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

«__» _____ 2017г.

Рабочая программа дисциплины

ЗАЩИТА ИНФОРМАЦИИ

(год начала подготовки – 2013)

Специальность
18.05.01 – Химическая технология энергонасыщенных материалов и изделий

Специализации
Все специализации

Квалификация (степень) выпускника

Инженер

Форма обучения

Очная

Факультет **инженерно-технологический**

Кафедра **химической энергетики**

Санкт-Петербург

2017 Б1.В.05

ЛИСТ СОГЛАСОВАНИЯ

Должность	Подпись	Ученое звание, фамилия, инициалы
профессор		Улыбин В.Б.

Рабочая программа дисциплины «Защита информации» обсуждена на заседании кафедры химической энергетики
протокол от «___» _____2017 № __
Заведующий кафедрой А.С. Мазур

Одобрено учебно-методической комиссией инженерно-технологического факультета
протокол от «___» _____2017 № __
Председатель В.В.Прояев

СОГЛАСОВАНО

Руководитель направления подготовки «Химическая технология энергонасыщенных материалов и изделий»		профессор, д.т.н. В.В. Самонин
Начальник методического отдела учебно-методического управления		Т.И.Богданова
Начальник УМУ		С.Н.Денисенко
Директор библиотеки		Т.Н. Старостенко

СОДЕРЖАНИЕ

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: ОК – 5, ОПК – 3, ПК – 10.

Коды компетенции	Результаты освоения ООП *(содержание компетенций)*	Перечень планируемых результатов обучения по дисциплине
ОК – 5	Способность использовать основы правовых знаний в различных сферах профессиональной деятельности	**Знать:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия. **Уметь:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия **Владеть:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами
ОПК – 3	Способность решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Уметь:** планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Владеть:** организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.

Коды компетенции	Результаты освоения ООП *(содержание компетенций)*	Перечень планируемых результатов обучения по дисциплине
ПК – 10	Способность изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследований	**Уметь:** Искать и получать сведения из источников инфорации различного рода

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к дисциплинам по выбору вариативной части (Б1.В.05) и изучается на 4 курсе в 7 семестре.

В методическом плане дисциплина опирается на элементы компетенций, сформированные при изучении дисциплин «Информатика» и «Основы права», «Основы экологии», «Введение в специальность», «Основы научных исследований».

Данная дисциплина заканчивает формирование компетенций ОК – 5 и ОПК – 3.

Компетенция ПК-10, освоенная при изучении данной дисциплины, будет развиваться далее в дисциплине «Метрология, стандартизация и сертификация»

Все знания, умения, навыки, полученные при изучении этой дисциплины, будут использованы при выполнении ВКР и дальнейшей трудовой деятельности.

3 Объем дисциплины

Вид учебной работы	Всего, академических часов
	Очная форма обучения
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	3/108
Контактная работа с преподавателем:	54
занятия лекционного типа	18
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	54
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
			Семинары и/или практические занятия	Лабораторные работы		
1.	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Правовое обеспечение информационной безопасно	2	4	-	6	ОК – 5, ОПК – 3
2.	Источники и каналы утечки информации. Средства и методы физической защиты.	2	4	-	6	ОК – 5, ОПК – 3
3	Обеспечение безопасности обработки и хранения информации в вычислительных системах.	2	4	-	6	ОК – 5, ПК – 10
4	Защита информации от несанкционированного доступа к информации. Криптографическое закрытие информации.	2	4	-	6	ОК – 5, ОПК – 3
5	Перечень сведений, составляющих государственную тайну. Формы допуска к государственной тайне	2	4	-	6	ОК – 5, ОПК – 3
6	Обеспечение безопасности обработки информации в распределенных вычислительных системах. Средства защиты информации в сетях передачи данных.	2	4	-	6	ОК – 5, ПК – 10
7	Методологические и технологические основы комплексного обеспечения информационной безопасности. Построение систем охраны и защиты информации.	2	4	-	6	ОК – 5, ОПК – 3
8	Разработка и реализация политики безопасности организации Технология оценки и управления рисками информационной безопасности.	2	4	-	6	ОК – 5, ПК – 10
9	Защита от компьютерных вирусов.	2	4	-	6	ОК – 5, ОПК – 3
	Итого	18	36	-	54	

