МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____/ Шубаева В.Г./
«18» 06 20 19 г.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ КАЧЕСТВОМ И ЗАЩИТА ИНФОРМАЦИИ

Рабочая программа дисциплины

Направление подготовки	27.03.02 Управление качеством
Направленность (профиль) программы	Управление качеством в бизнес-системах
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составители:
_____ / д.э.н., профессор Стельмашонок Е.В.
_____ / к.э.н., доцент Соколовская С.А.

Санкт-Петербург
2019

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ 3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ 3
4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ 3
5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ 4
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА 6
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 7
7.1. Методические указания для обучающегося по освоению дисциплины 7
7.2. Организация самостоятельной работы 7
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 8
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 9
9.1 Учебно-методическое и информационное обеспечение дисциплины 9
9.2. Материально-техническое обеспечение учебного процесса 10
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 10
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: дать студентам необходимые знания, умения и навыки в области современных информационных технологий, применяемых в настоящее время в управлении качеством, а также защиты информации

Задачи:

- приобретение прикладных знаний в области использования методов и средств моделирования при исследовании сложных процессов и систем;
- овладение навыками самостоятельного использования инструментальных программных средств моделирования систем.
- формирование умения использования современных программных средств защиты информации;
- выработка практических навыков работы пользователя для защиты данных в операционной среде;
- закрепление полученных знаний по обработке и защите информации в среде пакетов прикладных программ универсального назначения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В. «Информационные технологии в управлении качеством и защита информации» относится к вариативной части Блока 1, является обязательной для освоения обучающимся после выбора обучающимся направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы представлены в таблице 3.1.

Таблица 3.1 – Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
1	2	3
ПК-6: способностью использовать знания о принципах принятия решений в условиях неопределенности, о принципах оптимизации	Первый уровень (пороговый) (ПК-6)-1	Декомпозиция II Уметь: использовать современные программные средства защиты информации в условиях неопределенности У1(II) (ПК-6) Владеть: навыками самостоятельного использования инструментальных программных средств моделирования систем и защиты информации в условиях неопределенности В1(II) (ПК-6)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов, из которых 72 часа самостоятельной работы обучающегося отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: экзамен - 6 семестр, экзамен – 7 семестр.

Распределение фонда времени по темам дисциплины по очной форме обучения представлено в таблице 4.1

Таблица 4.1 – Распределение фонда времени по темам дисциплины (очная форма обучения)

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	2	3	4	5
Тема.1. Составляющие национальных интересов Российской Федерации в информационной сфере				5
Тема.2. Понятие, сущность и актуальность защиты информации				5
Тема.3. Риски и угрозы информационной безопасности				5
Тема.4. Правовое обеспечение информационной безопасности				5
Тема.5. Антивирусная защита				5
Тема.6. Системы идентификации и аутентификации		4		5
Тема 7. Системы разграничения доступа		4		5
Тема.8. Стеганографические методы		12		6
Тема.9. Криптографические методы		12		6
Тема.10. Технология электронной подписи		8		6
Тема.11. Методы защиты в операционных системах		8		7
Всего за 6 семестр		**48**		**60**
Тема 12. Основные понятия и характеристика методов моделирования процессов и систем				11
Тема.13. Структурные технологии моделирования процессов и систем управления качеством		12		12
Тема.14. Объектно-ориентированные технологии моделирования процессов и систем управления качеством		12		12
Тема.15. Имитационные технологии моделирования процессов и систем управления качеством		12		12
Тема.16. Интегрированные технологии моделирования процессов и систем управления качеством		12		13
Всего за 7 семестр		**48**		**60**
Всего по дисциплине		**96**		**120**

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Тема 1. Составляющие национальных интересов Российской Федерации в информационной сфере

Понятие и современная концепция национальной безопасности. Теоретические основы национальной политики в сфере защиты информации. Место информационной безопасности в системе национальной безопасности. Задачи в области обеспечения информационной безопасности Российской Федерации. Реализация Стратегии национальной безопасности Российской Федерации до 2020. Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Особенности обеспечения

информационной безопасности в различных сферах общественной жизни. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Понятия информационной войны и информационного оружия. Проблема общемирового противодействия угрозам информационной безопасности.

Тема 2. Понятие, сущность и актуальность защиты информации

Существующие подходы к содержательной части понятия «защита информации». Методологическая основа раскрытия сущности и определения понятия защиты информации. Цели защиты информации. Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации. Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации. Проблема информационной безопасности предприятия. Причины актуальности и важности проблемы обеспечения информационной безопасности.

Тема 3. Риски и угрозы информационной безопасности

Понятие угрозы информационной безопасности. Основные виды и источники угроз информационной безопасности. Внутренние и внешние угрозы. Понятие уязвимости информационной системы, атаки на систему. Понятие риска. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Политика безопасности. Информационные риски. Управление рисками. Качественный и количественный анализ риска. Методики оценки рисков. Модель оценки рисков. Экономические последствия атак на информацию. Структура ущерба предприятия от реализации угроз информационной безопасности.

