делопроизводство. Ноу-хау. | 6 | |

### 4.3. Занятия семинарского типа

#### 4.3.1. Семинары, практические занятия

| № раздела дисциплины | Наименование темы и краткое содержание занятия | Объем, акад. часы | Примечание |
|---|---|---|---|
| 1 | Изучение законодательной базы в области защиты информации и информационных технологий | 2 | |
| 2 | Анализ угроз информационной системы. Формирование комплекса требований к системе защиты | 2 | |
| 3 | Биометрическая идентификации и элементы криптоанализа | 4 | |
| 4 | Криптографическое закрытие информации. Ассиметричные алгоритмы. Контроль подлинности, целостности и авторства сообщений | 4 | |
| 4 | Самостоятельная разработка программного продукта, реализующего алгоритм (элемент) криптографического закрытия информации | 6 | |
| 5 | Построение модели ролевой политики безопасности | 2 | |
| 6 | Изучение таксонометрии стандартов безопасности | 2 | |
| 7 | Изучения средств защиты программных продуктов. Изучение средств антивирусной безопасности | 6 | |
| 8 | Программы для ЭВМ и БД – объекты охраны интеллектуальной собственности. Комплексная защита | 4 | |

#### 4.3.2. Лабораторные занятия

Лабораторные занятия учебным планом не предусмотрены.

### 4.4.Самостоятельная работа обучающихся

| № раздела-дисциплины | Перечень вопросов для самостоятельного изучения | Объем, акад. часы |
|---|---|---|
| 1 | Безопасность функционирования информационных систем | 4 |
| 2 | Свойства защищенных систем | 4 |
| 3 | Механизмы подтверждения подлинности пользователя. Биометрия. Схема идентификации с нулевой передачей знаний | 4 |
| 4 | Исследование криптографических алгоритмов. Сравнение отечественного и американского стандартов шифрования. | 6 |
| 5 | Ролевая политика безопасности | 2 |
| 6 | Единые критерии безопасности информационных технологий | 4 |
| 7 | Средства обнаружения и защиты программ от разрушающих | 4 |

| № раздела-дисциплины | Перечень вопросов для самостоятельного изучения | Объем, акад. часы |
|---|---|---|
| | программных воздействий | |
| 8 | Программно-аппаратные средства защиты ЭВМ и сетей, ограничения доступа к компонентам сетей предприятий. | 4 |
| | **Итого** | **32** |

Самостоятельная работа проводится с целью углубления знаний по дисциплине и предусматривает:

– чтение студентами рекомендованной литературы и усвоение теоретического материала дисциплины;
– подготовку к лабораторным занятиям;
– работу с Интернет-источниками;
– подготовку к сдаче экзамена.

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

### 4.5 Тестирование

| | **Вопрос** | **Варианты ответов** |
|---|---|---|
| 1 | Установите хронологическую последовательность появления основополагающих документов с определением понятия «национальная безопасность». | • послание Президента США Конгрессу<br>• послание Президента РФ Федеральному собранию<br>• Концепция национальной безопасности РФ, утвержденная Указом Президента РФ |
| 2 | Основными задачами Федеральной службы безопасности РФ в области защиты информации являются … | • ведение реестра сертификатов ключей для цифровых подписей уполномоченных лиц федеральных органов государственной власти<br>• противодействие иностранным техническим разведкам<br>• обеспечение защиты сведений, составляющих государственную тайну<br>• осуществление мер, связанных с допуском граждан к сведениям, составляющим государственную тайну<br>• разработка и производство шифров и ключевых документов к шифровальным средствам<br>• допуск предприятий к проведению работ, связанных с использованием сведений, составляющих коммерческую тайну (за рубежом) |
| 3 | Согласно федеральному закону № 149-ФЗ от 27.07.2006 г. «Об информации, информационных | *Укажите не менее двух вариантов ответов*<br>• предоставляемую по соглашению лиц, участвующих в соответствующих отношени- |

