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
_____2016 г.

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки
15.03.04 Автоматизация технологических процессов и производств

Направленность программы
Автоматизация технологических процессов и производств (по отраслям)

Квалификация
Бакалавр

Форма обучения
Очная

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

Санкт-Петербург
2016

Б1.В.13

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 №4от «09» апреля 2015

Заведующий кафедрой Т.Б. Чистякова

Одобрено учебно-методической комиссией факультета информационных технологий и управления
протокол от «20»ноября2015 № 4

Председатель В.В. Куркина

СОГЛАСОВАНО

Руководитель направления подготовки «Автоматизация технологических процессов и производств»		В.В. Куркина
Директор библиотеки		Т.Н. Старостенко
Начальник методического отдела учебно-методического управления		Т.И. Богданова
Начальник УМУ		С.Н. Денисенко

Содержание

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

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

Коды компетенции	Результаты освоения ООП *(содержание компетенций)*	Перечень планируемых результатов обучения по дисциплине
ОПК-2	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-- технологий и с учетом основных требований информационной безопасности	**знать** виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты, **уметь** выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-техни-ческие мероприятия по защите информации в ИС; **владеть** навыками работы с различными источниками информации
ОПК-3	способностью использовать современные информационные технологии, технику, прикладные программные средства при решении задач профессиональной деятельности	**знать** требования информационных систем и методы обеспечения информационной безопасности; **уметь** проводить обследования, выявлять информационные потребности пользователей, формировать требования к информационной системе **владеть** навыками эксплуатирования и сопровождения информационных систем и сервисов
ПК-1	способностью собирать и анализировать исходные информационные данные для проектирования технологических процессов изготовления продукции, средств и систем автоматизации, контроля,технологического оснащения, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством; участвовать в работах по расчету и проектированию процессов изготовления продукции и указанных средств и систем с использованием современных информационных технологий, методов и средств проектирования	**знать** методы идентификации; модели и методы криптографии, **уметь** применять методы защиты компьютерной информации при использовании и проектировании ИС в различных областях; **владеть** навыками работы с программно- инструментальными средствами

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.13 «Информационная безопасность» принадлежит к вариативной части обязательных дисциплин. Дисциплина базируется на знаниях, полученных студентами в курсах «Информатика», «Основы права». Дисциплина изучается на 2-ом курсе в 3-м семестре.

3. Объем дисциплины

Вид учебной работы	Всего, академ. часов
	Очная форма обучения
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	3/108
Контактная работа с преподавателем:	**56**
занятия лекционного типа	18
занятия семинарского типа, в т.ч.	
семинары, практические занятия	36
лабораторные работы	
курсовое проектирование (КР или КП)	-
КСР	2
другие виды контактной работы (контроль)	
Самостоятельная работа	**25**
Форма текущего контроля (Кр, реферат, РГР, эссе)	-
Форма промежуточной аттестации (КР, КП , зачет, экзамен)	Экзамен (27)

4 Содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4.1 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Занятия лекционного типа, акад. часы	Занятия семинарского типа, академ. часы		Самостоятельная работа,акад. часы	Формируемые компетенции
			Семинары и/или практические	Лабораторные работы		
1	Защита информации.	2	4		4	ОПК-2
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	2	2			ОПК-2; ОПК-3;
3	Идентификация и аутентификация.	2	4		2	ОПК-2; ПК-1;
4	Основы криптографии.	4	12		6	ОПК-3; ПК-1;

5	Формальные модели безопасности.	2	2		2	ОПК-2; ОПК-3;
6	Стандарты безопасности.	2	2		1	ОПК-3;
7	Методы защиты программ от внешних воздействий.	2	6		4	ПК-1;
8	Вопросы организации информационной безопасности на предприятии.	2	4		6	ОПК-3; ПК-1
	Итого	18	36		25	