Тема 4. Правовое обеспечение информационной безопасности

Правовые меры защиты информации. Государственное регулирование в сфере информационной безопасности. Правовые режимы доступа к информации. Виды тайн. Персональные данные. Государственные регулирующие органы РФ. Компьютерные преступления.

Тема 5. Антивирусная защита

Вредоносное программное обеспечение. Классификация вредоносных программ. Понятие компьютерного вируса. Троянские программы. Основные типы компьютерных вирусов. Основные классы вредоносных программ по характеру воздействия на компьютерную систему. Основные тенденции развития вирусных технологий. Возможные последствия вирусных атак. Методы и средства антивирусной защиты.

Тема 6. Системы идентификации и аутентификации

Системы идентификации и аутентификации: основные определения, типы, область применения, классификация. Парольная защита. Общие подходы к построению парольных систем. Выбор паролей. Методы взлома паролей. Методы выбора паролей.

Тема 7. Системы разграничения доступа

Дискреционное и мандатное управление доступом. Уровни доступа. Ролевое управление доступом. Двухуровневое назначение прав доступа.

Тема 8. Стеганографические методы

Исторические методы стеганографии. Цифровая стеганография. Определения и методы цифровой стеганографии. Стегосистема. Области применения компьютерной стеганографии.

Тема 9. Криптографические методы

Основы современной криптографии. Понятия и определения современной криптографии. Стойкость шифра. Стойкость алгоритмов шифрования. Классификация криптоаналитических атак. Классификация криптографических алгоритмов. Исторические шифры. Требования, предъявляемые к современным алгоритмам шифрования. Симметричные алгоритмы шифрования. Алгоритмы шифрования с открытым ключом.

Тема 10. Технология электронной цифровой подписи

Алгоритмы электронной цифровой подписи. Хеширование. Типы криптографических хеш-функций. Защищенная цифровая подпись. Цифровые сертификаты.

Тема 11. Методы защиты в операционных системах

Защищенные информационные системы. Оценка безопасности операционной системы. Структура операционной системы. Инструменты настройки безопасности ОС Windows. Аутентификация пользователей Windows. Защищенная файловая система NTFS. Средства шифрования ОС Windows. Безопасное уничтожение данных. Методы защиты системных файлов в Windows. Защита работы пользователей в сети Windows.

Защита офисных документов. Технологии защиты баз данных.

Тема 12. Основные понятия и характеристика методов моделирования процессов и систем

Понятие модели. Цели, задачи и принципы моделирования. Классификация моделей. Общий порядок разработки моделей. Компьютерные технологии моделирования.

Тема 13. Структурные технологии моделирования процессов и систем управления качеством

Концепция структурного моделирования в управлении качеством. Программные средства структурного моделирования, их возможности и особенности использования.

Тема 14. Объектно-ориентированные технологии моделирования процессов и систем управления качеством

Концепция объектно-ориентированного моделирования в управлении качеством. Программные средства объектно-ориентированного моделирования, их возможности и особенности использования.

Тема 15. Имитационные технологии моделирования процессов и систем управления качеством

Концепция имитационного моделирования в управлении качеством. Программные средства имитационного моделирования, их возможности и особенности использования.

Тема 16. Интегрированные технологии моделирования процессов и систем управления качеством

Концепция интеграции технологий в управлении качеством. Интегрированные программные средства моделирования, их возможности и особенности использования.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия / Семинарские занятия / Лабораторные работы

№ темы	Тема занятия	Вид занятия / Оценочное средство
1	2	3
6,7	Создание учетных записей пользователей, шифрование и управление доступом к файлам и папкам на локальном компьютере	ПЗ: Решение практических задач
8	Изучение методов цифровой стеганографии	ПЗ: Решение практических задач
9	Изучение криптографических методов	ПЗ: Решение практических задач
10	Использование цифровой подписи проектов VBA	ПЗ: Решение практических задач,
11	Изучение средств защиты от несанкционированного доступа на примере программного обеспечения MS Office	ПЗ: Решение практических задач,

13	Изучение структурного средства Business Studio для моделирования бизнес-процессов	ПЗ: Решение практических задач,
14	Изучение объектно-ориентированного средства IBM Rational Rose для моделирования бизнес-процессов	ПЗ: Решение практических задач
15	Изучение средства имитационного моделирования ARENA для моделирования бизнес-процессов	ПЗ: Решение практических задач
16	Изучение интегрированного программного средства ARIS для моделирования бизнес-процессов	ПЗ: Решение практических задач,

* ПЗ – практические занятия, СЗ – семинарские занятия, ЛР – лабораторные работы

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1. Методические указания для обучающегося по освоению дисциплины

Для формирования четкого представления об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине в самом начале учебного курса обучающийся должен ознакомиться с учебно-методической документацией:

– рабочей программой дисциплины: с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, перечнем знаний и умений, которыми в процессе освоения дисциплины должен владеть обучающийся,

– порядком проведения текущего контроля успеваемости и промежуточной аттестации;

– графиком консультаций преподавателей кафедры.