| | | |
|---|---|---|
| | технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется на информацию … | ях<br>• свободно распространяемую<br>• распространение которой в РФ ограничивается или запрещается<br>• которая в соответствии с федеральными законами не подлежит предоставлению или распространению<br>• которая в соответствии с федеральными законами РФ подлежит предоставлению или распространению<br>• ограниченно распространяемую за пределами территории РФ |
| 4 | В Перечень сведений, составляющих государственную тайну, включена информация … | *Укажите не менее двух вариантов ответов*<br>• о разведывательной, контрразведывательной и оперативно-розыскной деятельности<br>• о результатах финансового мониторинга в отношении юридических и физических лиц РФ<br>• о достижениях науки и техники, о научно-исследовательских, опытно-конструкторских, проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства<br>• о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства<br>• о разработке, технологии, производстве, об объемах производства, о хранении, утилизации ядерных боеприпасов, их составных частей<br>• о содержании планов развития отдельных регионов РФ в части промышленности по изготовлению и ремонту вооружения и военной техники, объемов производства, поставок |
| 5 | Федеральный закон № 98-ФЗ от 29.07.2004 г. «О коммерческой тайне» регулирует отношения, связанные с … | *Укажите не менее двух вариантов ответов*<br>• установлением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам<br>• информацией коммерческой тайны, которая имеет коммерческую ценность в силу неизвестности ее третьим лицам<br>• прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам |

| | | |
|---|---|---|
| | | • изменением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам<br>• информацией органов государственной власти, иных государственных органов, органов местного самоуправления |
| 6 | Субъектами обеспечения безопасности выступают … | *Укажите не менее двух вариантов ответов*<br>• государство, осуществляющее функции в области безопасности через органы законодательной, исполнительной и судебной власти<br>• резиденты РФ, осуществляющие административные функции в области безопасности<br>• законодательство, регламентирующее отношения в сфере безопасности<br>• оборонные министерства и ведомства РФ<br>• граждане, которые в соответствии с законодательством обладают правами и обязанностями по участию в обеспечении безопасности РФ<br>• государственные, общественные и иные организации и объединения |
| 7 | Установите соответствие между этапами жизненного цикла компьютерных вирусов и их функциональными характеристиками:<br><br>1) инфицирование<br>2) латентная фаза<br>3) инкубационный период<br>4) этап выполнения целевых функций<br>5) фаза проявления | • ожидание активизации вируса<br>• процесс саморазмножения вируса<br>• процесс активизации и выполнения специальных функций вируса<br>• внедрение в компьютерную систему в целях ее заражения<br>• процесс сопровождения визуальными или звуковыми эффектами<br>• процесс самоуничтожения вируса |
| 8 | Установите соответствие между способами и признаками разграничения доступа к информации<br><br>Разграничение по уровню секретности -1<br>Разграничение по специальным спискам -2<br>Разграничение по матрицам полномочий -3<br>Разграничение по специальным мандатам -4 | • Формирование двумерной матрицы, по строкам которой содержатся идентификаторы пользователей, а по столбцам – идентификаторы защищаемых элементов данных<br>• Защищаемые данные распределяются по массивам таким образом, чтобы в каждом массиве содержались данные всех уровней секретности<br>• Каждому защищаемому элементу присваивается персональная уникальная метка, доступ к этому элементу будет разрешен пользователю, который в своем запросе предъявит метку элемента<br>• Для каждого элемента защищаемых данных составляется перечень пользователей, имеющих право доступа к соответствующему элементу |