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.	2	
2	Классификация средств защиты. Службы и механизмы обеспечения безопасности.	2	
3	Идентификация и аутентификация. Основные понятия и концепции. Биометрия.	2	
4	Основы криптографии. Основные понятия и определения. Криптографические алгоритмы. Контроль целостности информации. Функции хеширования. Электронная подпись.	4	
5	Формальные модели безопасности. Политика безопасности. Основные модели и критерии защищенности.	2	
6	Стандарты безопасности. Роль и задачи стандартов. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	2	
7	Методы защиты программ от внешних воздействий.	2	
8	Организация информационной безопасности на предприятии. Правовые, организационные и технические мероприятия. Документальное обеспечение. Защита интеллектуальной собственности: защита программ для ЭВМ и баз данных.	2	

4.3. Занятия семинарского типа

4.3.1. Семинары, практические занятия

№ раздела дисципли-ны	Наименование темы и краткое содержание занятия	Объем, акад. часы	Примечание
1	Изучение законодательной базы в области защиты информации и информационных технологий	2	
2	Анализ угроз информационной системы. Формирование комплекса требований к системе защиты	2	
3	ПО «Daily». Биометрическая идентификации и элементы криптоанализа	4	
4	Изучение основ криптографии с помощью компьютерной обучающей и тестирующей системы «Криптография	2	
4	PGP. Криптографическое закрытие информации. Ассиметричные алгоритмы. Контроль подлинности, целостности и авторства сообщений	4	
4	Самостоятельная разработка программного продукта, реализующего алгоритм (элемент) криптографического закрытия информации	6	
7	«Itkey». Изучения средств защиты программных продуктов	6	
5	Построение модели ролевой политики безопасности	2	
6	Изучение таксонометрии стандартов безопасности	2	
8	Изучение средств антивирусной безопасности	2	
8	Программы для ЭВМ и БД – объекты охраны интеллектуальной собственности. Комплексная защита	4	

4.3.2. Лабораторные занятия

Не предусмотрены.

4.4.Самостоятельная работа обучающихся

№ раздела-дисципли-ны	Перечень вопросов для самостоятельного изучения	Объем, акад. часы
1	Безопасность функционирования информационных систем	4
2	Свойства защищенных систем	
3	Механизмы подтверждения подлинности пользователя. Биометрия. Схема идентификации с нулевой передачей знаний	2
4	Исследование Шеннона в области криптографии. Сравнение отечественного и американского стандартов шифрования. Функции дискретного логарифмирования	6

№ раздела-дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы
5	Ролевая политика безопасности	2
6	Единые критерии безопасности информационных технологий	1
7	Средства обнаружения и защиты программ от разрушающих программных воздействий	4
8	Программно-аппаратные средства защиты ЭВМ и сетей, ограничения доступа к компонентам сетей предприятий.	6
	Итого	**25**

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

– чтение студентами рекомендованной литературы и усвоение теоретического материала дисциплины;

– подготовку к лабораторным занятиям;

– работу с Интернет-источниками;

– подготовку к сдаче экзамена.

Планирование времени на самостоятельную работу, необходимого на изучение настоящей дисциплины, студентам лучше всего осуществлять на весь семестр, предусматривая при этом регулярное повторение пройденного материала.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Методические указания для обучающихся по организации самостоятельной работы по дисциплине, включая перечень тем самостоятельной работы, формы текущего контроля по дисциплине и требования к их выполнению размещены в электронной информационно-образовательной среде СПбГТИ(ТУ) на сайте: http://media.technolog.edu.ru

6. Фонд оценочных средств для проведения промежуточной аттестации

Своевременное выполнение обучающимся мероприятий текущего контроля позволяет превысить (достигнуть) пороговый уровень («удовлетворительно») освоения предусмотренных элементов компетенций.

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

Промежуточная аттестация по дисциплине проводится в форме экзамена.

К сдаче экзамена допускаются студенты, выполнившие все формы текущего контроля.

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

Фонд оценочных средств по дисциплине представлен в Приложении № 1.

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

а) основная литература

1 Головин, Ю. А. Информационные сети : учеб. для вузов / Ю. А. Головин, А. А. Суконщиков, С. А. Яковлев. – М. : Академия, 2011. – 376 с.

2 Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – 5-е изд., стер. – М. : Академия, 2011. – 331 с.

3 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. - (Профессиональное образование). - Библиогр.: с. 401-408

4 Норенков, И. П. Автоматизированные информационные системы : учеб. пособие / И. П. Норенков. – М. : Изд-во МГТУ им. Н.Э. Баумана, 2011. – 342 с.

