Автономная некоммерческая организация высшего образования
Национальный открытый институт г. Санкт-Петербург
Кафедра математических и естественно-научных дисциплин

Рабочая программа учебной дисциплины

«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки - 38.03.01 Экономика
Направленность (профиль) подготовки – Экономика предприятий и организаций
Квалификация выпускника – бакалавр
Форма обучения – очная, заочная, очно-заочная

Санкт-Петербург
2021

Рабочая программа учебной дисциплины «Защита информации» (Б1.В.05) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.01 «Экономика» (Приказ Минобрнауки России № 954 от 12.08.2020) к обязательному минимуму содержания и уровню подготовки дипломированного бакалавра.

Рабочая программа рассмотрена и утверждена на заседании кафедры математических и естественно-научных дисциплин (протокол № 10/18 от 06.03.2021г.).

Зав. кафедрой: _____Боброва Л.В., к.т.н.

Рабочую программу подготовила: _____Боброва Л.В., к.т.н.

СОДЕРЖАНИЕ

1. Цель и задачи дисциплины

Цель дисциплины - 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 ОПОП ВО

Учебная дисциплина «Защита информации» (Б1.В.05) включена в часть, формируемую участниками образовательных отношений (обязательные дисциплины) Блока 1 «Дисциплины (модули)», согласно ФГОС ВО для направления подготовки 38.03.01 «Экономика».

Предшествующими курсами, на которых непосредственно базируется дисциплина «Защита информации» является курс Информатики.

Дисциплина «Защита информации» является основополагающей для изучения дисциплин вариативной части учебного плана: Информационные модели в экономике, Компьютеризация финансовых расчетов.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Общепрофессиональные компетенции:

Код общепрофессиональной компетенции	**Наименование общепрофессиональной компетенции**	**Код и наименование индикатора достижения общепрофессиональной компетенции**
ОПК-5	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ИОПК-5.1. Имеет навыки работы с компьютером как средством управления информацией, способен работать с информацией в глобальных компьютерных сетях. ИОПК-5.2. Применяет знания об основных методах, способах и средствах получения, хранения и переработки информации в целях реализации функций профессиональной деятельности с учетом основных требований информационной безопасности

		ИОПК-5.3. Решает стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий

Профессиональные компетенции:

Код профессиональной компетенции	**Наименование профессиональной компетенции**	**Код и наименование индикатора достижения профессиональной компетенции**
ПК-5	Способен использовать для решения коммуникативных задач современные технические средства и информационные технологии	ПК-5.1. Участвует в проведении комплексного обследования информационных потребностей, средств информационного и аппаратного обеспечения существующей ИТ-архитектуры предприятия ПК-5.2. Участвует в проекте формирования целевой ИТ-архитектуры предприятия и ее компонентов ПК-5.3. Решает коммуникативные задачи профессиональной деятельности с применением технических средств и информационных технологий

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.

***Овладеют*:**

- способностями работы со средствами защиты информации.

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Общая трудоемкость дисциплины «Защита информации» для направления 38.03.01 «Экономика» составляет 4 зачетных единиц или 144 часов общей учебной нагрузки (см. табл. 1,2 и 3).

Таблица 1

Структура дисциплины
(очная/заочная/очно-заочная форма обучения)

№ п/п	Наименование раздела дисциплины	Семестр /курс	Всего часов	Виды учебной работы (в академических часах)			Форма контроля
				Л	СР	ПЗ	

1.	Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия	3/2	27/26/26	9/7/7	9/12/12	9/7/7	Тестирование
2.	Защищенная информационная система. Уровни и структура ИБ	3/2	27/28/28	9/8/8	9/12/12	9/8/8	Тестирование
3.	Модели и стандарты в сфере ИБ и управления рисками ИБ	4/2	27/26/26	9/7/7	9/12/12	9/7/7	Тестирование
4.	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	4/2	27/28/28	9/8/8	9/12/12	9/8/8	Тестирование
	Промежуточная аттестация		**36/36/36**				**Экзамен**
	ИТОГО:		**144/144/144**	**36/30/30**	**36/48/48**	**36/30/30**	

4.2. 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 современного предприятия	Тема 1. Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности Тема 2. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности Тема 3. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности	Знать: современные средства, методы и технология обеспечения информационной безопасности Уметь: обосновывать организационно-технические мероприятия по защите информации в ИС Владеть: навыками организации работ по обеспечению информационной безопасности на предприятиях ОПК-5; ПК-5
2.	Защищенная информационная система. Уровни и структура ИБ	Тема 4. Виды защищаемой информации. Модель угроз и модель информационной безопасности Тема 5. Понятие защищенной информационной системы. Программа информационной безопасности Тема 6. Организационно-распорядительные документы в сфере информационной безопасности. Политика информационной безопасности	Знать: Виды защищаемой информации Уметь: составлять программу информационной безопасности Владеть: способностью работы со средствами защиты информации ОПК-5; ПК-5
3.	Модели и стандарты в сфере ИБ и управления рисками ИБ	Тема 7. Управление информационными рисками Тема 8. Стандартизация в сфере информационной безопасности	Знать: модели и стандарты в сфере ИБ и управления рисками ИБ Уметь: выявлять угрозы информационной безопасности

