

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Пекаревский Борис Владимирович
Должность: Проректор по учебной и методической работе
Дата подписания: 15.11.2023 16:20:58
Уникальный программный ключ:
3b89716a1076b80b2c167df0f27c09d01782ba84



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
12 апреля 2021 г.

Рабочая программа дисциплины
Информационная безопасность

Направление подготовки
27.03.04 Управление в технических системах

Направленность программы
**Информационно-техническое обеспечение автоматизированных систем
управления технологическими процессами**

Квалификация
Бакалавр

Форма обучения
очная

Факультет **информационных технологий и управления**
Кафедра **систем автоматизированного проектирования и управления**

Санкт-Петербург
2021

Б1.В.01

ЛИСТ СОГЛАСОВАНИЯ

Должность	Подпись	Ученое звание, инициалы, фамилия
Разработчик		Г.В. Кузнецова

Рабочая программа дисциплины «Информационная безопасность» обсуждена на заседании кафедры систем автоматизированного проектирования и управления протокол от «29» марта 2021 года №6

Заведующий кафедрой

Т.Б. Чистякова

Одобрено учебно-методической комиссией факультета информационных технологий и управления протокол от «07» апреля 2021 года №7

Председатель

В.В. Куркина

СОГЛАСОВАНО

Руководитель направления подготовки «Управление в технических системах»		доцент И.В. Рудакова
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	4
2. Место дисциплины в структуре образовательной программы	5
3. Объем дисциплины	5
4 Содержание дисциплины	6
4.1 Разделы дисциплины и виды занятий	6
4.2. Занятия лекционного типа	7
4.3. Занятия семинарского типа	8
4.4. Самостоятельная работа обучающихся	8
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	9
6. Фонд оценочных средств для проведения промежуточной аттестации	9
7. Перечень учебных изданий, необходимых для освоения дисциплины	10
8. Перечень электронных образовательных ресурсов, необходимых для освоения дисциплины	11
9. Методические указания для обучающихся по освоению дисциплины	12
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине	12
11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	14
12. Особенности освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья	14
<i>Приложение № 1 к рабочей программе дисциплины Фонд оценочных средств для проведения промежуточной аттестации по дисциплине «Информационная безопасность»</i>	<i>15</i>

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)
<p>ПК-2</p> <p>Способен выполнять формализацию данных и загрузку информации в АСУ, решать задачи диагностики нештатных ситуаций и отказов АСУТП, понимать структуру прикладных программных проектов на уровне АСУТП, выполнять разработку отдельных блоков прикладного программного обеспечения</p>	<p>ПК-2.3</p> <p>Применение методов обеспечения информационной безопасности при анализе, изучении и разработке блоков прикладного программного обеспечения АСУТП</p>	<p>знать</p> <ul style="list-style-type: none"> • требования информационных систем, виды угроз ИС и методы обеспечения информационной безопасности; • правовые основы защиты компьютерной информации; стандарты, • организационные, технические и программные методы и модели защиты (методы идентификации; методы и средства криптографии) <p>уметь</p> <ul style="list-style-type: none"> • применять методы защиты компьютерной информации в различных областях, в том числе АСУТП; • проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе; • выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; <p>владеть</p> <p>навыками работы с различными источниками информации, навыками эксплуатации информационных систем и сервисов; навыками работы с программно-инструментальными средствами</p>

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.01 «Информационная безопасность» принадлежит к вариативной части обязательных дисциплин. Дисциплина базируется на знаниях, полученных студентами в курсах «Информатика», «Основы права». Дисциплина изучается на 2-ом курсе в 3-м семестре.

3. Объем дисциплины

Вид учебной работы	Всего, академ. часов
	Очная форма обучения
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	3/108
Контактная работа с преподавателем:	56
занятия лекционного типа	18
занятия семинарского типа, в т.ч.	
семинары, практические занятия	36
лабораторные работы	
курсовое проектирование (КР или КП)	-
КСР	2
другие виды контактной работы (контроль)	
Самостоятельная работа	52
Форма текущего контроля (Кр, реферат, РГР, эссе)	-
Форма промежуточной аттестации (КР, КП, <u>зачет</u> , экзамен)	зачет

4 Содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часа.

