

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Пекаревский Борис Владимирович
Должность: Проректор по учебной и методической работе
Дата подписания: 10.11.2023 17:44:10
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
ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки

18.05.01 Химическая технология энергонасыщенных материалов и изделий

Квалификация
Специалист

Форма обучения
Очная

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

Санкт-Петербург
2021

ЛИСТ СОГЛАСОВАНИЯ

Должность разработчика	Подпись	Ученое звание, инициалы, фамилия
доцент		Г.В. Кузнецова

Рабочая программа дисциплины «Защита информации» 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 18.05.01 «Химическая технология энергонасыщенных материалов и из- делий»		Т.В. Украинцева
Директор библиотеки		Т.Н. Старостенко
Начальник методического отдела учебно-методического управления		Т.И. Богданова
Начальник учебно-методического управления		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
4.3.1 Семинары, практические занятия.....	8
4.3.2 Лабораторные занятия	8
4.4 Самостоятельная работа обучающихся	9
5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	10
6 Фонд оценочных средств для проведения промежуточной аттестации	10
7 Перечень учебных изданий, необходимых для освоения дисциплины	10
а) печатные издания	10
б) электронные учебные издания	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
10.1 Информационные технологии	12
10.2 Программное обеспечение	13
10.3 Базы данных и информационные справочные системы.....	13
11 Материально-техническое обеспечение освоения дисциплины в ходе реализации образовательной программы.....	13
12 Особенности освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья.....	13
Приложения: 1 Фонд оценочных средств для проведения промежуточной аттестации	
2 Форма титульного листа для оформления отчетов о практических работах	

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

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения (дескрипторы)
<p>ОПК-3 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.</p>	<p>ОПК-3.6 Обработка и хранение информации в профессиональной деятельности с помощью баз данных и компьютерных сетевых технологий, с соблюдением информационной безопасности.</p>	<p>Знать</p> <ul style="list-style-type: none"> - основы законодательства РФ в области защиты информации; правовые аспекты регулирования отношений в информационной сфере, основные задачи национальной безопасности РФ (ЗН-1); - виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты; основные статьи Закона о государственной тайне, уголовный кодекс при правонарушениях в области информационной безопасности (ЗН-2); - требования информационных систем и методы обеспечения информационной безопасности, в том числе, правила поведения на режимных объектах, обязанности при работе с секретными документами (ЗН-3); - способы и виды организационных и технических мероприятий по защите информации (ЗН-4); <p>уметь</p> <ul style="list-style-type: none"> - ориентироваться в источниках информации, работать с Интернет – ресурсами, правовыми базами; анализировать профессиональную информацию, работать с источниками информации, содержащими сведения о гостайне (У-1); - применять методы защиты информации в различных областях; обосновывать организационно-технические мероприятия по защите информации в ИС; соблюдать требования режимных объектов (У-2); <p>владеть</p> <ul style="list-style-type: none"> - навыками работы с различными источниками информации; сведениями об организации и проведении процесса защиты информации (Н-1).

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» (Б1.О.29) относится к Блоку 1 «Дисциплины (модули)» обязательной части образовательной программы специалитета и изучается на 5 курсе в 10 семестре. В методическом плане дисциплина опирается на элементы компетенций, сформированные при изучении дисциплин «Основы права», «Психология и социальные коммуникации», «Основы научных исследований», «Общая химическая технология».

Полученные в процессе изучения дисциплины знания, умения и навыки могут быть использованы при выполнении выпускной квалификационной работы и в дальнейшей работе.

3. Объем дисциплины

Вид учебной работы	Всего, ЗЕ/акад. часов
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	3/108
Контактная работа с преподавателем:	72
занятия лекционного типа	36
занятия семинарского типа, в т.ч.	36
семинары, практические занятия	36
лабораторные работы	-
курсовое проектирование (КР или КП)	-
КСР	-
другие виды контактной работы	-
Самостоятельная работа	36
Форма текущего контроля (Кр, реферат, РГР, эссе)	-
Форма промежуточной аттестации (КР, КП, зачет, экзамен)	Зачет

