Автономная некоммерческая организация высшего образования
"НАЦИОНАЛЬНЫЙ ОТКРЫТЫЙ ИНСТИТУТ
Г.САНКТ-ПЕТЕРБУРГ"
Кафедра математических и естественнонаучных дисциплин

Рабочая программа дисциплины

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки 09.03.03 Прикладная информатика

Профиль подготовки – Прикладная информатика в экономике

Квалификация выпускника – бакалавр

Форма обучения – очная, заочная

Санкт-Петербург
2021

Программа дисциплины "Информационная безопасность" и её учебно-методическое обеспечение требованиями (ФГОС ВО: Приказ Минобрнауки России от 19 сентября 2017 г. № 922 к обязательному минимуму содержания и уровню подготовки дипломированного бакалавра по блоку 1 "Дисциплины (модули)" (Б1.О.16, обязательная часть) федерального государственного образовательного стандарта высшего образования по направлению 09.03.03 "Прикладная информатика".

Программа рассмотрена и утверждена на заседании кафедры математических и естественнонаучных дисциплин, протокол № 1/21 от «_06__»_сентября_____2021__г.

Зав. кафедрой _____ Боброва Л.В._____

Рабочую программу подготовили: _____преп. Егорова О.П.

СОДЕРЖАНИЕ

1. Цель и задачи дисциплины

Цель дисциплины является формирование у студентов правильных основ знаний по информационной безопасности (ИБ), необходимых специалистам, занимающимся вопросами проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС).

Задачами дисциплины является изучение:

- дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности ВС/ИС;
- сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

2. Место дисциплины в структуре ООП

Дисциплина «Информационная безопасность» входит в часть обязательных дисциплин (Б1.О.16) ОПОП блока 1 «Дисциплины (модули)», включенных согласно ФГОС ВО, в учебный план направления подготовки 09.03.03 Прикладная информатика. Предшествующими курсами, на которых непосредственно базируется дисциплина «Информационная безопасность» является курсы «Информатика и программирование», «Архитектура электронных вычислительных машин и вычислительные системы», «Операционные системы».

Дисциплина «Информационная безопасность» является основополагающей для изучения дисциплин базовой части учебного плана: «Проектирование информационных систем», «Информационные системы и технологии», а также дисциплин вариативной части «Корпоративные информационные системы», «Электронная коммерция», «Интернет-экономика», «Интернет-банкинг»..

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Универсальные компетенции (УК):

Наименование категории (группы) универсальных компетенций	**Код и наименование универсальной компетенции выпускника**	**Код и наименование индикатора достижения универсальной компетенции**
Системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач. УК-1.2.Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности. УК-1.3.Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений
Разработка и реализация проектов	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения,	УК-2.1.Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.2.Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и

	исходя из действующих правовых норм, имеющихся ресурсов и ограничений	основные направления работ. УК-2.3.Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.

Общепрофессиональные компетенции (ОПК):

Код общепрофессиональной компетенции выпускника	**Наименование общепрофессиональной компетенции выпускника**	**Код и наименование индикатора достижения общепрофессиональной компетенции выпускника**
ОПК-2	ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства и использовать их при решении задач профессиональной деятельности	ОПК-2.1. Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. ОПК-2.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
ОПК-3	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1.Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2.Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры

		с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3.Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ОПК-6	Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования	ОПК-6.1. Знает основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования. ОПК-6.2.Умеет применять методы теории систем и системного анализа, математического, статистического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий. ОПК-6.3.Владеет навыками проведения инженерных расчетов основных показателей результативности создания и применения информационных систем и технологий.

Профессиональные компетенции (ПК):

Код профессиональной компетенции выпускника	**Наименование профессиональной компетенции выпускника**	**Код и наименование индикатора достижения профессиональной компетенции выпускника**
ПК-1	Способность проводить	**знать:** отраслевую

	обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе.	специализированную терминологию, технологии сбора информации стандарты проектирования и разработки информационного контента и пользовательского интерфейса **уметь:** разрабатывать концептуальную модель прикладной области; выбирать инструментальные средства и технологии для создания информационного обеспечения решения прикладных задач **владеть** методами анализа прикладной области и прикладных процессов; информационных потребностей
ПК-2	Способность разрабатывать и анализировать прикладное программное обеспечение	**знать**: компьютерные технологии представления и управления данными; основы сетевых технологий; основы программирования информационного контента на языках высокого уровня; **уметь:** разрабатывать программное обеспечение с помощью языков программирования информационного контента; размещать информационный контент в глобальных и локальных сетях; использовать инструментальные среды поддержки разработки, системы управления контентом; адаптировать и конфигурировать программное обеспечение для решения поставленных задач; **владеть** методами адаптивного сопровождения программного продукта или информационного ресурса.