		Тема 9. Математические модели систем и процессов защиты информации. Сервисы ИБ и защита от инсайдеров	Владеть: анализом и выбирать методы и средства обеспечения информационной безопасности ОПК-5; ПК-5
4.	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	Тема 10. Криптографические методы защиты информации Тема 11. Защита информационной инфраструктуры от атак. Антивирусные средства защиты Тема 12. Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ	Знать: методы и средства обеспечения информационной безопасности Уметь: обосновывать организационно-технические мероприятия по защите информации в ИС Владеть: способностью работы со средствами защиты информации ОПК-5; ПК-5

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО 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

№ п/п	Разделы Темы	Образовательные технологии
1.	Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия	Интерактивная лекция с использованием мультимедиа Участие в вебинаре Использование электронного учебника, электронной библиотеки возможностей сети Интернет
2	Защищенная информационная система. Уровни и структура ИБ	Интерактивная лекция с использованием мультимедиа. Проведение практической работы с использованием системы Moodle. Использование электронного учебника, электронной библиотеки, возможностей сети Интернет. Участие в вебинаре.
3	Модели и стандарты в сфере ИБ и управления рисками ИБ	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
(очная/заочная/очно-заочная форма обучения)

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы	Часы	Компетенции
1	Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия	Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности. [1] из п. 7.3	9/12/12	ОПК-5; ПК-5
2	Защищенная информационная система. Уровни и структура ИБ	Организационно-распорядительные документы в сфере информационной безопасности. [1] из п. 7.3	9/12/12	ОПК-5; ПК-5
3	Модели и стандарты в сфере ИБ и управления рисками ИБ	Стандартизация в сфере информационной безопасности. [1] из п. 7.3	9/12/12	ОПК-5; ПК-5
4	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ. [1] из п. 7.3.	9/12/12	ОПК-5; ПК-5

7. Учебно-методическое и информационное обеспечение дисциплины:

7.1. Список основной и дополнительной литературы

а) основная литература

1. Мельников Д. А. Информационная безопасность открытых систем [Электронный ресурс]: учебник. – М.: Флинта, 2019. – 444 с. – Режим доступа: http://znanium.com.

2. Партыка Т. Л. Информационная безопасность [Электронный ресурс]: учебное пособие / Т. Л. Партыка, И. И. Попов. – М.: ФОРУМ. 2020. – 432 с. – Режим доступа: http://znanium.com.

б) дополнительная литература

3. Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е. К. Баранова, А. В. Бабаш. – М.: ИЦ РИОР, 2020. – 336 с. – Режим доступа: http://znanium.com.
4. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]:учебное пособие. – М.: ИНФРА-М, 2021. – 118 с. – Режим доступа: http://znanium.com.

7.2. Базы данных, информационно-справочные и поисковые системы

Лицензионные ресурсы:

1. КонсультантПлюс [Электронный ресурс]: Справочная правовая система. - Режим доступа: http://www.consultant.ru/.
2. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/.
3. Электронно-библиотечная система Библиоклуб [Электронный ресурс]. - Режим доступа: http://biblioclub.ru/.
4. Электронная библиотечная система IPR books [Электронный ресурс]. - Режим доступа: https://www.iprbookshop.ru/.

Открытые Интернет-источники:

http://www.lib.ru/

Библиотека Максима Мошкова.

Крупнейшая бесплатная электронная библиотека российского Интернета. Библиотека постоянно пополняется.

http://elibrary.ru/defaultx.asp

«eLibrary.ru». Российская электронная библиотека. Полные тексты зарубежной и отечественной научных периодических изданий

http://www.gumer.info/

Библиотека Гумер - гуманитарные науки. Коллекция книг по социальным и гуманитарным и наукам: истории, культурологии, философии, политологии, литературоведению, языкознанию, журналистике, психологии, педагогике, праву, экономике и т.д.

http://www.rsl.ru/

Российская государственная библиотека. Собрание электронных копий ценных и наиболее спрашиваемых печатных изданий и электронных документов из фондов РГБ и других источников. Электронная библиотека состоит из четырех коллекций, включает 400 тыс. документов и постоянно пополняется.

http://www.public.ru/

«Публичная Библиотека». Интернет-библиотека СМИ. Полные тексты периодических изданий на русском языке (традиционные и электронные СМИ, новостные ленты, блоги).

http://www.encyclopedia.ru/
«Мир энциклопедий». Сайт с крупнейшей подборкой самых разнообразных энциклопедий.

http://www.csrjournal.com/liveexperience/socreports/
Каталог нефинансовой отчетности «Журнала корпоративной социальной ответственности».

www.iso.org
Международная организация по стандартизации.

http://www.iblfrussia.org
Международный форум лидеров бизнеса.

http://www. http://www.gost.ru/
Федеральное агентство по техническому регулированию и метрологии.

www.amr.ru
Ассоциация менеджеров России.

http://www.csr-rspp.ru/
Комитет Российского союза промышленников и предпринимателей.

http://www.knigafund.ru/
Электронно-библиотечная система «КнигаФонд»

http://www.ebdb.ru/
«eBdb». Поисковая система по фондам электронных библиотек. С помощью этого сервиса можно искать книги в электронных библиотеках Интернета - объем базы данных свыше 2 млн. изданий.

http://bukinist.agava.ru
"Букинист". Поисковая система предназначена для поиска книг и других электронных текстов, имеющихся в свободном доступе в Интернет.

http://www.poiskknig.ru/
Поиск электронных книг. Возможность поиска электронных книг. В базе данных более 67000 записей.