4.1 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Занятия лекционного типа, акад. часы	Занятия семинарского типа, акад. часы		Самостоятельная работа, акад. часы	Формируемые компетенции	Формируемые индикаторы
			Семинары и/или практические	Лабораторные			
1	Защита информации.	2	4		4	ПК-2	ПК-2.3
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	2	2		6		
3	Идентификация и аутентификация.	2	4		2		
4	Основы криптографии.	2	10		8		
5	Политика безопасности.	2	2		2		
6	Стандарты безопасности.	2	2		4		
7	Информация ограниченного доступа. Конфиденциальное делопроизводство	2	4		6		
8	Защита результатов интеллектуальной деятельности (РИД).	2	4		10		
9	Вопросы организации информационной безопасности на предприятии. Безопасность АСУ ТП.	2	4		10		
	Итого	18	36		52		

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	2	Лекция-визуализация (ЛВ)
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	2	ЛВ
3	Идентификация и аутентификация. Основные понятия и концепции. Биометрия.	2	ЛВ
4	Основы криптографии. Основные понятия и определения. Криптографические алгоритмы. Контроль целостности информации. Функции хеширования. Электронная под-	2	ЛВ
5	Формальные модели безопасности. Политика безопасности. Основные модели и	2	ЛВ
6	Стандарты безопасности. Роль и задачи стандартов. Критерии и классы защищенности средств вычислительной техники и	2	ЛВ
7	Информация ограниченного доступа. Конфиденциальное делопроизводство	2	ЛВ
8	Защита результатов интеллектуальной деятельности. Патентное и авторское право. Объекты и	2	ЛВ
9	Организация информационной безопасности на предприятии. Правовые, организационные и технические мероприятия. Документальное обеспечение. Безопасность	2	ЛВ

4.3. Занятия семинарского типа

4.3.1. Семинары, практические занятия

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1	Основные понятия в области защиты информации и информационных технологий. Правовой и технический аспект	2	КтСм
2	Анализ угроз информационной системы. Формирование комплекса требований к системе защиты	2	КтСм
1-9	Законодательство РФ в области защиты информации. Работа с открытыми юридическими системами (Консультант +, Гарант)	4	КтСм
4	PGP. Криптографическое закрытие информации. Асимметричные алгоритмы. Контроль подлинности, целостности и авторства сообщений	2	КтСм
3	ПО «Daily». Биометрическая идентификация и элементы криптоанализа	4	КтСм
4	«Itkey». Изучения средств защиты программных продуктов	6	КтСм
5	Построение модели ролевой политики безопасности	2	КтСм
6	Изучение таксонометрии стандартов безопасности	2	КтСм
7	Информация ограниченного доступа. Законодательство РФ. Тайна	6	
8	Защита результатов интеллектуальной деятельности. Патентное и авторское право. Объекты и условия охраны Патентные исследования. Программы для ЭВМ и БД – объекты охраны интеллектуальной собственности. Комплексная защита	6	КтСм

4.3.2. Лабораторные занятия

Не предусмотрены.

4.4. Самостоятельная работа обучающихся

№ раздел-дисциплин	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
1	Безопасность функционирования информационных систем	4	Устный опрос
2,9	Безопасность АСУ ТП. Законодательство РФ. Методы и средства.	10	Устный опрос
3	Механизмы подтверждения подлинности пользователя. Биометрия. Схема идентификации с нулевой передачей знаний	2	Устный опрос

№ раздела дисциплин	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
4	Исследование Шеннона в области криптографии. Российский стандарт по криптографическим преобразованиям. Сравнение отечественного и американского стандартов шифрования.	6	Устный опрос
5	Ролевая политика безопасности	2	Устный опрос
6	Единые критерии безопасности информационных технологий	2	Устный опрос,
7	Информация ограниченного доступа	6	Отчеты по работам
4	Средства обнаружения и защиты программ от разрушающих программных воздействий	4	Устный опрос
8	Программно-аппаратные средства защиты ЭВМ и сетей, ограничения доступа к компонентам сетей предприятий.	4	Устный опрос
8	Защита РИД. Законодательство. Информационный поиск (маркетинговые и патентные исследования)	8	Устный опрос
9	Реферат по индивидуальному заданию	4	Доклад
	Итого	52	

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.

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.

Промежуточная аттестация по дисциплине проводится в форме зачета.

К сдаче зачета допускаются студенты, выполнившие все формы текущего

контроля.

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

Фонд оценочных средств по дисциплине представлен в Приложении № 1.

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

7. Перечень учебных изданий, необходимых для освоения дисциплины

а) печатные издания

1. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – 5-е изд., стер. – Москва : Academia, 2011. – 331 с. – ISBN 978-5-7695-7738-3.

2. Падерно, П. И. Качество информационных систем : учебник / П. И. Падерно, Е. А. Бурков, Н. А. Назаренко. – Москва : Академия, 2015. – 224 с. – ISBN 978-5-4468-1040-6.

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : Форум ; Москва : ИНФРА-М, 2013. – 415 с. – ISBN 978-5-8199-0331-5 (ИД Форум). – ISBN 978-5-16-003132-3 (Инфра-М).