Ожидаемые результаты**:** *в результате изучения дисциплины бакалавры приобретут:*

Знания:

- видов угроз ИС и методов обеспечения информационной безопасности.

Умения:

- выявлять угрозы информационной безопасности;
- обосновывать организационно-технические мероприятия по защите информации в ИС.

Представления:

о круге задач, решаемых при защите информации об основных сферах применения полученных знаний.

Овладеют:

- способностью работы со средствами защиты информации.

4. Структура и содержание дисциплины

Структура преподавания дисциплины

Общая трудоемкость дисциплины «Информационная безопасность» для направления 09.03.03 Прикладная информатика составляет 5 зачетных единиц или 180 часов общей учебной нагрузки (см. табл. 1,2 и 3).

Таблица 1

Структура дисциплины
Дляочной/ заочной формы обучения

№ п/п	Наименование раздела дисциплины	Курс	Всего часов	Виды учебной работы (в академических часах)			Форма контроля
				Л	СР	ПЗ	
1.	Ключевые аспекты и вопросы формирования информационной безопасности	3/3	26/26	3/1	20/24	3/1	Тестиро-вание
2.	Защта информации в информационных сетях. Понятия сервисов безопасности	3/3	26/26	3/1	19/23	4/2	Тестиро-вание
3.	Понятия о служебной и государственной тайне. Шифрование информации	3/3	26/26	6/2	16/22	4/2	Тестиро-вание
4.	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	3/3	26/26	6/2	13/21	7/3	Тестиро-вание
5.	**Промежуточная аттестация**	35/3	**4/4**				**Зачет с оценкой**
	***Итого*:**		108/108	18/6	72/90	18/8	

Содержание дисциплины

Содержание разделов/тем дисциплины представлено в табл. 2.

Таблица 2

Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела	Результат обучения, формируемые компетенции
1.	Ключевые аспекты и вопросы формирования информационной безопасности	Защита ПК от несанкционированного доступа. Механизмы защиты компьютеров от несанкционированного доступа. Физическая защита. Опознавание (аутентифика-ция). Криптография	Знать: Основы защиты ПК от несанкционированного доступа Уметь: проводить физическую защиту информации Владеть механизмами защиты компьютеров от несанкционированного доступа. УК-1, УК-2, ОПК-2, ОПК-3
2.	Защита информации в информационных сетях. Понятия сервисов безопасности	Защита информации в сетях. Цели защиты информации в сетях ЭВМ. Уровни защиты протокола передачи данных в сети. Особенности защиты информации в вычислительных сетях. Понятие сервисов безопасности.	Знать: цели защиты информации в сетях ЭВМ. Уметь: работать с уровнями защиты протоколов передачи данных в сети. Владеть: особенностями защиты информации в вычислительных сетях УК-1, ОПК-3, ОПК-6
3.	Понятия о служебной и государственной тайне. Шифрование информации	Понятие о служебной и государственной тайне . Грифы ограничения доступа к информации. Снятие грифа конфиденциальности с информации. История шифрования информации. Симметрическое шифрование информации. Ассиметричное шифрование информации.	Знать: международное и российское законодательство в сфере информационной безопасности Уметь: Строить структуру нормативно-правовых документов деятельности компании на базе российского законодательства Владеть: методами шифрования информации УК-2, ОПК-2, ПК-1
4.	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	Компьютерные вирусы. Классификация компьютерных вирусов. Антивирусные программы. Спамы. Виды спамеров. Защита от спамов. Защита на уровне сервера. Утечка почтового адреса. Диспетчер писем. Клиентские антиспам-фильтры.	Знать: классификация компьютерных вирусов. Владеть: Защитой информации на уровне сервера ОПК-3, ПК-2

5. Образовательные технологии

В соответствии с требованиями ФГОС удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 20% аудиторных занятий. Используемые в процессе изучения дисциплины образовательные технологии представлены в табл. 3.

Таблица 3

Образовательные технологии

№ пп	Разделы Темы	Образовательные технологии
1.	Ключевые аспекты и вопросы формирования информационной безопасности	Интерактивная лекция с использованием мультимедиа Участие в вебинаре Использование электронного учебника, электронной библиотеки возможностей сети Интернет
2	Защита информации в информационных сетях. Понятия сервисов безопасности	Интерактивная лекция с использованием мультимедиа. Проведение практической работы с использованием системы Moodle. Использование электронного учебника, электронной библиотеки, возможностей сети Интернет. Участие в вебинаре.
3	Понятия о служебной и государственной тайне. Шифрование информации	Интерактивная лекция с использованием мультимедиа Участие в вебинаре Использование электронного учебника, электронной библиотеки возможностей сети Интернет
4	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	Интерактивная лекция с использованием мультимедиа. Проведение практической работы с использованием системы Moodle. Использование электронного учебника, электронной библиотеки, возможностей сети Интернет. Участие в вебинаре.

