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
«_____» _____2019г.

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки

09.03.01Информатика и вычислительная техника

Направленность программы бакалавриата

Автоматизированные системы обработки информации и управления

Квалификация

Бакалавр

Форма обучения

Заочная

Факультет **информационных технологий и управления**

Кафедра **систем автоматизированного проектирования и управления**

Санкт-Петербург

2019

Б1.О.17

ЛИСТ СОГЛАСОВАНИЯ

Должность	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 года № 9

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

Одобрено учебно-методической комиссией факультета информационных технологий и управления
протокол от «15»мая2019 года№ 9

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

СОГЛАСОВАНО

Руководитель направления подготовки «Информатика и вычислительная техника»		профессор Т.Б. Чистякова
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 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 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) **уметь** выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; (У-1) **владеть** навыками работы с различными источниками информации (В-1)
	ОПК-3.5 Применение методов обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности	**знать** организационные, технические и программные методы и модели защиты(ЗН-2) **уметь** применять методы защиты компьютерной информации при использовании и проектировании ИС в различных областях; (У-2) **владеть** навыками работы с программно- инструментальными средствами (В-2)
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1 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) **уметь** проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе (У-3) **владеть** навыками эксплуатирования и сопровождения информационных систем и сервисов (В-3)

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.17 «Информационная безопасность» принадлежит к обязательной части. Дисциплина базируется на знаниях, полученных студентами в курсах « «Операционные системы», «Разработка программных систем», «Вычислительные системы, сети и телекоммуникации», «Базы данных», «Правовые основы информатики». Дисциплина изучается на 5-м курсе заочного бакалавриата.

3. Объем дисциплины

Вид учебной работы	Всего, академических часов
	заочная форма обучения
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	4/144
Контактная работа с преподавателем:	**14**
занятия лекционного типа	6
занятия семинарского типа, в т.ч.	
семинары, практические занятия	8
лабораторные работы	
курсовое проектирование (КР или КП)	-
КСР	
другие виды контактной работы (контроль)	9
Самостоятельная работа	**121**
Форма текущего контроля (Кр, реферат, РГР, эссе)	**3 кр**
Форма промежуточной аттестации (КР, КП , зачет, экзамен)	Экзамен (9)

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
			Семинары и/или практические занятия	Лабораторные работы		
1	Основы информационной безопасности. Основные понятия защиты информации.	0,5	1		10	ОПК-3
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	0,5			10	ОПК-3; ОПК-4;
3	Идентификация и аутентификация. Управление доступом.	0,5	1		10	ОПК-3; ОПК-4;
4	Основы криптографии.	2	2		28	ОПК-3; ОПК-4;
5	Политики безопасности.	0,5	0,5		13	ОПК-3; ОПК-4;
6	Стандарты безопасности.	0,5	0,5		20	
7	Методы защиты программ от внешних воздействий.	0,5	2		15	ОПК-4;
8	Вопросы организации информационной безопасности на предприятии.	1	1		15	ОПК-3; ОПК-4;
	Итого	6	8		121	

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.	0,5	
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	0,5	
3	Идентификация и аутентификация. Основные понятия и концепции. Биометрия. Управление доступом.	0,5	

4	Основы криптографии. Основные понятия и определения. Криптографические алгоритмы. Контроль целостности информации. Функции хеширования. Электронная подпись.	2	
5	Формальные модели безопасности. Политика безопасности. Основные модели и критерии защищенности.	0,5	
6	Стандарты безопасности. Роль и задачи стандартов. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	0,5	
7	Методы защиты программ от внешних воздействий. Антивирусная защита	0,5	
8	Организация информационной безопасности на предприятии. Правовые, организационные и технические мероприятия. Конфиденциальное делопроизводство. Интеллектуальная собственность и авторское право.	1	