4.2 Занятия лекционного типа

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1	**Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Правовое обеспечение информационной безопасно.** Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, концепция ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, проблемы информационной войны; правовые и нормативные акты в области ИБ.	2	-
2	**Источники и каналы утечки информации. Средства и методы физической защиты.** Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Общие вопросы организации противодействия технической разведке; основные органи-зационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации: электромагнитные, электрические (проводные), виброа-кустические; защита технических средств от утечки ин-формации по этим каналам; роль и место технической за-щиты информации.	2	-
3	**Обеспечение безопасности обработки и хранения информации в вычислительных системах.** Проблемы обеспечения безопасности обработки	2	-

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
	и хранения информации в вычислительных системах. Основные положения теории информационной безопасности информационных систем. Три вида возможных нарушений информационной системы. Понятие угрозы информации в компьютерной системе. Уязвимые места вычислительных систем. Угрозы безопасности информации; ценность		
4	**Защита информации от несанкционированного доступа к информации. Криптографическое закрытие информации.** Способы преодоления компьютерных систем защиты информации. Задачи защиты от несанкционированного доступа к информации. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Взаимная проверка подлинности и другие случаи опознания. Допуск к ресурсам вычислительной системы. Способы разграничения доступа к компьютерным ресурсам. Использование матрицы установления полномочий. Разграничение доступа по уровням секретности и категориям. Управление доступом.	2	-
5	**Перечень сведений, составляющих государственную тайну. Формы допуска к государственной тайне.** Перечень сведений, составляющих государственную тайну. Этапы и критерии оформления форм допуска к документам, содержащим государственную тайну	2	-
6	**Обеспечение безопасности обработки информации в распределенных вычислительных системах. Средства защиты информации в сетях передачи данных.** Информационная безопасность в условиях функционирования в России глобальных сетей. Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные	2	-

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
	только для распределенной вычислительной среды. Задачи защиты информации в сетях передачи данных. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети.		
7	**Методологические и технологические основы комплексного обеспечения информационной безопасности. Построение систем охраны и защиты информации.** Основные технологии построения защищенных ЭИС.; Базовые этапы построения системы комплексной защиты вычислительных систем. Классификация способов и средств комплексной защиты информации. Организационная структура системы комплексной защиты информационно-программного обеспечения. Управление системой защиты.	2	-
8	**Разработка и реализация политики безопасности организации Технология оценки и управления рисками информационной безопасности.** Использование защищенных компьютерных систем. Модели безопасности и их применение. Обеспечение ИБ в нормальных и чрезвычайных ситуациях Содержание политики безопасности. Обеспечение безопасности компьютерной информации. Аудит безопасности. Концепция политики безопасности. Тестирование процедур и механизмов безопасности. Аварийный план. Реагирование на нарушение информационной безопасности. Проведение расследования. Адекватность механизмов защиты реальным угрозам	2	-
9	**Защита от компьютерных вирусов.** Понятия о видах вирусов. Понятие компьютерного вируса. История появления компьютерных вирусов и факторы, влияющие на их распространение. Основные этапы жизненного цикла вирусов. Схемы заражения. Способы маскировки, используемые вирусами. Общая организация защиты от компьютерных вирусов. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов.	2	-

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
	Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Использование средств аппаратного и программного контроля.		

