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
22 апреля 2022 г.

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки
15.03.04 Автоматизация технологических процессов и производств

Направленность программы бакалавриата
Автоматизация технологических процессов и производств

Квалификация
Бакалавр

Форма обучения
заочная

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

Санкт-Петербург
2022

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 «15» апреля 2022 года №6

Заведующий кафедрой Т.Б. Чистякова

Одобрено учебно-методической комиссией факультета информационных технологий и управления
протокол от «20» апреля 2022 года №8

Председатель В.В. Куркина

СОГЛАСОВАНО

Руководитель направления подготовки		О.А. Ремизова
Директор библиотеки		Т.Н. Старостенко
Начальник методического отдела учебно-методического управления		М.З. Труханович
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)
ПК-2 Способен осуществлять настройку и внедрение программного обеспечения автоматизированных систем, организовывать работу информационных баз данных, анализировать данные о функционировании АСУП с целью обоснования требований к содержанию и построению технической и организационно- распорядительной документации на всех этапах ее жизненного цикла.	ПК-2.1 Применение методов обеспечения информационной безопасности при анализе, изучении и разработке блоков прикладного программного обеспечения АСУТП	**знать** • 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) **уметь** • 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; **владеть** навыками работы с различными источниками информации**,** навыками эксплуатации информационных систем и сервисов; навыками работы с программно- инструментальными средствами

2. Место дисциплины в структуре образовательной программы

ДисциплинаБ1.В.01«Информационная безопасность» принадлежит к части, формируемой участниками образовательных отношений. Дисциплина базируется на знаниях, полученных студентами в курсах «Информатика», «Основы права». Дисциплина изучается на 2-ом курсе в 3-м и 4ом семестрах.

3. Объем дисциплины

Вид учебной работы	Всего, ак. ч	В том числе	
	заочная форма	3семестр	4 семестр
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	3/108	36	72
Контактная работа с преподавателем:	**12**		
занятия лекционного типа	4	4	
занятия семинарского типа, в т.ч.	-		
семинары, практические занятия (в том числе практическая подготовка)	8		8
лабораторные работы (в том числе практическая подготовка)	-		
курсовое проектирование (КР или КП)	-		
КСР	2		2
другие виды контактной работы (контроль)	-		
Самостоятельная работа	**92**	**32**	**60**
Форма текущего контроля (Кр, реферат, РГР, эссе)	**4**		**4**
Форма промежуточной аттестации (КР, КП ,зачет, экзамен)	зачет		Зачет, 2 кр

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, академ. часы		Самостоятельная работа, акад. часы	Формируемые компетенции . индикаторы
			Семинары и/или практические	Лаборат. работы		
1	Защита информации.	0,3	1		5	ПК-2.1
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	0,2			6	
3	Идентификация и аутентификация.	0,2	1		8	
4	Основы криптографии.	1	2		15	
5	Политика безопасности.	0,5	0,5		8	
6	Стандарты безопасности.	0,5	0,5		8	
7	Информация ограниченного доступа. Конфиденциальное делопроизводство	0,3	2		5	
8	Вопросы организации информационной безопасности на предприятии. Безопасность АСУ ТП.	1	1		5	
	Итого	4	8		60	

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.	0,3	Лекция-визуализация (ЛВ)
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	0,2	ЛВ
3	Идентификация и аутентификация. Основные понятия и концепции. Биометрия.	0,2	ЛВ
4	Основы криптографии. Основные понятия и определения. Криптографические алгоритмы. Контроль целостности информации. Функции хеширования. Электронная подпись.	1	ЛВ
5	Формальные модели безопасности. Политика безопасности. Основные модели и критерии защи-	0,5	ЛВ
6	Стандарты безопасности. Роль и задачи стандартов. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	0,5	ЛВ
7	Информация ограниченного доступа. Конфиденциальное делопроизводство	0,3	ЛВ
8	Организация информационной безопасности на предприятии. Правовые, организационные и технические мероприятия. Документальное обеспечение. Безопасность АСУ ТП.	1	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	Изучение законодательной базы в области защиты информации и информационных технологий	1	КтСм
3	ПО «Daily». Биометрическая идентификации и элементы криптоанализа	1	КтСм
4-6	PGP. Криптографическое закрытие информации. Ассиметричные алгоритмы. Электронная подпись. Контроль целостности и авторства сообщений.	2	КтСм
4,5,8	«Itkey». Изучения средств защиты программных продуктов	4	КтСм

4.3.2. Лабораторные занятия

Не предусмотрены.