| | | |
|---|---|---|
| | | • Защищаемые данные распределяются по массивам таким образом, чтобы в каждом массиве содержались данные одного уровня секретности |
| 9 | Установите правильную последовательность этапов проведения аудита информационной безопасности на предприятии. | *Установите правильную последовательность в предложенной совокупности ответов*<br>анализ информации с целью оценки текущего уровня информационной безопасности предприятия<br>разработка рекомендаций по повышению уровня информационной безопасности предприятия<br>разработка регламента, устанавливающего состав и порядок проведения работ<br>сбор исходной информации: интервьюирование сотрудников предприятия, заполнение опросных листов, анализ предоставленной организационно-распорядительной и технической документации |
| 10 | Установите соответствие между видами и признаками преднамеренных угроз безопасности компьютерных систем:<br>1) по цели реализации угрозы<br>2) по принципу воздействия на компьютерную систему<br>3) по характеру воздействия на компьютерную систему<br>4) по способу активного воздействия на компьютерную систему (объект атаки) | *Установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов*<br>использование скрытых каналов<br>несанкционированное использование конфиденциальной информации<br>использование специально разработанных программ<br>опосредованное воздействие через других пользователей компьютерной системы<br>нарушение существующей политики безопасности |
| 11 | Установите соответствие между классом компьютерных вирусов и их типом:<br>1) по способу распространения в компьютерной системе<br>2) по способу заражения других объектов компьютерной системы<br>3) по деструктивным возможностям<br>4) по особенностям реализуемого алгоритма | *Установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов*<br>• неопасные<br>• потенциальные<br>• файловые<br>• резидентные<br>• «стелс»-вирусы |

| | | |
|---|---|---|
| 12 | Установите соответствие между видами и средствами идентификации и аутентификации пользователей:<br>1) биометрические системы<br>2) технические системы<br>3) парольные системы | *Установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов*<br>• набор символов<br>• iButton<br>• алгоритмы шифрования<br>• отпечатки пальцев |

## 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

Своевременное выполнение обучающимся мероприятий текущего контроля позволяет превысить (достигнуть) пороговый уровень («удовлетворительно») освоения предусмотренных элементов компетенций.

Результаты дисциплины считаются достигнутыми, если для всех элементов компетенций превышен (достигнут) пороговый уровень освоения компетенции на данном этапе.

Промежуточная аттестация по дисциплине проводится в форме экзамена.

К сдаче экзамена допускаются студенты, выполнившие все формы текущего контроля.

При сдаче экзамена, студент получает три вопроса из перечня вопросов, время подготовки студента к устному ответу - до 40 мин.

Билет №1

1. Информационная безопасность системы. Базовые понятия**: у**гроза, уязвимость, атака. Виды угроз. Классификация угроз
2. ГОСТ 28147-89. Режимы шифрования. Достоинства и недостатки. Имитовставка: понятие и применение.
3. Безопасность ПО. Методы и средства.

Фонд оценочных средств по дисциплине представлен в Приложении № 1.

## 7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

***а) печатные издания:***

1 Головин, Ю. А. Информационные сети : учеб. для вузов / Ю. А. Головин, А. А. Суконщиков, С. А. Яковлев. – Москва : Академия, 2011. – 376 с.

2 Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – 5-е изд., стер. – Москва : Академия, 2011. – 331 с.

***в) электронные учебные издания:***

3 Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров. – 5-е изд., стер. – Санкт-Петербург : Лань, 2019. – 324 с.

4 Тумбинская, М.В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М.В. Тумбинская, М.В. Петровский. – Санкт-Петербург : Лань, 2019. – 344 с.

5 Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие / С.Н. Никифоров. – 2-е изд., стер. – Санкт-Петербург : Лань, 2019. – 96 с.

6 Никифоров, С.Н. Методы защиты информации. Шифрование данных : учебное пособие / С.Н. Никифоров. – 2-е изд., стер. – Санкт-Петербург : Лань, 2019. – 160 с.

7 Модели и способы взаимодействия пользователя с киберфизическим интеллектуальным пространством : монография / И.В. Ватаманюк, Д.К. Левоневский, Д.А. Малов [и др.]. – Санкт-Петербург : Лань, 2019. – 176 с.