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	**Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Правовое обеспечение информационной безопасно.** Изучение нормативно-правовых актов регулирующих деятельность в сфере информационной безопасности, руководящих документов по защите информации от несанкционированного доступа ФСТЭК России.	4	Дискуссия
2	**Источники и каналы утечки информации. Средства и методы физической защиты.** Контроль физического доступа в помещения. Технические средства защиты телекоммуникационных систем от побочных электромагнитных излучений	4	
3	**Обеспечение безопасности обработки и хранения информации в вычислительных системах.** Физическая безопасность информационных ресурсов. Управление правами пользователей по доступу к информационным ресурсам. Безопасное масштабирование компьютерных сетей	4	
4	**Защита информации от несанкционированного доступа к информации. Криптографическое закрытие информации.** Технические средства противодействия промышленному шпионажу. Основные положения криптографии. Характеристики криптоалгоритмов.	4	Дискуссия
5	**Перечень сведений, составляющих государственную тайну. Формы допуска к государственной тайне.** Изучение нормативных документов	4	
6	**Обеспечение безопасности обработки информации в распределенных**	4	

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
	вычислительных системах. Средства защиты информации в сетях передачи данных. Программно-аппаратное средство защиты от несанкционированного доступа к информации Secret Net. Конфигурирование основных функций системы защиты информации Secret Net 5.		
7	**Методологические и технологические основы комплексного обеспечения информационной безопасности. Построение систем охраны и защиты информации.** Установка полномочий работы с конфиденциальными документами различной важности. Назначение прав доступа	4	Дискуссия
8	**Разработка и реализация политики безопасности организации Технология оценки и управления рисками информационной безопасности.** Разработка рекомендаций работы с персоналом предприятия по обеспечению информационной безопасности	4	
9	**Защита от компьютерных вирусов.** Определение компьютерного вируса. Основные признаки вирусного поражения. Понятия о видах вирусов, классификация.. Обзор антивирусных программ.	4	

4.4 Самостоятельная работа обучающихся

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
1	**Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Правовое обеспечение информационной безопасности** Изучение нормативных документов по теме	2	-
2	**Источники и каналы утечки информации. Средства и методы физической защиты** Эволюция понятий «государственная тайна» и «военная тайна» в России	2	-
3	**Обеспечение безопасности обработки и хранения информации в вычислительных системах**	2	-
4	**Защита информации от несанкционированного доступа к информации. Криптографическое закрытие информации** Принципы работы и виды специальных технических средств защиты от утечки информации по техническим каналам. Изучение и работа со средствами защиты информации.	2	-
5	**Перечень сведений, составляющих государственную тайну. Формы допуска к государственной тайне** Изучение нормативных документов по теме.	2	-
6	**Обеспечение безопасности обработки информации в распределенных вычислительных системах. Средства защиты информации в сетях передачи данных.** Восстановление работоспособности компьютерной системы с помощью: использования безопасного режима; использования консоли восстановления; использования утилиты восстановления. Дублирование информации методом создания резервных копий.	2	-
7	**Методологические и технологические основы комплексного обеспечения информационной**	2	-

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
	безопасности. Построение систем охраны и защиты информации Модели безопасности и их применение. Модель матрицы доступа: добровольное и принудительное управление доступом. Модель распространения прав доступа. Модель многоуровневой защиты данных. Модель безопасности информационных потоков.		
8	**Разработка и реализация политики безопасности организации Технология оценки и управления рисками информационной безопасности** Управление рисками. Методики оценки рисков Системы управления политикой безопасности. Работа с персоналом и оборудованием. Автоматизированные системы как объекты защиты информации. Организация проектирования автоматизированных систем в защищенном исполнении. Условия и режимы эксплуатации автоматизированных систем.	2	-
9	**Защита от компьютерных вирусов.** Антивирусные средства. Стратегия борьбы с вирусами. Установка и администрирование антивирусных пакетов программ. Про-граммы Kaspersky AntiVirus и Dr. Web	2	-

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.

В процессе обучения студенты участвуют в дискуссиях. В конце семестра предусмотрен зачет.

Зачет предусматривают выборочную проверку освоения предусмотренных элементов компетенций и комплектуется теоретическими вопросами (для проверки знаний и умений).

Зачет проводится в соответствии с СТП СПб ГТИ 016-2015. КС УКДВ. Порядок проведения зачетов и экзаменов. Время подготовки к ответу – до 30 минут.