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	1	
3	ПО «Daily». Биометрическая идентификации и элементы криптоанализа	1	
4-6	PGP. Криптографическое закрытие информации. Ассиметричные алгоритмы. Электронная подпись. Контроль целостности и авторства сообщений.	2	
4,5,7	«Itkey». Изучения средств защиты программных продуктов	3	
8	Программы для ЭВМ и БД – объекты охраны интеллектуальной собственности. Комплексная защита	1	

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	Основы информационной безопасности. Основные понятия защиты информации. ФЗ № 149. Безопасность функционирования информационных систем. Свойства защищенных систем	10
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	10
3	Идентификация и аутентификация. Управление доступом. Механизмы подтверждения подлинности пользователя. Парольная идентификация. Программно – аппаратные средства. Биометрия.	10
4	Основы криптографии. Исследование криптографических алгоритмов. Симметричное, ассиметричное шифрование. Классификация систем шифрования. Алгоритмы. Требования к криптосистемам. ГОСТ 28147-89. Алгоритмы контроля целостности. Функции хеширования, свойства, применение. Электронная подпись. Законодательство РФ. Функции, алгоритмы, применение. Системы распределения открытых ключей. Удостоверяющий центр.	28
5	Политики безопасности. Базовые структуры и функции. Мандатная, дискреционная и ролевая политики. Принципы построения, достоинства и недостатки.	13
6	Стандарты безопасности.	20
7	Методы защиты программ от внешних воздействий. Средства обнаружения и защиты программ от разрушающих программных воздействий Защита от копирования, контроль целостности, резервирование.	15
8	Вопросы организации информационной безопасности на предприятии. Законодательная база. Конфиденциальное делопроизводство. Режим коммерческой тайны. Государственная тайна. Защита интеллектуальной собственности. Организационные мероприятия. Программно-аппаратные средства защиты ЭВМ и сетей, ограничения доступа к компонентам сетей предприятий.	15
	Итого	**121**

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;
– выполнение контрольных работ;
– 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.

4.4.1 Темы контрольных работ

Задание по дисциплине включает три самостоятельных модуля

1. Аналитическое исследование

Задание подразумевает поиск информации в открытых источниках (в том числе Internet), ее аналитический обзор и сравнительный анализ результатов, и представление в виде отчета в тестовом формате или в виде мультимедийной презентации (в электронном и бумажном варианте).

2. Тестовое задание

Подготовьтесь к коллоквиуму по теме "Криптография". Ответьте на поставленные вопросы.

3. Практическое задание предполагает разработку программного продукта по заданной теме. Необходимо наличие исполняемого модуля, исходных данных и руководства пользователя, описывающего алгоритм работы программы, условия использования, принятые допущения и ограничения (в электронном и бумажном варианте).

1. Аналитическое исследованиеМетоды и средства обеспечения безопасности

Задание подразумевает поиск информации в открытых источниках (в том числе Internet), ее аналитический обзор и сравнительный анализ результатов, и представление в виде отчета в тестовом формате или в виде мультимедийной презентации (в электронном и бумажном варианте).

1. Политика безопасности организации. Правовой, организационный и технический аспект.
2. Обеспечение безопасности сайтов. Цель и сущность, объекты охраны, методы и средства.
3. Обеспечение безопасности базы данных. Угрозы, особенности, методы и средства защиты.
4. Биометрические средства идентификации.
5. Хэш-функции: понятие, принцип функционирования, свойства, особенности использование. Сравнительный анализ.
6. Электронная подпись: понятие, принцип функционирования, свойства, особенности использование. Инфраструктура открытых ключей.
7. Обеспечение безопасности при удаленном доступе к ресурсам.
8. Безопасность VPN.
9. Обеспечение целостности информации
10. Обеспечение безопасности сети организации
11. Безопасность промышленных сетей
12. Системы оценки рисков

2. Тестовое заданияКриптография

Подготовьтесь к коллоквиуму по теме "Криптография". Ответьте на поставленные вопросы.