6. Самостоятельная работа студентов

Сведения по организации самостоятельной работы студентов в процессе изучения дисциплины представлены в табл. 4

Таблица 4

Характеристика самостоятельной работы студентов

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы	Часы	Компетенции (ОПК, ПК)
1.	Ключевые аспекты и вопросы формирования информационной безопасности	Механизмы защиты компьютеров от несанкционированного доступа. Опознавание (аутентификация).	20/24	УК-1, УК-2, ОПК-2, ОПК-3
2	Защита информации в информационных сетях. Понятия сервисов безопасности	Защита информации в сетях.. Уровни защиты протокола передачи данных в сети. Особенности защиты информации в вычислительных сетях..	19/23	УК-1, ОПК-3, ОПК-6
3	Понятия о служебной и государственной тайне. Шифрование информации	Понятие о служебной и государственной тайне . Симметрическое шифрование информации. Ассиметричное шифрование информации.	16/22	УК-2, ОПК-2, ПК-1
4	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	Антивирусные программы. Спамы. Виды спамеров. Защита от спамов. Защита на уровне сервера. Диспетчер писем. Клиентские антиспам-фильтры.	13/21	ОПК-3, ПК-2

7. Учебно-методическое и информационное обеспечение дисциплины

Список основной и дополнительной литературы

а) основная литература

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш, Изд-во РИОР, 2021, 336 с. (бакалавриат). Режим доступа: https://znanium.com/catalog/document?id=364911.

2. Озерский, С.В. Информационная безопасность: учебное пособие / С.В. Озерский и др. , Самарский юридический институт ФСИН РФ, 2019. – 84 с. (бакалавриат). Режим доступа https://znanium.com/catalog/document?id=358668.

3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин, Издательский дом ФОРУМ, 2021. – 416 с. (профессиональное образование). Режим доступа https://znanium.com/catalog/document?id=364622

4. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1 - Режим доступа: http://znanium.com/catalog/product/997105

5. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — М. : ИНФРА-М, 2018. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/13571. - Режим доступа: http://znanium.com/catalog/product/925825

6. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

б) дополнительная литература

1. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: ISBN 978-5-00091-079-5. Режим доступа: http://znanium.com

2. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. Режим доступа: http://biblioclub.ru

3. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 Режим доступа: http://biblioclub.ru

Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 432 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/987326

4. Криптография и безопасность в технологии .NET / Торстейнсон П., Ганеш Д.Г., - 3-е изд., (эл.) - М.:БИНОМ. ЛЗ, 2015. - 482 с.: ISBN 978-5-9963-2952-6 - Режим доступа: http://znanium.com/catalog/product/478090

5. Баранова Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 2-е изд. – Москва : РИОР : ИНФРА-М, 2014. – 256

6. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование:Бакалавриат). —Режим доступа. www.dx.doi.org/10.12737

в) программное обеспечение

ОС Windows XP, Windows 7, GPSS World (student version), «Matlab» и «Fann Explorer».

7.2 Базы данных, информационно-справочные и поисковые системы

Лицензионные ресурсы:
http://znanium.com/

Электронно-библиотечная система образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия. Удобный поиск по ключевым словам, отдельным темам и отраслям знания.

http://biblioclub.ru/

«Университетская библиотека онлайн».

Интернет-библиотека, фонды которой содержат учебники и учебные пособия, периодику, справочники, словари, энциклопедии и другие издания на русском и иностранных языках. Полнотекстовый поиск, работа с каталогом, безлимитный постраничный просмотр изданий, копирование или распечатка текста (постранично), изменение параметров текстовой страницы, создание закладок и комментариев.

Google, Yahoo, Yandex, Rambler и.т.д.

7.3. Перечень учебно-методических материалов, разработанных ППС кафедры

1. Рыбакова Е.А. Защита информации в информационных системах. Опорный конспект.- СПб: НОИР, 2013.- 37 стр.
2. Рыбакова Е.А. Защита информации. Криптография Методические указания к выполнению практических работ..- СПб: НОИР, 2014.- 19 стр.

7.4. Вопросы для самостоятельной подготовки

Разделы	Вопросы для самостоятельного изучения
Ключевые аспекты и вопросы формирования информационной безопасности	Механизмы защиты компьютеров от несанкционированного доступа. Опознавание (аутентификация).
Защита информации в информационных сетях. Понятия сервисов безопасности	Защита информации в сетях. Уровни защиты протокола передачи данных в сети. Особенности защиты информации в вычислительных сетях..
Понятия о служебной и государственной тайне. Шифрование информации	Понятие о служебной и государственной тайне . Симметрическое шифрование информации. Ассиметричное шифрование информации.
Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	Антивирусные программы. Спамы. Виды спамеров. Защита от спамов. Защита на уровне сервера. Диспетчер писем. Клиентские антиспам-фильтры.