Фонд оценочных средств по дисциплине представлен в Приложении № 1

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

а) основная литература:

1 Аппаратные ключи eToken. Средство защиты eToken Network Logon : Практикум / И. В. Ананченко ; СПбГТИ(ТУ). Каф. систем. анализа. - СПб. : [б. и.], 2015. - 26 с.

2 Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для среднего профессионального образования по группе спец. "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : Форум ; М. : ИНФРА-М, 2013. - 415 с.

б) дополнительная литература:

1 Елович, И. В. Информатика: Учебник для вузов по техническим и естественнонаучным направлениям / И. В. Елович, И. В. Кулибаба; под ред. Г. Г. Раннева. - М. : Академия, 2011. - 394 с.

в). вспомогательная литература:

1 Секреты компьютерного шпионажа: Тактика и контрмеры: переводное издание / Дж. Макнамара; пер. с англ. А. В. Бутко, под ред. С. М. Молявко. - М.: БИНОМ. Лаборатория знаний, 2004. - 536 с.

2 Расторгуев, С.П. Основы информационной безопасности: учебное пособие для вузов по спец. "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем" и "Информационная безопасность телекоммуникационных систем" / С. П. Расторгуев. - М.: Academia, 2007. - 187 с.

3 Егоров, А.Ф. Управление безопасностью химических производств на основе новых информационных технологий: учебное пособие для вузов по направлению подготовки дипломированных специалистов 656500 "Безопасность жизнедеятельности" / А. Ф. Егоров, Т. В. Савицкая. - М. : Химия ; М. : КолосС, 2006. - 416 с.

4 Мельников, В.П. Информационная безопасность и защита информации: учебное пособие для вузов по спец. 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. - 2-е изд., стер. - М. : Academia, 2007. - 331 с. :

5 Барсуков, В. С. Безопасность: технологии, средства, услуги: справочное издание / В. С. Барсуков. - М.: КУДИЦ-ОБРАЗ, 2001. - 489 с.

6 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учебное пособие для вузов по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М.: ДМК-Пресс, 2008. - 542 с.

7 Романов, О.А. Организационное обеспечение информационной безопасности: учебник для вузов по спец. "Организация и технология защиты

информации" направления подготовки "Информационная безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М.: Академия, 2008. - 190 с.

8 Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебное пособие для вузов по спец. 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем" / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова и др. - М.: Горячая линия - Телеком, 2009. - 552 с.

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

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

ЭБС «Лань». Принадлежность-сторонняя. Адрес сайта – http://e.lanbook.com Наименование организации – ООО «Издательство «Лань». Договор № 04(40)12 от 29.10.2012г.

Справочно-поисковая система «Консультант-Плюс». Принадлежность – сторонняя. Контракт № 04(49)12 от 31.12.2012г. по оказанию информационных услуг с использованием экземпляров Специальных Выпусков Систем Консультант Плюс.

ЭБС «Научно-электронная библиотека eLibrary.ru». Принадлежность – сторонняя. Адрес сайта – http://elibrary.ru Наименование организации – ООО РУНЭБ. Договор № SU-18-02/2013-2 от 18.02.2013г. на оказание услуг по предоставлению доступа к изданиям в электронном виде.

9 Методические указания для обучающихся по освоению дисциплины

Все виды занятий по дисциплине «Защита информации» проводятся в соответствии с требованиями следующих СТП:

СТП СПб ГТИ 016-2015. КС УКДВ. Порядок проведения зачетов и экзаменов.

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;

видео и аудиоматериалы по курсу, представленные на сайт ehttp://media.technolog.edu.ru

взаимодействие с обучающимися через личный кабинет в единой информационной среде.

10.2 Программное обеспечение

ОС WINDOWS, OPEN OFFICE. Авторское программное обеспечение для расчета зон действия поражающих факторов, рисков, Matcad, ТОКСИ, FireCat , СОУТ, HZOB.