б) электронные учебные издания:

4. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. – 3-е изд., перераб. – Санкт-Петербург : Лань, 2021. – 236 с. – ISBN 978-5-8114-5632-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com> (дата обращения: 20.03.2021). – Режим доступа: по подписке.

5. Москвитин, А. А. Данные, информация, знания: методология, теория, технологии : монография / А. А. Москвитин. – Санкт-Петербург : Лань, 2019. – 236 с. – ISBN 978-5-8114-3232-5. – Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com> (дата обращения: 20.03.2021). – Режим доступа: по подписке.

6. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. – 2-е изд., стер. – Санкт-Петербург : Лань, 2019. – 160 с. – ISBN 978-5-8114-4042-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com>(дата обращения: 20.03.2021). — Режим доступа: по подписке.

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

Учебный план, рабочая программа дисциплины и учебно-методические материалы (URL:<https://media.technolog.edu.ru>).

Образовательные Интернет-порталы:

- федеральный портал «Российское образование» (URL: <http://www.edu.ru>);

- российский портал открытого образования (URL: <https://openedu.ru>).

Электронно-библиотечные системы:

- «Электронный читальный зал – БиблиоТех» (URL: <https://technolog.bibliotech.ru>);

- «Лань» (URL: <https://e.lanbook.com/books>).

Информационно-аналитический портал «Научная электронная библиотека» (URL: <https://elibrary.ru>).

Открытые нормативно-правовые информационные системы:

- Единая база ГОСТов РФ «GostExpert» (URL: <https://gostexpert.ru>);

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

ГОСТ 34.10-2012. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

- База нормативно-правовой документации «Консультант Плюс» (URL: <http://www.consultant.ru>);

- Информационная система нормативных документов и стандартов «NormaCS» (URL: <https://www.normacs.ru>):

Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации»

Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне»

Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»

Гражданский кодекс, часть 4

Международные мультидисциплинарные аналитические реферативные базы данных научных публикаций:

- Web of Science (URL: <http://apps.webofknowledge.com>);

- Scopus (URL: <http://www.scopus.com>).

- Всероссийский институт научной и технической информации (ВИНИТИ) (<http://www.viniti.msk.su/>)

- Международный центр научной и технической информации (МЦНТИ) (<http://www.icsti.su/portal/index.html>)

- Всероссийский научно-технический информационный центр (<http://www.vntic.org.ru/>)

<http://www.gpntb.ru/> - Государственная публичная научно-техническая библиотека (ГПНТБ)

Официальные сайты

<http://www.fips.ru/> - Федеральная служба по интеллектуальной собственности

Журнал «Проблемы информационной безопасности. Компьютерные системы» Ежеквартальный журнал издательства СПбГПУ под редакцией проф. Зегжды П.Д.

Информационные технологии: ежемес. теорет. и прикл. науч.-техн. журн. – М. : Новые технологии, 2008– .

Журнал «Проблемы информационной безопасности. Компьютерные системы» Ежеквартальный журнал издательства СПбГПУ под редакцией проф.

9. Методические указания для обучающихся по освоению дисциплины

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

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

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

СТП СПбГТИ 048-2009. КС УКВД. 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 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	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)

10.3. Базы данных и информационные справочные системы

Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно»), обеспечивающая свободный доступ к интегральному каталогу образовательных Интернет-ресурсов и электронной библиотеке учебно-методических материалов, в том числе для высшего образования (URL: <http://window.edu.ru>).

Правовые справочные системы «Консультант-Плюс», «Гарант»; патентные базы РОСПАТЕНТА.

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 компьютеры объединены 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 Intel Core i7-920 (2666 МГц), ОЗУ 6 Гб; НЖМД 250 Гб; CD/DVD привод, DVD-RW; видеокарта NVIDIA GeForce GT 220 (1024 Мб); звуковая и сетевая карты, встроенные в материнскую плату. Персональные компьютеры объединены в корпоративную вычислительную сеть кафедры и имеют выход в сеть «Интернет».
Лекционная аудитория	56 посадочных мест. Учебная мебель. Мультимедийный проектор NEC NP41. Ноутбук Asus с базой процессора Intel Core Duo T2000. Мультимедийная интерактивная доска Screen-Media.

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 учебный 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.

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

1. Перечень компетенций и этапов их формирования.