б)дополнительная литература

5 Методы и средства защиты компьютерной информации. Межсетевое экранирование : учеб. пособие / В.А. Мулюха [и др.] – СПб. : Изд-во Политехн. Ун-та, 2010. – 90 с.

6 Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие для вузов / А. А. Афанасьев [и др.], под ред. А.А. Шелупанова [и др.] . – М. : Горячая линия – Телеком. 2009. – 552с.

в)вспомогательная литература

7 Калинкина, Т. И. Телекоммуникационные и вычислительные сети : архитектура, стандарты и технологии / Т. И. Калинкина, Б. В. Костров, В. Н. Ручкин. – СПб: БХВ-Петербург, 2010. – 283 с.

8 Зегжда, Д. П. Основы безопасности информационных систем / Д. П.Зегжда А.М. Ивашко. – М.: Горячая линия – Телеком; 2006 г.; 452 с.

9 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (редак. От 02.07.2013)

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

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

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

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

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

г) программное обеспечение:

В качестве программного обеспечения в лабораторных работах используются InternetExplorer, BorlandC++ Builder, учебно-методический комплекс «Система защиты программного продукта» («ItKey»). Кузнецова Г.В., Авербух А.Б., Жадановская Н.П., свидетельство о государственной регистрации программы для ЭВМ №2007613442 от 15.08.07.

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

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

- электронно-библиотечные системы:

- электронная справочная система правовой информации Консультант+ http://www.consultant.ru
- «Электронный читальный зал – БиблиоТех» https://technolog.bibliotech.ru/;
- «Лань (Профессия)» https://e.lanbook.com/books/.
- http://www.viniti.msk.su/ - Всероссийский институт научной и технической информации (ВИНИТИ)
- http://www.icsti.su/portal/index.html - Международный центр научной и технической информации (МЦНТИ)
- http://www.vntic.org.ru/ - Всероссийский научно-технический информационный центр

9. Методические указания для обучающихся по освоению дисциплины

Все виды занятий по дисциплине «Информационнаябезопасность» проводятся в соответствии с требованиями следующих СТП:
СТП СПбГТИ 040-02. КС УКДВ. Виды учебных занятий. Лекция. Общие требования;
СТО СПбГТИ 018-2014. КС УКДВ. Виды учебных занятий. Семинары и практические занятия. Общие требования к организации и проведению.
СТП СПбГТИ 048-2009. КС УКДВ. Виды учебных занятий. Самостоятельная планируемая работа студентов. Общие требования к организации и проведению.

Планирование времени, необходимого на изучение данной дисциплины, лучше всего осуществлять на весь семестр, предусматривая при этом регулярное повторение пройденного материала.

Основными условиями правильной организации учебного процесса для студентов является:

плановость в организации учебной работы;
серьезное отношение к изучению материала;
постоянный самоконтроль.

На занятия студент должен приходить, имея багаж знаний и вопросов по уже изученному материалу.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

10.1. Информационные технологии

В учебном процессе по данной дисциплине предусмотрено использование информационных технологий:

чтение лекций с использованием слайд-презентаций;
изучение мультимедийных материалов;
работа со специально разработанными программными продуктами;
контроль знаний с помощью компьютерных тестов;
взаимодействие с обучающимися посредством электронной почты.

10.2. Программное обеспечение

MicrosoftOffice , «ItKey» свид-во №2007613442 от 15.08.07.; PGP; Daily

10.3. Информационные справочные системы

Правовые справочные системы «Консультант-Плюс», «Гарант».

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

Для ведения лекционных и практических занятий используется аудитория, оборудованная средствами оргтехники, на 15 посадочных мест.

Для проведения лабораторных занятий используется компьютерный класс, оборудованный персональными компьютерами, объединенными в сеть и имеющими доступ в интернет.

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
«Информационная безопасность»

1. Перечень компетенций и этапов их формирования.