4. Содержание дисциплины

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 занятия	Лабораторные работы			
1.	Информационная безопасности (ИБ) и защита информации. Основные понятия. Терминология. Стратегия национальной безопасности. Политика информационной безопасности РФ.	4	4	–	4	ОПК-3	ОПК-3.6
2.	Информация ограниченного доступа. Законодательство РФ. Государственная тайна. Коммерческая тайна. Конфиденциальное делопроизводство.	4	6	–	6	ОПК-3	ОПК-3.6
3.	Электронный документооборот. Электронная подпись.	2	4	-		ОПК-3	ОПК-3.6
4.	Вопросы организации информационной безопасности на предприятии. Концептуальная модель оценки рисков. Безопасность АСУ.	6	6	-	8	ОПК-3	ОПК-3.6
5.	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	2	–	-	4	ОПК-3	ОПК-3.6
6.	Идентификация и аутентификация.	2	4	-	2	ОПК-3	ОПК-3.6
7.	Основы криптографии.	4	6	-	4	ОПК-3	ОПК-3.6
8.	Политика безопасности.	2		-		ОПК-3	ОПК-3.6
9.	Стандарты безопасности.	2		-	2	ОПК-3	ОПК-3.6
10	Защита результатов интеллектуальной деятельности (РИД). Ноу-хау. Патентное и авторское право.	6	6	-	4	ОПК-3	ОПК-3.6
11	Правовое регулирование отношений, связанных с использованием информационных ресурсов. Основы договорных отношений. Договор о конфиденциальности. Лицензионный договор.	2		-	2	ОПК-3	ОПК-3.6
	итого	36	36		36		

4.2. Занятия лекционного типа

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1.	Информационная безопасности (ИБ) и защита информации. Основные понятия. Терминология. Информационные ресурсы и их свойства. Стратегия национальной безопасности. Политика информационной безопасности РФ.	4	Лекция-визуализация (ЛВ)
2.	Информация ограниченного доступа. Законодательство РФ. Государственная тайна. Коммерческая тайна. Конфиденциальное делопроизводство. Ответственность за нарушения законодательства. Персональные данные.	4	ЛВ
3.	Электронный документооборот. Электронная подпись. Юридический аспект.	2	ЛВ
4.	Вопросы организации информационной безопасности на предприятии. Организационные и технические мероприятия. Концептуальная модель оценки рисков. Безопасность АСУ. Социальная инженерия.	6	ЛВ
5.	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	2	ЛВ
6.	Идентификация и аутентификация. Биометрия	2	ЛВ
7.	Основы криптографии. Шифрование. Симметричные и ассиметричные алгоритмы. Контроль целостности информации. Подтверждение авторства документа.	4	ЛВ
8.	Политика безопасности. Дискреционная, мандатная, ролевая политика.	2	ЛВ
9.	Стандарты безопасности.	2	ЛВ
10.	Защита результатов интеллектуальной деятельности (РИД). Гражданский кодекс, часть 4. Патентное и авторское право. Ноу-хау. Служебное произведение. Конкурентные исследования	6	ЛВ
11.	Правовое регулирование отношений, связанных с использованием информационных ресурсов. Основы договорных отношений. Договор о конфиденциальности. Лицензионный договор.	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
1-4	Изучение законодательной базы РФ в области защиты информации и информационных технологий Работа со справочными правовыми системами "Консультант Плюс", "Гарант". Семинар-дискуссия по актуальным проблемам. Учебное исследование на основе законодательной базы и общедоступных источников и дискуссия по проблеме. Анализ конкретных ситуаций	18	КтСм
4	Анализ угроз информационной системы. Формирование комплекса требований к системе защиты. Система оценки рисков, дерево событий. Учебное исследование	4	КтСм
6	Биометрическая идентификации	2	КтСм
7	Криптографическое закрытие информации. Ассиметричные алгоритмы. Контроль подлинности, целостности и авторства сообщений (PGP, Merlin)	6	КтСм
10	Защита результатов интеллектуальной деятельности. Учебное исследование (поиск и анализ информации – конкурентные исследования)	6	КтСм

4.3.2. Лабораторные занятия

Учебным планом не предусмотрены.

4.4. Самостоятельная работа обучающихся

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
1-11	Изучение законодательной базы РФ в области защиты информации и информационных технологий. Работа со справочными правовыми системами "Консультант Плюс", "Гарант".	2	Устный опрос, отчеты к практическим работам
2-3	Правовые основы работы с информацией ограниченного доступа. Содержание стратегии национальной безопасности РФ	2	Устный опрос
2	Информационные ресурсы. Основные свойства информации. Виды информации в правовой системе	2	Устный опрос
3	Информация ограниченного доступа. Правила поведения на режимном объекте.	2	Устный опрос
3	Электронный документооборот. Электронная подпись. Федеральный закон «Об электронной подписи» (ФЗ № 63)	2	Устный опрос
4	Безопасность функционирования информационных систем. Системы оценки рисков	2	Устный опрос,
4	Системы оценки рисков. Дерево событий	4	Отчеты по работам
4	Основы информационной безопасности на предприятии. Конфиденциальность. Коммерческая тайна. Источники несанкционированного доступа к информации на предприятии.	2	Устный опрос
4,5	Безопасность АСУ ТП. Структура, особенности	2	Устный опрос
4	Подготовка кадров. Социальная инженерия	4	Устный опрос
6	Механизмы подтверждения подлинности пользователя. Биометрия.	2	Устный опрос
8	Системы контроля доступа	2	Устный опрос
8	Программно-аппаратные средства защиты ЭВМ и сетей, ограничения доступа к компонентам сетей предприятий.	2	Устный опрос
9	Единые критерии безопасности информационных технологий	2	
10,11	Конкурентные исследования	4	Устный опрос, подготовка к практической работе

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

- работу с источниками информации и чтение рекомендованной литературы,
- усвоение теоретического материала дисциплины;
- подготовку к практическим занятиям;
- работу с Интернет-источниками;
- подготовку к сдаче зачета.