10.3 Информационные справочные системы

Справочно-поисковая система «Консультант-Плюс». Принадлежность – сторонняя. Контракт № 04(49)12 от 31.12.2012г. по оказанию информационных услуг с использованием экземпляров Специальных Выпусков Систем Консультант Плюс.

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

Лекционные кабинеты: 190013, г.Санкт-Петербург, Московский проспект, д. 24-26/49, лит.А №3 -52 м^2, 6 – 129 м^2, 14 – 61 м^2.

Оборудование лекционных аудиторий: Мультимедийная система, (проектор P1166-и 3 штуки), ноутбук aser aspire 9300- 3 штуки (программное обеспечение: ОС WINDOWS.,OPEN OFFICE) экран ScreenMedia -3 штуки, WI-FI роутер, учебно- наглядные пособия, вместимость 30-40 посадочных мест.

Обучающиеся ЛОВЗ обеспечиваются специальными электронными ресурсами.

Компьютерный класс: 190013, г.Санкт-Петербург Московский проспект, д. 24-26/49, лит.А №4 -30 м^2.

Оборудование компьютерного класса: 7 ПК Intel Pentium, с сетевыми фильтрами, 1ПК Intel Pentium с колонками и сетевым концентратором, Монитор 17 LGT710BH – 7 шт.). WI-FI роутер. Доступ по локальной сети к единой информационной системе, сайту библиотеки СПбГТИ(ТУ) с системой электронного поиска, электронными библиотеками, доступ к сайту «Роспатента», "Росстата", "Ростехнадзора", Internet. Программное обеспечение: ОС WINDOWS, OPEN OFFICE, Авторское программное обеспечение для расчета зон действия поражающих факторов, рисков, Matcad, ТОКСИ, FireCat , СОУТ, HZOB.

Обучающиеся ЛОВЗ обеспечиваются специальными электронными ресурсами.

Помещения для практических и лабораторных занятий: 190005, г.Санкт-Петербург Московский проспект, д. 24-26/49, лит.А №12 -19 м^2; ,№7 -67 м^2 , №19 -21 м^2 , № 35.-25 м^2.

Оборудование лабораторного класса: Помещения оснащены мебелью, учебно-наглядными пособиями, справочной литературой. Вместимость аудиторий 30 посадочных мест.

Обучающиеся ЛОВЗ обеспечиваются специальными электронными ресурсами

Помещения для самостоятельной работы: 190013, г.Санкт-Петербург Московский проспект, д. 24-26/49, лит.А №18 -19 м^2, №6а -28 м^2, №18 -8 м^2

Оборудование: Письменные столы, стулья, весы ВЛЭ-1100, сушильные шкафы, термостаты воздушные, водяные, химическая посуда, WI-FI, 30 посадочных мест.

Обучающиеся ЛОВЗ обеспечиваются специальными электронными ресурсами.

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 г.

Приложение № 1
к рабочей программе дисциплины

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

1 Перечень компетенций и этапов их формирования

Компетенции		
Индекс	**Формулировка**	**Этап формирования**
ОК – 5	Способность использовать основы правовых знаний в различных сферах профессиональной деятельности	заключительный
ОПК – 3	Способность решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	заключительный
ПК – 10	Способность изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследований	промежуточный

1. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкала оценивания.

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компетенции
Освоение раздела № 1	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации,	Ответы на вопросы 1,29,30,53,68, 83. Зачет.	ОК – 5, ОПК – 3

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компетенции
	исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.		
Освоение раздела № 2	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.	Ответы на вопросы 13-15,21,26,41,59-63. Зачет.	ОК – 5, ОПК – 3
Освоение раздела № 3	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых	Ответы на вопросы 10-12,45-47,51,52. Зачет.	ОК – 5, ПК – 10

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компетенции
	возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.		
Освоение раздела № 4	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.	Ответы на вопросы 22,23,27,28,31,32,36-38,69,79-80. Зачет.	ОК – 5, ОПК – 3
Освоение раздела № 5	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать	Ответы на вопросы 54-58,64,65,66. Зачет.	ОК – 5, ОПК – 3