Компетенции		
Индекс	Формулировка	Этап формирования
ПК-2	Способен выполнять формализацию данных и загрузку информации в АСУ, решать задачи диагностики нештатных ситуаций и отказов АСУТП, понимать структуру прикладных программных проектов на уровне АСУТП, выполнять разработку отдельных блоков прикладного программного обеспечения	промежуточный

1. 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)
ПК-2.3 Применение методов обеспечения информационной безопасности при анализе, изучении и разработке блоков прикладного программного обеспечения АСУТП	знать <ul style="list-style-type: none"> требования информационных систем, виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты, организационные, технические и программные методы и модели защиты (методы идентификации; методы и средства криптографии) 	Правильные ответы на вопросы №1-11, 29-39 к экзамену	Слабо ориентируется 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
	уметь <ul style="list-style-type: none"> применять методы защиты компьютерной информации в различных областях, в том числе АСУТП; проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе; выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; 	Правильные ответы на вопросы № 17-28, 35, 39-43 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
	владеть <ul style="list-style-type: none"> навыками работы с различными источниками информации, навыками эксплуатации информационных систем и сервисов; навыками работы с программно-инструментальными средствами 	Правильные ответы на вопросы № 12-16, 22-28,41-45 к экзамену	Слабо ориентируется в информационном массиве данных, не может выделить причинно-следственные связи и взаимозависимости Слабо ориентируется в теме, выполняет алгоритмы с ошибками	Ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости с небольшими ошибками. Выполняет алгоритмы с небольшими ошибками	Уверенно ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости Выполняет алгоритмы качественно и без ошибок

Шкала оценивания соответствует СТО СПбГТИ(ТУ): промежуточная аттестация проводится в форме зачета

3. Типовые контрольные вопросы для сдачи зачета

1. Понятие информационной безопасности и основные проблемы.
2. Информационная безопасность системы. Базовые понятия: угроза, уязвимость, атака. Виды угроз.
3. Характеристики информации. Задачи информационной безопасности.
4. Способы обеспечения защиты: законодательные, административные, технические. Основные механизмы и службы защиты.
5. Теоретические основы информационной безопасности. Криптографические методы закрытия информации. Кодирование и шифрование.
6. Криптография. Основные понятия. Правило Кирхгофа. Классификация методов шифрования.
7. Криптография: симметричные и асимметричные алгоритмы. Принцип действия, пример.
8. Гаммирование. Общее понятие и применение.
9. 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. PGP. Принцип функционирования. Свойства ключа.
14. Хэш-функции. Определение, свойства, применение.
15. Электронная подпись. Понятие, структура построения, использование.
16. Проверка целостности данных. Методы и функции.
17. Политика безопасности. Определение. Функции, виды, базовые представления.
18. Мандатная модель Белла-Ла Падулы. Достоинства и недостатки.
19. Дискреционная модель Харрисона-Руззо-Ульмана. Достоинства и недостатки.
20. Ролевая политика безопасности. Формальное представление. Достоинства и недостатки. Виды.
21. Стандарты безопасности. Основные цели и функции. Пользователи.
22. Реестр и его использование для обеспечения безопасности программного продукта.
23. Безопасность БД. Методы и средства.
24. Безопасность ПО. Методы и средства.
25. Идентификация и аутентификация. Биометрическая защита.
26. Структура системы защиты от несанкционированного доступа.
27. Статические и динамические характеристики среды.
28. Безопасность АСУ ТП. Особенности
29. Законодательство РФ в области защиты информации. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
30. Стратегия национальной безопасности.

31. Государственная тайна. Законодательство. Базовый список сведений. Режим, особенности, ответственность за нарушения.
32. Коммерческая тайна. ФЗ № 98 «О коммерческой тайне». Конфиденциальный документооборот.
33. Коммерческая тайна. Режим, особенности, ответственности за нарушение режима КТ.
34. Персональные данные. Основные понятия, категорирование. Обработка персональных данных

35. Аудит ИБ на предприятии. Цели и задачи
36. Информация и ее свойство: качество, адекватность, достоверность и избыточность.
37. Информация по категории доступа и порядок ее предоставления
38. Владелец информации: понятие, права, обязанности.
39. Интеллектуальная собственность. Понятие, охраняемые результаты, авторское и патентное право.
40. Ноу-хау. Особенности правовой охраны.
41. Исключительное и неисключительное право на объекты интеллектуальной деятельности. Основы договорных взаимоотношений.
42. Лицензионный договор. Понятие, виды, основные разделы. Сублицензия
43. Служебное произведение. Права и обязанности сторон.
44. Маркетинговые исследования. Суть, цели и задачи. Алгоритм
45. Патентные исследования. Суть, цели и задачи. Алгоритм

Вопросы для оценки сформированности элементов компетенции:

ПК-2.3 1-26

К зачету допускаются студенты, выполнившие все формы текущего контроля. При сдаче зачета, 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) 016-2014. КС УКВД. Порядок проведения зачетов и экзаменов.