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 и требования к их выполнению размещены в электронной информационно-образовательной среде СПбГТИ(ТУ) на сайте: <https://media.technolog.edu.ru>.

6. Фонд оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Зачет предусматривает выборочную проверку освоения предусмотренных элементов компетенций и комплектуется тремя теоретическими вопросами из разных разделов дисциплины (приложение 1), время подготовки студента к устному ответу – до 40 мин.

Пример варианта вопросов на зачете:

Вариант № 1

1. Государственная тайна. Законодательство. Базовый список сведений. Режим, особенности, ответственность за нарушения.
2. Лицензионный договор. Понятие, виды, особенности.
3. Социальная инженерия. Понятие, особенности использования.

Результаты освоения дисциплины считаются достигнутыми, если для всех элементов компетенций достигнут пороговый уровень освоения компетенции на данном этапе – «зачет».

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 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.

7. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. – 3-е изд., стер. – Санкт-Петербург : Лань, 2021. – 124 с. – ISBN 978-5-8114-7970-2. – 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 «Защита информации» проводятся в соответствии с требованиями следующих СТП (СТО):

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

2 СТП СПбГТИ 020-2011. КС УКДВ. Виды учебных занятий. Практические занятия. Общие требования к организации и проведению.

3 СТО СПбГТИ(ТУ) 016-2015. КС УКДВ. Порядок организации и проведения зачётов и экзаменов.

4 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;
- готовность технических и программных средств ЭВМ;
- серьезное отношение к изучению материала;
- постоянный самоконтроль.

На занятия студент должен приходить, имея знания 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;
- использование технических и программных средств для выполнения практической части дисциплины;

- взаимодействие с обучающимися посредством электронной информационно-образовательной среды.

10.2. Программное обеспечение

- 1 Операционная система MicrosoftWindows.
- 2 Многоцелевой универсальный редактор векторной графики MicrosoftVisio.
- 3 Система управления базами данных Microsoft Access.
- 4 Пакет офисных программ LibreOffice или ApacheOpenOffice.

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-техническое обеспечение освоения дисциплины в ходе реализации образовательной программы

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 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 NVIDIA GeForceGT 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 NECNP41. Ноутбук Asus абj на базе процессора IntelCoreDuo T2000. Мультимедийная интерактивная доска ScreenMedia.

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 28.08.2014.

**Фонд оценочных средств
для проведения промежуточной аттестации по
дисциплине «Защита информации»**

1. Перечень компетенций и этапов их формирования.

Индекс компетенции	Содержание	Этап формирования
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	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-3.6 Обработка и хранение информации в профессиональной деятельности с помощью баз данных и компьютерных сетевых технологий, с соблюдением информационной безопасности	знает основы законодательства РФ в области защиты информации; правовые аспекты регулирования отношений в информационной сфере, основные задачи национальной безопасности РФ (ЗН-1);	Правильные ответы на вопросы № 9-20 к зачету	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
	знает виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты; основные статьи Закона о государственной тайне, уголовный кодекс при правонарушениях в области информационной безопасности (ЗН-2);	Правильные ответы на вопросы №1-5, 18-24 к зачету	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
	Знает требования информационных систем и методы обеспечения информационной безопасности, в том числе, правила поведения на режимных объектах, обязанности при работе с секретными документами (ЗН-3);	Правильные ответы на вопросы №1-5, 32-35 к зачету	Слабо ориентируется в законодательной базе РФ в информационной сфере. Допускает в ответе серьезные ошибки	Хорошо ориентируется в законодательной базе РФ в информационной сфере, немного путается в терминах	Хорошо ориентируется в вопросе. Может применить эти знания для решения текущих задач и приводит примеры