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компетенции
	эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.		
Освоение раздела № 6	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.	Ответы на вопросы 16-17,42,48,76-77. Зачет.	ОК – 5, ПК – 10
Освоение раздела № 7	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации.	Ответы на вопросы 6-9,39,40,43,44. Зачет.	ОК – 5, ОПК – 3

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компетенции
	Умеет: навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.		
Освоение раздела № 8	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет; борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.	Ответы на вопросы 2-4,21,24,25,49, 50,78,81-82. Зачет.	ОК – 5, ПК – 10
Освоение раздела № 9	**Знает:** принципы информационной безопасности; основные угрозы информационной безопасности; структуру государственной тайны и коммерческой тайны предприятия; отличия между формами допуска к документам; методы и критерии оценки эффективности мероприятий по защите информации; содержание перечня сведений, относящихся к государственной тайне. **Владеет:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации. **Умеет:** навыками безопасной работы в сети Интернет;	Ответы на вопросы 5, 18-20,33-35,49,67,70-75. Зачет.	ОК – 5, ОПК – 3

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компетенции
	борьбы с компьютерными вирусами; организации раздельного доступа к файлам и папкам на компьютере; способами ограничения доступа к информации, представляющей собой государственную тайну.		

Шкала оценивания соответствует СТО СПбГТИ(ТУ):

промежуточная аттестация проводится в форме зачета, результат оценивается – «зачет», «незачет».

3. Типовые контрольные задания для проведения промежуточной аттестации.

1. Дайте определение термину информация
2. Средства и механизмы обеспечения аудита и методы анализа данных аудита.
3. Анализ безопасности DNS технологии.
4. Методы и средства контроля и сохранения целостности сетевого трафика.
5. Доступ на основе одноранговых паролей – достоинства и недостатки, методы и средства взлома.
6. Комплексный подход к построению систем антивирусной защиты.
7. Средства анализа защищенности компьютерной системы.
8. Защита информации в системах электронной почты.
9. Системы обнаружения сетевых атак.
10. Виды и средства атак на локальный компьютер.
11. Виды и средства атак на удаленный компьютер в сети.
12. Особенности и средства защиты информации в беспроводных сетях.
13. Виртуальные приватные сети (VPN). Сравнительный анализ средств построения.
14. Анализ возможности обеспечения безопасности в ОС Windows XP.
15. Сетевые атаки. Особенности, методы и средства защиты.
16. Методы и средства поиска программ-закладок и недокументированных функций в программном обеспечении.
17. Методы и средства считывания удаленных данных и данных с поврежденных магнитных носителей информации.
18. Методы и средства выявления сканирования портов.
19. Методы «социальной инженерии».
20. Политика безопасности организации – структура и особенности.
21. Анализ рисков информационной безопасности в компьютерных системах.
22. Управление рисками информационной безопасности в компьютерных системах.

23. Разработка рекомендаций работы с персоналом предприятия по обеспечению информационной безопасности.
24. Специфика проведения расследования инцидентов в сфере информационной безопасности.
25. Аварийный план действий в случае совершения атаки – структура и средства поддержки.
26. Сетевые вирусы. Особенности. Средства и способы удаления и предупреждения заражения.
27. Защита речевой информации при ее передаче по каналам связи.
28. Защита акустической информации, циркулирующей в защищаемых помещениях.
29. Правовое обеспечение информационной безопасности.
30. Методы и средства защиты интеллектуальной собственности.
31. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
32. Организация защищенного документооборота.
33. Анализ и оценка угроз информационной безопасности объекта.
34. Оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа.
35. Средства и методы физической защиты объектов.
36. Организация пропускного и внутриобъектового режима.
37. Организационные методы обеспечения информационной безопасности.
38. Защита информации при авариях и экстремальных ситуациях.
39. Обеспечение информационной безопасности учреждения при осуществлении международного научно-технического и экономического сотрудничества
40. Организационные и технические мероприятия, используемые для противодействия технической разведке.
41. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по каналам электромагнитных излучений и наводок.
42. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.
43. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы.
44. Парольное разграничение доступа и комбинированные методы.
45. Защита программных средств от несанкционированного копирования, исследования и модификации.
46. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.
47. Проблемы ключей системы шифрования.
48. Установление подлинности, электронная цифровая подпись.
49. Технология восстановления дисковой и оперативной памяти.
50. Особенности защиты информации в базах данных.
51. Защита программ от изменения и контроль целостности.

52. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях.
53. Защита документа в Microsoft Office.
54. Государственное регулирование в области информационной безопасности.
55. Ответственность за нарушение правовых норм защиты информации.
56. Структура и требования стандартов информационной безопасности.
57. Специальные требования и рекомендации по технической защите конфиденциальной информации
58. Средства охранной сигнализации на территории и в помещениях объекта информатизации.
59. Классификация каналов утечки информации.
60. Способы съема акустической информации.
61. Методы и средства защиты от утечки акустической информации.
62. Способы съема информации с телефонной линии.
63. Способы съема информации с каналов передачи информации.
64. Методы и средства обнаружения средств съема информации.
65. Правовые нормы обеспечения защиты информации на предприятии.
66. Проведение комплексных специальных проверок помещений.
67. Преодоление парольной защиты.
68. Физическая защита ПЭВМ от НСД. Контроль вскрытия аппаратуры.
69. Назначения и функции аппаратных модулей доверенной загрузки.
70. Методы и средства идентификации и аутентификации пользователей.
71. Назначение и структура подсистемы аудита.
72. Виды компьютерных вирусов.
73. Методы обнаружения известных и неизвестных вирусов.
74. Методы удаления последствий заражения вирусами.
75. Профилактика заражения вирусами КС. Действия пользователя при обнаружении заражения КС вирусами.
76. Масштабирование и сегментация локальных сетей в целях защиты информации.
77. Применение межсетевых экранов для. защиты информации при межсетевом взаимодействии.
78. Методы и средства восстановления работоспособности КС.
79. Функции администратора защищенной операционной системы по созданию и управлению учетными записями пользователей.
80. Обеспечение безопасности ресурсов с помощью файловой системы NTFS.
81. Политика и организация аудита ресурсов и событий системы защиты операционной системы.
82. Конфиденциальный обмен информацией с использованием асимметричных ключей шифрования.
83. Структура и функции системы защиты информации Secret Net.

а) Вопросы для оценки сформированности элементов компетенции ОК – 5 :

1. Дайте определение термину информация

2. Средства и механизмы обеспечения аудита и методы анализа данных аудита.
3. Анализ безопасности DNS технологии.
4. Методы и средства контроля и сохранения целостности сетевого трафика.
5. Доступ на основе одноранговых паролей – достоинства и недостатки, методы и средства взлома.
6. Комплексный подход к построению систем антивирусной защиты.
7. Средства анализа защищенности компьютерной системы.
8. Защита информации в системах электронной почты.
9. Системы обнаружения сетевых атак.
10. Виды и средства атак на локальный компьютер.
11. Виды и средства атак на удаленный компьютер в сети.
12. Особенности и средства защиты информации в беспроводных сетях.
13. Виртуальные приватные сети (VPN). Сравнительный анализ средств построения.
14. Анализ возможности обеспечения безопасности в ОС Windows XP.
15. Сетевые атаки. Особенности, методы и средства защиты.
16. Методы и средства поиска программ-закладок и недокументированных функций в программном обеспечении.
17. Методы и средства считывания удаленных данных и данных с поврежденных магнитных носителей информации.
18. Методы и средства выявления сканирования портов.
19. Методы «социальной инженерии».
20. Политика безопасности организации – структура и особенности.
21. Анализ рисков информационной безопасности в компьютерных системах.
22. Управление рисками информационной безопасности в компьютерных системах.
23. Разработка рекомендаций работы с персоналом предприятия по обеспечению информационной безопасности.
24. Специфика проведения расследования инцидентов в сфере информационной безопасности.
25. Аварийный план действий в случае совершения атаки – структура и средства поддержки.
26. Сетевые вирусы. Особенности. Средства и способы удаления и предупреждения заражения.
27. Защита речевой информации при ее передаче по каналам связи.
28. Защита акустической информации, циркулирующей в защищаемых помещениях.
29. Правовое обеспечение информационной безопасности.
30. Методы и средства защиты интеллектуальной собственности.
31. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
32. Организация защищенного документооборота.
33. Анализ и оценка угроз информационной безопасности объекта.
34. Оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа.