Компетенции		
Индекс	**Формулировка**	**Этап формирования**
ОПК-2	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-- технологий и с учетом основных требований информационной безопасности	промежуточный
ОПК-3	способностью использовать современные информационные технологии, технику, прикладные программные средства при решении задач профессиональной деятельности	промежуточный
ПК-1	способностью собирать и анализировать исходные информационные данные для проектирования технологических процессов изготовления продукции, средств и систем автоматизации, контроля,технологического оснащения, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством; участвовать в работах по расчету и проектированию процессов изготовления продукции и указанных средств и систем с использованием современных информационных технологий, методов и средств проектирования	промежуточный

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

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания *(правильные ответы на вопросы к экзамену)*	Компетенции
Освоение раздела № 1	Основные понятия и определения. Источники и риски функционирования информационных систем. Угрозы, атаки и уязвимости компьютерных систем. Основные задачи обеспечения безопасности информации.	№ 1-4	ОПК-2; ОПК-3
2	Классификация средств защиты. Службы и механизмы обеспечения безопас-	№ 3-4	ОПК-2;

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания *(правильные ответы на вопросы к экзамену)*	Компетенции
	ности.		
3	Идентификация и аутентификация. Основные понятия и концепции. Биометрия.	№ 28-30	ОПК-3; ПК-1
4	Основы криптографии. Основные понятия и определения. Криптографические алгоритмы. Контроль целостности информации. Функции хеширования. Электронная подпись.	№ 5-15	ПК-1;
5	Формальные модели безопасности. Политика безопасности. Основные модели и критерии защищенности.	№ 16-19	ОПК-3
6	Стандарты безопасности. Роль и задачи стандартов. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	№ 20-24	ОПК-3
7	Методы защиты программ от внешних воздействий.	№ 25-30	ОПК-3;
8	Организация информационной безопасности на предприятии. Правовые, организационные и технические мероприятия. Документальное обеспечение. Защита интеллектуальной собственности: защита программ для ЭВМ и баз данных.	№ 1-4,6,15,16, 24-30	ОПК-2; ОПК-3;

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

3. Типовые контрольные вопросы для сдачи экзамена

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.

10. ГСЧ: типы, применение. Число инициализации.

9. ГОСТ 28147-89. Ключевая информация. Основной шаг криптоприобразования.

10. ГОСТ 28147-89. Режимы шифрования. Достоинства и недостатки. Имитовставка: понятие и применение.

11. RSA

12. PGP. Принцип функционирования. Свойства ключа.

13. Хэш-функции. Определение, свойства, применение.

14. Электронная подпись. Понятие, структура построения, использование.

15. Проверка целостности данных. Методы и функции.

16. Политика безопасности. Определение. Функции, виды, базовые представления.

17. Мандатная модель Белла-Ла Падулы. Достоинства и недостатки.

18. Дискреционная модель Харрисона-Руззо-Ульмана. Достоинства и недостатки.

19. Ролевая политика безопасности. Формальное представление. Достоинства и недостатки. Виды.

20. Стандарты безопасности. Основные цели и функции. Пользователи.

21. Оранжевая книга-первый стандарт. Таксономия критериев безопасности.

22. Стандарты безопасности. Обобщенные показатели сравнения стандартов.

23. Единые критерии безопасности информационных технологий. Основные понятия и положения. Профиль и проект защиты.

24. Единые критерии безопасности информационных технологий. Требования безопасности (функциональные и адекватности). Таксономия критериев.

25. Реестр и его использование для обеспечения безопасности программного продукта.

26. Безопасность БД. Методы и средства.

27. Безопасность ПО. Методы и средства.

28. Идентификация и аутентификация. Биометрическая защита.

29. Структура системы защиты от несанкционированного доступа.

30. Статические и динамические характеристики среды.

Вопросы для оценки сформированности элементов компетенции:

ОПК-2: № 1-4, 20-24
ОПК-3 № 11-19
ПК-1 № 5-10, 25-30

К экзамену допускаются студенты, выполнившие все формы текущего контроля. При сдаче экзамена, студент получает три вопроса из перечня, приведенного выше.

Время подготовки студента к устному ответу на вопросы - до 40 мин.

4. Методические материалы для определения процедур оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Промежуточная аттестация по дисциплине проводится в соответствии с требованиями СТП

СТО СПбГТИ(ТУ) 016-2015. КС УКДВ. Порядок проведения зачетов и экзаменов.