	знает способы и виды организационных и технических мероприятий по защите информации (ЗН-4);	Правильные ответы на вопросы № 10,11 к зачету	Путается в перечислении средств и способов	Перечисляет средства и способы защиты с небольшими ошибками	Уверенно и без ошибок перечисляет средства и способы защиты, принципы и особенности ведения работ
	умеет ориентироваться в источниках информации, работать с Интернет – ресурсами, правовыми базами; анализировать профессиональную информацию, работать с источниками информации, содержащими сведения о гостайне (У-1);	Правильные ответы на вопросы № 1-15 к зачету	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
	умеет применять методы защиты информации в различных областях; обосновывать организационно-технические мероприятия по защите информации в ИС; соблюдать требования режимных объектов (У-2);	Правильные ответы на вопросы № 8-22,28-33 № 1-9, 14-24 к зачету	Имеет слабое представление о методах защиты Перечисляет основные этапы, способы и термины с ошибками	Может оценить риски и предложить методы защиты с помощью наводящих вопросов	Способен самостоятельно оценить риски, легко ориентируется в терминах.
	владеет навыками работы с различными источниками информации; сведениями об организации и проведении процесса защиты информации (Н-1).	Правильные ответы на вопросы № 2-4,11-12,23-24 к зачету	Слабо ориентируется в информационном массиве данных, не может выделить причинно-следственные связи и взаимозависимости	Ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости с небольшими ошибками	Уверенно ориентируется в информационном массиве данных, отслеживает причинно-следственные связи и взаимозависимости

3. Типовые контрольные задания для проведения промежуточной аттестации

1. Понятие информационной безопасности и основные проблемы. Основные задачи в области обеспечения защиты информации
2. Законодательство РФ в области защиты информации. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Стратегия национальной безопасности.
4. Государственная тайна. Законодательство. Базовый список сведений. Режим, особенности, ответственность за нарушения.
5. Информационная безопасность системы. Базовые понятия: угроза, уязвимость, атака. Виды угроз. Классификация угроз
6. Характеристики информации. Задачи информационной безопасности.
7. Способы обеспечения защиты: законодательные, административные, технические. Основные механизмы и службы защиты.
8. Криптографические методы закрытия информации.
9. Криптография. Основные понятия. Правило Кирхгоффа. Классификация методов шифрования.
10. Криптография: симметричные и асимметричные алгоритмы. Принцип действия
11. Гаммирование. Общее понятие и применение.
12. Электронная подпись. Понятие, алгоритм построения, использование.
13. Проверка целостности данных. Методы и функции.
14. Политики безопасности. Определение. Функции, виды, базовые представления.
15. Принципы организации доступа к информации.
16. Стандарты безопасности. Основные цели и функции. Пользователи.
17. Единые критерии безопасности информационных технологий. Основные понятия и положения. Профиль и проект защиты.
18. Идентификация и аутентификация. Биометрическая защита.
19. Социальная инженерия. Понятие, использование.
20. Коммерческая тайна. ФЗ № 98 «О коммерческой тайне». Конфиденциальный документооборот.
21. Аудит ИБ на предприятии. Цели и задачи
22. Информация и ее свойство: качество, адекватность, достоверность и избыточность.
23. Информация по категории доступа и порядок ее предоставления
24. Владелец информации: понятие, права, обязанности.
25. Интеллектуальная собственность. Понятие, охраняемые результаты, авторское и патентное право.
26. Ноу-хау. Особенности правовой охраны.
27. Исключительное и неисключительное право на объекты интеллектуальной деятельности. Основы договорных взаимоотношений.
28. Лицензионный договор. Понятие, виды, основные разделы. Сублицензия
29. Служебное произведение. Права и обязанности сторон.
30. Коммерческая тайна. Режим, особенности, ответственности за нарушение режима КТ.
31. Персональные данные. Основные понятия, категорирование. Обработка персональных данных

При сдаче зачета студент получает три вопроса из перечня, приведенного выше
Время подготовки студента к устному ответу на вопросы – до 40 мин.

5. Методические материалы для определения процедур оценивания знаний, умений и навыков, характеризующих этапы формирования компетенций.

Промежуточная аттестация по дисциплине проводится в соответствии с требованиями СТО СПбГТИ(ТУ) 016-2015. КС УКДВ. Порядок организации и проведения зачетов и экзаменов.

По дисциплине промежуточная аттестация проводится в форме зачета.

Шкала оценивания на зачете – «зачет», «незачет». При этом «зачет» соотносится с пороговым уровнем сформированности компетенции.

**Форма титульного листа для оформления
практических работ**

Минобрнауки России
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный технологический институт
(технический университет)»

Факультет: Информационных технологий и управления

Кафедра: Систем автоматизированного проектирования и управления

Направление подготовки: 18.05.01 Химическая технология энергонасыщенных материалов
и изделий

Уровень подготовки: Специалист

Учебная дисциплина: Защита информации

Группа: _____

О Т Ч Е Т О Р А Б О Т Е № _

ТЕМА:

Преподаватель

Кузнецова Г.В.

Исполнители

Отметка о зачете _____

Санкт-Петербург

2021