35. Средства и методы физической защиты объектов.
36. Организация пропускного и внутриобъектового режима.
37. Организационные методы обеспечения информационной безопасности.
38. Защита информации при авариях и экстремальных ситуациях.
39. Обеспечение информационной безопасности учреждения при осуществлении международного научно-технического и экономического сотрудничества
40. Организационные и технические мероприятия, используемые для противодействия технической разведке.
41. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по каналам электромагнитных излучений и наводок.

б) Вопросы для оценки сформированности элементов компетенции ОПК – 3:

42. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы.
43. Парольное разграничение доступа и комбинированные методы.
44. Защита документа в Microsoft Office.
45. Государственное регулирование в области информационной безопасности.
46. Ответственность за нарушение правовых норм защиты информации.
47. Структура и требования стандартов информационной безопасности.
48. Специальные требования и рекомендации по технической защите конфиденциальной информации
49. Средства охранной сигнализации на территории и в помещениях объекта информатизации.
50. Классификация каналов утечки информации.
51. Способы съема акустической информации.
52. Методы и средства защиты от утечки акустической информации.
53. Способы съема информации с телефонной линии.
54. Способы съема информации с каналов передачи информации.
55. Методы и средства обнаружения средств съема информации.
56. Правовые нормы обеспечения защиты информации на предприятии.
57. Проведение комплексных специальных проверок помещений.
58. Преодоление парольной защиты.
59. Физическая защита ПЭВМ от НСД. Контроль вскрытия аппаратуры..
60. Назначения и функции аппаратных модулей доверенной загрузки.
61. Методы и средства идентификации и аутентификации пользователей.
62. Назначение и структура подсистемы аудита.
63. Виды компьютерных вирусов.
64. Методы обнаружения известных и неизвестных вирусов.
65. Методы удаления последствий заражения вирусами.
66. Профилактика заражения вирусами КС. Действия пользователя при обнаружении заражения КС вирусами.
67. Функции администратора защищенной операционной системы по созданию и управлению учетными записями пользователей.
68. Обеспечение безопасности ресурсов с помощью файловой системы NTFS.
69. Структура и функции системы защиты информации Secret Net.

в) Вопросы для оценки сформированности элементов компетенции ПК – 10:

70. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.
71. Защита программных средств от несанкционированного копирования, исследования и модификации.
72. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.
73. Проблемы ключей системы шифрования.
74. Установление подлинности, электронная цифровая подпись.
75. Технология восстановления дисковой и оперативной памяти.
76. Особенности защиты информации в базах данных.
77. Защита программ от изменения и контроль целостности.
78. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях.
79. Масштабирование и сегментация локальных сетей в целях защиты информации.
80. Применение межсетевых экранов для защиты информации при межсетевом взаимодействии.
81. Методы и средства восстановления работоспособности КС.
82. Политика и организация аудита ресурсов и событий системы защиты операционной системы.
83. Конфиденциальный обмен информацией с использованием асимметричных ключей шифрования.

4. Типовые контрольные задания для проведения текущего контроля.

4.1 Темы для дискуссий:

1. Противодействие шпионажу на предприятиях.
2. Блокирование доступа к социальным сетям, сайтам с рабочего компьютера, панацея от взлома или дисциплинарная мера.
3. Промышленный шпионаж в современном мире.
4. Всемирная паутина благо или опасность.
5. Способы обеспечения защиты информации.
6. Криптоалгоритмы, что это и где они применяется.

6. 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.