1) Найдите десятичный эквивалент двоичного числа 01001101:__

2) Найдите двоичный эквивалент числа 100:_____

3) Потоковые шифры могут обрабатывать тексты:
   Посимвольно
   По битового
   По байтово
   По блочно

4) Алгоритмы шифрования бывают:
   Симметричные
   Ассиметричные
   Смешанные

5) При длине ключа N, размер ключевого пространства определяется по формуле:
   N!
   2^N
   2^N+1

6) Алгоритм RSA основан на следующем математическом обосновании:
   - проблема факторизации больших чисел
   - проблема дискретного логарифма
   - нахождение точек на эллиптической кривой

7) В каких алгоритмах шифрования используются более длинные ключи, для обеспечения их одинаковой криптостойкости:
   - в симметричных
   - в ассиметричных

8) Правило Кирхгоффа говорит о:
   - безопасности информационных систем
   - ключевой информации при шифровании
   - наличии слабых мест в информационной системе

9) Ключевой информацией ГОСТа 28147-89 являются
   - заблица замен
   - синхропосылка ГПЧ
   - ключ 256 бит
   - 8 ключей по 256 бит
   - размер регистра сдвига
   - количество проходов основного шага криптопреобразования

10) Синхропосылка это:
   - стартовой число ГПЧ
   - средство контроля целостности сообщения

- средство подтверждения авторства текста

11) Имитовставка используется для:
- контроля целостности
- проверки авторства
- является элементом цифровой подписи

12) Отметьте свойства хеш-функций, необходимые для ее криптографического использования:
- Однонаправленность
- Сжатие
- Стойкость к коллизиям
- Стойкость к нахождению первого прообраза
- Стойкость к нахождению второго прообраза

13) Сопоставьте режим шифрования и его особенности:

Простая замена		Одинаковые блоки исходного текста дают одинаковые блоки закрытого текста
Гаммирование		Для одинаковых блоков шифруемой информации необходимы различные синхропосылки
Гаммирование с обратной связью		Работает с зацеплением блоков и обеспечивает распространение ошибок

14) Электронная подпись позволяет подтвердить
- авторство сообщения
- целостность сообщения
- наличие защифрованного сообщения

15) Хеш - функции используются для:
- проверки целостности сообщений
- формирования цифровой подписи
- шифрования информации

16) Какие методы могут использоваться для идентификации пользователя:
- биометрические характеристики
- логин и пароль
- ключевая информация на внешнем носителе

17) К видам резервного копирования относятся:
-инкрементное
- полное
- архивное

18) Показателями криптостойкости являются:
- размер ключевого пространства
- среднее время, необходимое для криптоанализа
- время хранения ключевой информации

	Вопрос	**Варианты ответов**
1	Установите хронологическую последовательность появления основополагающих документов с определением понятия «национальная	• послание Президента США Конгрессу • послание Президента РФ Федеральному собранию

	безопасность».	• 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 • противодействие иностранным техническим разведкам • обеспечение защиты сведений, составляющих государственную тайну • осуществление мер, связанных с допуском граждан к сведениям, составляющим государственную тайну • разработка и производство шифров и ключевых документов к шифровальным средствам • 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 технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется на информацию … _____	*Укажите не менее двух вариантов ответов* • предоставляемую по соглашению лиц, участвующих в соответствующих отношениях • свободно распространяемую • распространение которой в РФ ограничивается или запрещается • которая в соответствии с федеральными законами не подлежит предоставлению или распространению • которая в соответствии с федеральными законами РФ подлежит предоставлению или распространению • ограниченно распространяемую за пределами территории РФ
4	В Перечень сведений, составляющих государственную тайну, включена информация … _____	*Укажите не менее двух вариантов ответов* • о разведывательной, контрразведывательной и оперативно-розыскной деятельности • о результатах финансового мониторинга в отношении юридических и физических лиц РФ • о достижениях науки и техники, о научно-исследовательских, опытно-конструкторских, проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства • о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства • о разработке, технологии, производстве, об