7.5. Вопросы для подготовки к зачету

1. Перечислите основные механизмы защиты ПК от несанкционированного доступа.
2. Перечислите основные методы идентификации пользователей.
3. Что такое распознавание в режиме диалога.
4. Что такое распознавание опознавание по специальным идентификационным карточкам.
5. В чем заключается работа хеш-функции
6. Перечислите средства для опознавания компонентов обработки данных.
7. Перечислите задачи защиты информации в сетях ЭВМ.
8. Основное назначение сетевого уровням защиты информации в сети
9. Какой контроль осуществляется на транспортном уровне
10. Что такое криптозащита?
11. Что такое сервис безопасности?
12. Что является гарантом целостности передаваемых данных
13. Перечислите уровни защиты протоколов передачи данных в сети.
14. Назовите особенность защиты информации в вычислительных сетях
15. Назовите место сервисов безопасности в архитектуре информационных систем
16. Что такое служебная тайна?
17. Какие вы знаете грифы ограничения доступа.
18. Перечислите правила доступа к файлам с различным уровнем доступности, если пользователь имеет уровень доступа «Секретно»
19. Что такое симметричное шифрование
20. Перечислите признаки проявления вирусов
21. Перечислите вирусы, классифицируемые по среде обитания
22. Перечислите виды антивирусных программ.
23. Что такое компьютерный вирус, как он проявляется и какие средства используются для защиты от него?
24. Что такое спам.
25. Перечислите методы защиты от спамов.

Тесты для репетиционного тестирования расположены на сервере дистанционных образовательных технологий вуза.

Темы курсовых и контрольных работ, рефератов, курсовых проектов

Не предусмотрено.

8. Методические рекомендации по изучению дисциплины

Изучение дисциплины производится в тематической последовательности. Каждому практическому занятию и самостоятельному изучению материала предшествует лекция по данной теме.

Для успешного усвоения материала при начитке лекций студентам сообщаются адреса электронной почты, по которым они могут получить в электронном виде материал, отражающей основные положения теоретических основ и практических методов дисциплины.

В качестве оценочных средств для текущего контроля успеваемости и промежуточной аттестации предлагается использовать тестовые задания.

Методические рекомендации для преподавателя

Преподавание дисциплины «Информационная безопасность» базируется на компетентностном, практико-ориентированном подходе. Методика преподавания дисциплины направлена на организацию систематической планомерной работы студента в течение семестра независимо от формы его обучения. В связи с этим следует обратить внимание на особую значимость организаторской составляющей профессиональной деятельности преподавателя.

Основная работа со студентами проводится на аудиторных лекциях и лабораторных занятиях. Лекционный курс включает установочные, проблемные, обзорные лекции. Интерактивность лекционного курса обеспечивается оперативным опросом или тестированием в конце занятия. Широко применяются методы диалога, собеседований и дискуссий в ходе лекции. Проблемное обучение базируется на примерах из истории науки. Самостоятельная работа студентов всех форм обучения организуется на учебном сайте университета. Практические занятия построены с целью ознакомления студентов с методами научных исследований, привития им навыков научного экспериментирования, творческого исследовательского подхода к изучению предмета, логического мышления.

9. Материально-техническое обеспечение дисциплины

1. Компьютерный класс, позволяющий проводить вебинары
2. Аудитории, оснащенные мультимедиа оборудованием для демонстрации презентаций, видеопродукции
3. Возможность подключения к платформе Moodle.

Требования к программному обеспечению, используемому при изучении учебной дисциплины:

Для изучения дисциплины используется лицензионное программное обеспечение, в том числе:

- Microsoft Office
- Интернет-навигаторы.

10. Согласование и утверждение рабочей программы дисциплины
Лист согласования рабочей программы дисциплины

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Прикладная информатика (утвержденному Приказом от 19 сентября 2017 г. № 922, учебным планом института по этому же направлению, утвержденному ученым советом 20.12.2017г).

Автор программы - преп Егорова О.П.

_____ _____

Дата Подпись

Программа рассмотрена и утверждена на заседании кафедры математических и естественнонаучных дисциплин, протокол № 1/21 от «_06__»_сентября_____2021__г.

Зав. кафедрой _____ Боброва Л.В._____

Декан факультета _____ Пресс И.А.

(подпись) (Фамилия и инициалы)

Согласовано

Проректор по учебной работе _____ (подпись) Тихон М.Э. (ФИО)

ЛИСТ ИЗМЕНЕНИЙ,
ВНОСИМЫХ В РАБОЧУЮ ПРОГРАММУ

Номер изменения	Дата	Страницы с изменениями	Перечень и содержание откорректированных разделов рабочей программы