## 8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

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

**- электронно-библиотечные системы:**

- электронная справочная система правовой информации «Консультант+» http://www.consultant.ru
- «Электронный читальный зал – БиблиоТех» https://technolog.bibliotech.ru/;
- «Лань» https://e.lanbook.com/books/.
- http://www.viniti.msk.su/ - Всероссийский институт научной и технической информации (ВИНИТИ)
- http://www.icsti.su/portal/index.html - Международный центр научной и технической информации (МЦНТИ)
- http://www.vntic.org.ru/ - Всероссийский научно-технический информационный центр

## 9. Методические указания для обучающихся по освоению дисциплины

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

СТО СПбГТИ 020-2011. КС УКДВ. Виды учебных занятий. Лабораторные занятия. Общие требования к организации и проведению.

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 багаж знаний и вопросов 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;

изучение мультимедийных материалов;

работа со специально разработанными программными продуктами;

контроль знаний с помощью компьютерных тестов;

взаимодействие с обучающимися посредством электронной информационно-образовательной среды.

### 10.2. Программное обеспечение

В учебном процессе используется лицензионное системное и прикладное программное обеспечение, приведенное в таблице 1.

Таблица 1 – Лицензионное программное обеспечение

| Наименование программного продукта | Лицензия |
|---|---|
| Microsoft Windows 7, 8.1 | Лицензия по договору с СПбГТИ(ТУ) DreamSpark |
| Microsoft Visual Studio 2008, 2010, 2012 | |
| Microsoft Visual C++ 2008 | |
| Microsoft Microsoft .Net Framework 4.0, 4.5 | |
| Microsoft Access 2007, 2013 | |
| Microsoft Visio 2010 | |
| LibreOffice, Apache OpenOffice.org | Бесплатная лицензия |
| PGP | Ограниченная лицензия |

Кроме лицензионного программного обеспечения сторонних производителей при проведении учебных занятий широко используются проблемно-ориентированные программные комплексы для решения задач в области информатики и вычислительной техники, разработанные на кафедре САПРиУ СПбГТИ(ТУ) (таблица 2).

Таблица 2 – Используемые в учебном процессе проблемно-ориентированные программные комплексы, разработанные на кафедре САПРиУ СПбГТИ(ТУ)

| Наименование программного комплекса | Номер и дата выдачи свидетельства об официальной/государственной регистрации программы для ЭВМ |
|---|---|
| ПК для изучения средств и методов защиты программных продуктов (ПО «Мерлин») | 2016662700 от 28.09.2016 |

### 10.3. Информационные справочные системы

Правовые справочные системы «Консультант-Плюс», «Гарант».

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

Для проведения занятий по дисциплине на кафедре систем автоматизированного проектирования и управления СПбГТИ(ТУ) имеется необходимая материально-техническая база, соответствующая действующим санитарным и противопожарным правилам и нормам:

| Наименование компьютерного класса кафедры | Оборудование |
|---|---|
| Класс интегрированных систем проектирования и управления химико-технологическими процессами | 30 посадочных мест.<br>Учебная мебель, пластиковая доска.<br>Персональные компьютеры (15 шт.): двухядерный процессор Intel Core 2 Duo (2,33 ГГц); ОЗУ 4096 Мб; НЖМД 250 Гб; CD/DVD привод, DVD-RW; видеокарта NVIDIA GeForce 8500 GT; звуковая и сетевая карты, встроенные в материнскую плату.Персональные компьютерыобъединены в корпоративную вычислительную сеть кафедры и имеют выход в сеть «Интернет». |
| Класс информационных и интеллектуальных систем | 40 посадочных мест.<br>Учебная мебель, пластиковая доска.<br>Персональные компьютеры (20 шт.): четырехядерный процессор IntelCorei7-920 (2666 МГц), ОЗУ 6 Гб; НЖМД 250 Гб; CD/DVD привод, DVD-RW; видеокарта NVIDIAGeForceGT 220 (1024 Мб); звуковая и сетевая карты, встроенные в материнскую плату.Персональные компьютерыобъединены в корпоративную вычислительную сеть кафедры и имеют выход в сеть «Интернет». |
| Лекционная аудитория | 56 посадочных мест.<br>Мультимедийный проектор NECNP41. НоутбукAsusa6jнабазепроцессораIntelCoreDuoT2000.<br>Мультимедийная интерактивная доска ScreenMedia. |

Лицензионное системное и прикладное программное обеспечение, используемое в учебном процессе по дисциплине, перечислено в подразделе № 10.2.