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

Темы	Вопросы для самостоятельного изучения
Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия	1.Подготовка предварительного варианта концепции информационной безопасности компании. 2.Построение структуры нормативно-правовых

	документов деятельности компании на базе российского законодательства в сфере информационного права
Защищенная информационная система. Уровни и структура ИБ	1.Разработка параметров защищенности программных и информационных систем компании и программы ИБ 2.Описание структуры информационных рисков, построение модели процесса оценки рисков, составление списка мероприятий для уменьшения рисков. 3.Обзор программных продуктов для оценки информационных рисков.
Модели и стандарты в сфере ИБ и управления рисками ИБ	1.Разработка модели общей и частных политик информационной безопасности компании. 2.Подготовка нормативного документа для введения в действия политики ИБ 3.Формирование опорной системы стандартов для реализации информационной безопасности предприятия. 4.Подготовка описания охраняемой информации, «портрета» нарушителя, модели угроз, построение модели информационной безопасности
Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	1. Подготовка базовой совокупности сервисов информационной защиты. Выбор и внедрение средств криптографической защиты информации. 2. Формирование программно-аппаратных и технических средств защиты информационных ресурсов от внешних атак и вирусной опасности. Построение комплексной системы информационной защиты.

7.5. Вопросы для подготовки к зачету

1. Методы защиты информации
2. К криптографическим механизмам защиты информации
3. В мерах защиты информации, что такое «Управление доступом».
4. Архивация данных
5. Опознавание в диалоговом режиме
6. Какие действия относятся к прослушиванию каналов
7. Назовите неформальным методам защиты информации
8. В инженерно-технических средствах защиты что относится к структурному скрытию информации
9. Перечислите уровни защиты данных в сети
10. Чем обусловлены особенности защиты информации в вычислительных сетях
11. Модель «песочница» в Java-технологии
12. Что относится к сервису безопасности протоколирование/аудит
13. Где должен присутствовать сервис активного аудита
14. Куда целесообразно выносить криптографические средства
15. Перечислите, что включает в себя активный аудит
16. Опишите методы доступа пользователя с различными уровнями, если информация имеет уровень доступа «не секретно».
17. Что относится к проблемам информационной безопасности

18. Какой уровень доступа должен иметь пользователь и файл, для того чтобы пользователь мог записывать информацию в файл

19. Что такое система грифования документов

20.Отличительные особенности компьютерных вирусов

21. Что такое Спам

7.6. Вопросы для подготовки к экзамену

1. Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности

2. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности

3. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности

4. Виды защищаемой информации. Модель угроз и модель информационной безопасности

5. Понятие защищенной информационной системы. Программа информационной безопасности

6. Организационно-распорядительные документы в сфере информационной безопасности. Политика информационной безопасности

7. Управление информационными рисками

8. Стандартизация в сфере информационной безопасности

9. Математические модели систем и процессов защиты информации. Сервисы ИБ и защита от инсайдеров

10. Криптографические методы защиты информации

11. Защита информационной инфраструктуры от атак. Антивирусные средства защиты

12. Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ

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

Темы курсовых и контрольных работ, рефератов, курсовых проектов

Не предусмотрено учебным планом.

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.

8.1. Методические рекомендации для преподавателя

Преподавание дисциплины «Защита информации» базируется на компетентном, 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. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения.

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;

- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;

- в форме электронного документа;

- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;

- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;

- в форме электронного документа;

- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

- устройством для сканирования и чтения с камерой SARA CE;

- дисплеем Брайля PAC Mate 20;

- принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

- акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемыми эргономическими партами СИ-1;

- компьютерной техникой со специальным программным обеспечением.

11. Согласование и утверждение рабочей программы дисциплины

Лист согласования рабочей программы дисциплины

Рабочая программа учебной дисциплины «Защита информации» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.03.01 «Экономика» (утвержденным Приказом № 954 от 12.08.2020г.), учебным планом института по тому же направлению (утвержденным ученым советом «23» декабря 2020г.).

Автор программы - Боброва Л.В., к.т.н.
(Ф.И.О., учёная степень, учёное звание, должность)

_____ _____
Дата Подпись

Рабочая программа рассмотрена и утверждена на заседании кафедры математических и естественно-научных дисциплин (протокол №10/18 от 06.03.2021г.).

Зав. кафедрой _____ Боброва Л.В.
(подпись) (ФИО)

Декан _____ Пресс И.А.
(подпись) (ФИО)

СОГЛАСОВАНО

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