4.4.Самостоятельная работа обучающихся

№ Раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
1	Основы информационной безопасности. Основные понятия защиты информации. ФЗ № 149. Безопасность функционирования информационных систем. Свойства защищенных систем	5	Устный опрос
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	6	Устный опрос
3	Идентификация и аутентификация. Управление доступом. Механизмы подтверждения подлинности пользователя. Парольная идентификация. Программно – аппаратные средства. Биометрия.	8	Устный опрос
4	Основы криптографии. Классификация систем шифрования. Симметричное, ассиметричное шифрование. Алгоритмы. Требования к криптосистемам. ГОСТ 28147-89. Алгоритмы контроля целостности. Функции хеширования, свойства, применение. Электронная подпись. Законодательство РФ. Функции, алгоритмы, применение. Инфраструктура открытых ключей. Удостоверяющий центр.	11	Устный опрос, (тест КР2)
5	Политики безопасности. Базовые структуры и функции. Мандатная, дискреционная и ролевая политики. Принципы	8	Устный опрос

№ Раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
	построения, достоинства и недостатки.		
6	Стандарты безопасности.	8	Устный опрос,
7	Методы защиты программ от внешних воздействий. Средства обнаружения и защиты программ от разрушающих программных воздействий Защита от копирования, контроль целостности, резервирование.	5	Отчеты по работам
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.	5	Устный опрос
1-8	Реферат по индивидуальному заданию	4	КР1 Реферат-доклад -презентация
	Итого	60	

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.

4.4.1 Темы контрольных работ

Задание по дисциплине включает две контрольные работы

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 и в виде мультимедийной презентации (в электронном и бумажном варианте).

2. Тестовое задание

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

1. Аналитическое исследование Методы 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 и 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. Обеспечение целостности информации
9. Обеспечение безопасности сети организации
10. Безопасность промышленных сетей
11. Системы оценки рисков

2. Тестовое задания Криптография

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

14) 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

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

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: 20.03.2022). – 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: 20.03.2022). – 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: 20.03.2022). — 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 «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 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 управленияСПбГТИ(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 IntelCore 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.Персональныекомпьютерыобъединены 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.Персональныекомпьютерыобъединены в корпоративную вычислительную сеть кафедры и имеют выход в сеть «Интернет».
Лекционная аудитория	56 посадочных мест. Учебная мебель. 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 28.08.2015г.

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**
ПК-2	Способен осуществлять настройку и внедрение программного обеспечения автоматизированных систем, организовывать работу информационных баз данных, анализировать данные о функционировании АСУП с целью обоснования требований к содержанию и построению технической и организационно- распорядительной документации на всех этапах ее жизненного цикла.	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-2.1Применение методов обеспечения информационной безопасности при анализе, изучении и разработке блоков прикладного программного обеспечения АСУТП	Называет требования информационных систем, виды угроз ИС и методы обеспечения информационной безопасности. Описывает 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	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.
	Применяет методы защиты компьютерной информации в различных областях, в том числе АСУТП. Проводит обследования, выявляет информационные потребности пользователей, формирует требования к информационной системе. Выявляет и оценивает угрозы информационной безопасности, обосновывает организационно-технические мероприятия по защите информации в ИС.	Правильные ответы на вопросы № 17-28, 35, 39-43	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.
	Применяет навыки работы с различными источниками информации**.** Использует навыки эксплуатации информационных систем и сервисов. Демонстрирует навыки работы с программно- инструментальными средствами.	Правильные ответы на вопросы № 12-16, 22-28,41-45	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 алгоритмыкачественно 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**: у**гроза, 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 Кирхгоффа. 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. Особеннности
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. Обладатель 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.

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) 016-2015. КС УКВД. Порядок проведения зачетов и экзаменов.