## 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 28.08.2015г.

**Приложение № 1**

к рабочей программе дисциплины

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

**1. Перечень компетенций и этапов их формирования.**

| **Компетенции** | | |
|---|---|---|
| **Индекс** | **Формулировка** | **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 |
| ОПК-4 | Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью | 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-3.4 Выбор и обоснование организационно-технических мероприятий по защите информации в информационных системах | **знает** виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты | Правильные ответы на вопросы №1-5, 18-24 к экзамену | Слабо ориентируется в в информационной сфере. Использует терминологию с ошибками | Хорошо ориентируется в информационной сфере, немного путается в терминах | Хорошо ориентируется в информационной сфере. Может применить эти знания для решения текущих задач и приводит примеры |
| | **умеет** выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; | Правильные ответы на вопросы № 1-9, 14-24 к экзамену | Для решения поставленных задач не может предложить достаточного плана исследований или предложить мероприятия по защите (с ошибками) | Способен разработать план исследований в соответствии с поставленными задачами с помощью наводящих вопросов, предложить мероприятия по защите | Способен самостоятельно оценивать угрозы информационной безопасности, разработать план обследований, предложить мероприятия по защите |
| | **владеет** навыками работы с различными источниками информации | Правильные ответы на вопросы № 2-4,11-12,23-24 к экзамену | Слабо ориентируется в информационном массиве данных, не может выделить причинно-следственные связи и взаимозависимости | Ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости с небольшими ошибками | Уверенно ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости |
| ОПК-3.5 Применение методов обеспечения информационной безопасности при решении стандартных задач профессио- | **знает** организационные, технические и программные методы и модели защиты | Правильные ответы на вопросы № 10,11 к экзамену | Путается в перечислении средств и методов защиты | Перечисляет средства и методы защиты с небольшими ошибками | Уверенно и без ошибок перечисляет средства и методы защиты, принципы и особенности ведения работ |

| | | | | | |
|---|---|---|---|---|---|
| нальной деятельности | **умеет** применять методы защиты компьютерной информации при использовании и проектировании ИС в различных областях; | Правильные ответы на вопросы № 8-22,28-33 к экзамену | Имеет слабое представление о методах защиты Перечисляет основные этапы, способы и термины с ошибками | Может оценить риски и предложить методы защиты с помощью наводящих вопросов | Способен самостоятельно оценить риски, легко ориентируется в терминах. |
| | **владеет** навыками работы с программно- инструментальными средствами | Правильные ответы на вопросы №8-22, 28-33 к экзамену | Слабо ориентируется в теме, выполняет алгоритмы с ошибками | Выполняет алгоритмы с небольшими ошибками | Выполняет алгоритмы качественно и без ошибок |
| ОПК-4.1 Применение правовых основ защиты компьютерной информации, а также стандартов, норм и правил на различных стадиях жизненного цикла информационной системы | **знает** требования информационных систем и методы обеспечения информационной безопасности; | Правильные ответы на вопросы №1-5, 32-35 к экзамену | Слабо ориентируется в законодательной базе РФ в информационной сфере. Использует терминологию с ошибками | Хорошо ориентируется в законодательной базе РФ в информационной сфере, немного путается в терминах | Хорошо ориентируется в законодательной базе РФ в информационной сфере. Может применить эти знания для решения текущих задач и приводит примеры |
| | **умеет** проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе | Правильные ответы на вопросы № 1-5, 32-39 к экзамену | Для решения поставленных задач не может предложить достаточного плана исследований (с ошибками) | Способен разработать план исследований в соответствии с поставленными задачами с помощью наводящих вопросов | Способен самостоятельно разработать план исследований в соответствии с поставленными задачами |
| | **владеет** навыками эксплуатирования и сопровождения информационных систем и сервисов | Правильные ответы на вопросы № 12-19, 27-31 к экзамену | Слабо ориентируется в информационном массиве данных, не может выделить причинно-следственные связи и взаимозависимости | Ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости с небольшими ошибками | Уверенно ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости |

## 3. Типовые контрольные вопросы для подготовки к экзамену

1. Понятие информационной безопасности и основные проблемы. Основные задачи в области обеспечения защиты информации
2. Законодательство РФ в области защиты информации.№149-ФЗ «Об информации, информационных технологиях и о защите информации». Стратегия национальной безопасности, закон о государственной тайне.
3. Информационная безопасность системы. Базовые понятия**: у**гроза, уязвимость, атака. Виды угроз. Классификация угроз
4. Характеристики информации. Задачи информационной безопасности.
5. Способы обеспечения защиты: законодательные, административные, технические. Основные механизмы и службы защиты.
6. Теоретические основы информационной безопасности. Криптографические методы закрытия информации. Кодирование и шифрование.
7. Криптография. Основные понятия. Правило Кирхгоффа. Классификация методов шифрования.
8. Криптография: симметричные и асимметричные алгоритмы. Принцип действия, пример.
9. Гаммирование. Общее понятие и применение.
10. ГСЧ: типы, применение. Число инициализации.
10. ГОСТ 28147-89. Ключевая информация. Основной шаг криптоприобразования.
11. ГОСТ 28147-89. Режимы шифрования. Достоинства и недостатки. Имитовставка: понятие и применение.
12. RSA
13. Метод Эль-Гамаля
14. PGP. Принцип функционирования. Свойства ключа.
15. Хэш-функции. Определение, свойства, применение.
16. Электронная подпись. Понятие, алгоритм построения, использование.
17. Проверка целостности данных. Методы и функции.
18. Политики безопасности. Определение. Функции, виды, базовые представления.
19. Принципы организации доступа к информации.
20. Мандатная модель Белла-Ла Падулы. Достоинства и недостатки.
21. Дискреционная модель Харрисона-Руззо-Ульмана. Достоинства и недостатки.
22. Ролевая политика безопасности. Формальное представление. Достоинства и недостатки. Виды.
23. Стандарты безопасности. Основные цели и функции. Пользователи.
24. Стандарты безопасности. Обобщенные показатели.
25. Единые критерии безопасности информационных технологий. Основные понятия и положения. Профиль и проект защиты.
26. Единые критерии безопасности информационных технологий. Требования безопасности (функциональные и адекватности). Таксономия критериев.

27. Реестр и его использование для обеспечения безопасности программного продукта.
28. Безопасность БД. Методы и средства.
29. Безопасность ПО. Методы и средства.
30. Идентификация и аутентификация. Биометрическая защита.
31. Основы вирусологии. Классификация вирусов, жизненный цикл, средства защиты.
32. Структура системы защиты от несанкционированного доступа.
33. Статические и динамические характеристики среды.
34. Конфиденциальный документооборот. Коммерческая тайна. ФЗ № 98 «О коммерческой тайне»
35. Аудит ИБ на предприятии. Цели и задачи, последовательность действий.

**Вопросы для оценки сформированности элементов компетенции:**

ОПК-4: № 1-5,32-39
ОПК-3 № 6-35

К экзамену допускаются студенты, выполнившие все формы текущего контроля. При сдаче экзамена, студент получает три вопроса из перечня, приведенного выше.

Время подготовки студента к устному ответу на вопросы - до 40 мин.

**4. Методические материалы для определения процедур оценивания знаний, умений, навыков и (или) опыта деятельности, 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.