		объемах производства, о хранении, утилизации ядерных боеприпасов, их составных частей • 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* • установлением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам • информацией коммерческой тайны, которая имеет коммерческую ценность в силу неизвестности ее третьим лицам • 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 • информацией органов государственной власти, иных государственных органов, органов местного самоуправления
6	Субъектами обеспечения безопасности выступают … _____	*Укажите не менее двух вариантов ответов* • государство, осуществляющее функции в области безопасности через органы законодательной, исполнительной и судебной власти • резиденты РФ, осуществляющие административные функции в области безопасности • законодательство, регламентирующее отношения в сфере безопасности • оборонные министерства и ведомства РФ • граждане, которые в соответствии с законодательством обладают правами и обязанностями по участию в обеспечении безопасности РФ • государственные, общественные и иные организации и объединения

7	Установите соответствие между этапами жизненного цикла компьютерных вирусов и их функциональными характеристиками: 1) инфицирование 2) латентная фаза 3) инкубационный период 4) этап выполнения целевых функций 5) фаза проявления	• ожидание активизации вируса • процесс саморазмножения вируса • процесс активизации и выполнения специальных функций вируса • внедрение в компьютерную систему в целях ее заражения • процесс сопровождения визуальными или звуковыми эффектами • процесс самоуничтожения вируса
8	Установите соответствие между способами и признаками разграничения доступа к информации Разграничение по уровню секретности -1 Разграничение по специальным спискам -2 Разграничение по матрицам полномочий -3 Разграничение по специальным мандатам -4	• Формирование двумерной матрицы, по строкам которой содержатся идентификаторы пользователей, а по столбцам – идентификаторы защищаемых элементов данных • Защищаемые данные распределяются по массивам таким образом, чтобы в каждом массиве содержались данные всех уровней секретности • Каждому защищаемому элементу присваивается персональная уникальная метка, доступ к этому элементу будет разрешен пользователю, который в своем запросе предъявит метку элемента • 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* анализ информации с целью оценки текущего уровня информационной безопасности предприятия разработка рекомендаций по повышению уровня информационной безопасности предприятия разработка регламента, устанавливающего состав и порядок проведения работ сбор исходной информации: интервьюирование сотрудников предприятия, заполнение опросных листов, анализ предоставленной организационно-распорядительной и технической документации
10	Установите соответствие между ви-	*Установите соответствие между нумеровани-*

	дами и признаками преднамеренных угроз безопасности компьютерных систем: 1) по цели реализации угрозы 2) по принципу воздействия на компьютерную систему 3) по характеру воздействия на компьютерную систему 4) по способу активного воздействия на компьютерную систему (объект атаки)	*ными объектами в формулировке задания и вариантами ответов* использование скрытых каналов несанкционированное использование конфиденциальной информации использование специально разработанных программ опосредованное воздействие через других пользователей компьютерной системы нарушение существующей политики безопасности
11	Установите соответствие между классом компьютерных вирусов и их типом: 1) по способу распространения в компьютерной системе 2) по способу заражения других объектов компьютерной системы 3) по деструктивным возможностям 4) по особенностям реализуемого алгоритма	*Установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов* • неопасные • потенциальные • файловые • резидентные • «стелс»-вирусы
12	Установите соответствие между видами и средствами идентификации и аутентификации пользователей: 1) биометрические системы 2) технические системы 3) парольные системы	*Установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов* • набор символов • iButton • алгоритмы шифрования • отпечатки пальцев

3. Практическое задание Разработка программного продукта

Практическое заданиепредполагает разработку программного продукта по заданной теме. Для представления работы к защите необходимо наличие исполняемого модуля, исходных данных и руководства пользователя, описывающего алгоритм работы программы, условия использования, принятые допущения и ограничения (в электронном и бумажном варианте).

В рамках задания предлагается разработать программный продукт, реализующий один из криптографических алгоритмов, использующихся в системах защиты информации.

1. Реализовать алгоритм криптографического закрытия информации методом гаммирования, в качестве гаммы использовать случайную последовательность, получаемую с помощью генератора случайных чисел.

2. Реализовать алгоритм криптографического закрытия информации методом перестановок, ключевая информация должна быть варьируемой пользователем через соответствующий интерфейс.
3. Реализовать алгоритм криптографического закрытия информации методом стеганографии (например, прячем текст в картинке).
4. Реализовать алгоритм криптографического закрытия информации методом "поворотной решетки", размер решетки должен задаваться пользователей (с ограничением по максимальному размеру).
5. Реализовать алгоритм криптографического закрытия информации методом последовательно подстановки и последующей перестановки.
6. Шифрование с открытым ключом. Реализовать алгоритм ассиметричного шифрования RSA (с ограничениями по длине ключа).
7. Шифрование с открытым ключом. Реализовать алгоритм ассиметричного шифрования Диффи – Хеллмана.
8. Для исходного текста произвольной длины вычислить хеш-значение по алгоритму SHA-1(самостоятельно реализовать алгоритм)
9. Для исходного текста произвольной длины вычислить хеш-значения с использованием нескольких хеш-функций.
10. Разработать программный продукт по самостоятельно выбранной теме в области обеспечения безопасности.

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 учебных изданий, необходимых 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 электронных образовательных ресурсов, 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 ин-

формации (МЦНТИ)

- http://www.vntic.org.ru/ - Всероссийский научно-технический информационный центр

9. Методические указания для обучающихся по освоению дисциплины

Все виды занятий по дисциплине «Информационнаябезопасность» 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 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 почты.

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	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	

Наименование программного продукта	Лицензия
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
Учебно-методический комплекс «Система защиты программного продукта» (ItKey)	2007613442 (15.08.07)

10.3. Базы данных и 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. Учебная мебель, пластиковая доска. 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. Учебная мебель, пластиковая доска. 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. Учебная мебель.

Наименование компьютерного класса кафедры	Оборудование
	Мультимедийный проектор NECNP41. НоутбукAsusa6jнабазепроцессораIntelCoreDuoT2000. 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 28.08.2019г.

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, 18-26 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 профессиональной деятельности	**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

	умеетприменять 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 Перечисляетосновные 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
	умеетпроводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе	Правильные ответы на вопросы № 1-5, 32-36 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

Шкала оценивания соответствует СТО СПбГТИ(ТУ):промежуточная аттестация проводится в форме экзамена, шкала оценивания – балльная.

3. Типовые контрольные вопросы для подготовки к экзамену

1. Понятие информационной безопасности и основные проблемы. Федеральная служба безопасности РФ. 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. Оранжевая книга-первый стандарт. Таксономия критериев безопасности.
25. Стандарты безопасности. Обобщенные показатели сравнения стандартов.

26. Единые критерии безопасности информационных технологий. Основные понятия и положения. Профиль и проект защиты.
27. Единые критерии безопасности информационных технологий. Требования безопасности (функциональные и адекватности). Таксономия критериев.
28. Реестр и его использование для обеспечения безопасности программного продукта.
29. Безопасность БД. Методы и средства.
30. Безопасность ПО. Методы и средства.
31. Идентификация и аутентификация. Биометрическая защита.
32. Основы вирусологии. Классификация вирусов, жизненный цикл, средства защиты.
33. Структура системы защиты от несанкционированного доступа.
34. Статические и динамические характеристики среды.
35. Конфиденциальный документооборот. Коммерческая тайна. ФЗ № 98 «О коммерческой тайне»
36. Аудит ИБ на предприятии. Цели и задачи, последовательность действий.

Вопросы для оценки сформированности элементов компетенции:

ОПК-3: № 1-5,32-36
ОПК-4 № 6-28, 29-36

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.