Систематическое выполнение учебной работы на занятиях лекционных и семинарских типов, а также выполнение самостоятельной работы позволит успешно освоить дисциплину.

В процессе освоения дисциплины обучающимся следует:

– слушать, конспектировать излагаемый преподавателем материал;

– ставить, обсуждать актуальные проблемы курса, быть активным на занятиях;

– задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений;

– выполнять задания практических занятий полностью и установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратится к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

Обучающимся, пропустившим занятия (независимо от причин), не имеющим письменного решения задач или не подготовившимся к данному занятию, рекомендуется не позже чем в 2 - недельный срок явиться на консультацию к преподавателю и отчитаться по теме.

7.2. Организация самостоятельной работы

Под самостоятельной работой обучающихся понимается планируемая работа обучающихся, направленная на формирование указанных компетенций, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, без его непосредственного участия.

Методическое обеспечение самостоятельной работы при наличии обучающихся лиц с ограниченными возможностями представляется в формах, адаптированных к

ограничениям их здоровья.

Виды самостоятельной работы по дисциплине представлены в таблице 7.2.1.

Таблица 7.2.1 – Организация самостоятельной работы обучающегося

№ темы	Вид самостоятельной работы
1	2
1	Подготовка к опросу по теме
2	Подготовка к опросу по теме
3	Подготовка к опросу по теме
4	Подготовка к опросу по теме
5	Подготовка к опросу по теме
6	Подготовка к опросу по теме. Подготовка к выполнению и защите индивидуального задания 1
7	Подготовка к опросу по теме
8	Подготовка к опросу по теме. Подготовка к выполнению и защите индивидуального задания 2
9	Подготовка к опросу по теме
10	Подготовка к опросу по теме.
11	Подготовка к опросу по теме.
1-11	Подготовка к экзамену.
12	Подготовка к опросу по теме
13	Подготовка к опросу по теме. Подготовка к выполнению и защите индивидуального задания 3
14	Подготовка к опросу по теме. Подготовка к выполнению и защите индивидуального задания 4
15	Подготовка к опросу по теме
16	Подготовка к опросу по теме.
12-16	Подготовка к экзамену

Каждый вид СРО, указанный в таблице 7.2.1 обеспечен методическими материалами.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «Информационные технологии в управлении качеством и защита информации» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

К интерактивным методам обучения относится выполнение индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 6,7,8,9,10,11, 13,14,15,16.

Выполнение индивидуальных заданий на ПК предполагает выполнение индивидуальных заданий по изучению пакетов прикладных программ, языков программирования, информационно-коммуникационных технологий (как правило, организационной формой таких занятий являются практические занятия в компьютерных классах).

9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1 Учебно-методическое и информационное обеспечение дисциплины

Таблица 9.1.1 – Учебно-методическое обеспечение дисциплины

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	**Основная/ дополнительная литература**	**Книгообеспеченность**	
		Кол-во экз. в библ. СПбГЭУ	**Электронные ресурсы**
Васильева И.Н: Информационные технологии и защита информации: учебное пособие/ И.Н. Васильева, Е.В. Стельмашонок.— Санкт-Петербург: СПбГИЭУ, 2011.— 271 с. – Сведения доступны также по Интернету: opac.unecon.ru.	основная	71	ЭБ OPAC.UNECON.RU
Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В.Сухостат, И.Н.Васильева .— Санкт-Петербург : Изд-во СПбГЭУ, 2019 .— 103 с. – Сведения доступны также по Интернету: opac.unecon.ru .	основная	35	ЭБ OPAC.UNECON.RU
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . — Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2020. — 592 с.	основная	–	ЭБС ZNANIUM
Тарзанов В.В. Информационные технологии в управлении качеством и защита информации : учебное пособие. Ч. 1 / В.В. Тарзанов, М. А. Шапченко. — Санкт-Петербург : СПбГИЭУ, 2011 .— 186 с. – Сведения доступны также по Интернету: opac.unecon.ru.	дополнительная	71	ЭБ OPAC.UNECON.RU
Обработка и обеспечение безопасности электронных данных .: учебное пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев [и др.]. — Электрон. дан.— Москва: МФПУ «Синергия», 2012.— 592 с	дополнительная	–	ЭБС Айбукс

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
1	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2	Научная электронная библиотека eLIBRARRY – www.elibrary.ru
3	Научная электронная библиотека КиберЛеника – www.cyberleninka.ru
4	База данных ПОЛПРЕД Справочники – www.polpred.com
5	База данных OECD Books, Papers & Statistics на платформе OECD iLibrary – www.oecd-ilibrary.org

Таблица 9.1.3 – Перечень информационных справочных систем (ИСС)

№	Наименование ИСС
1	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
2	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
3	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
4	Электронная библиотечная система BOOK.ru - www.book.ru
5	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
6	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
7	Электронная библиотека СПбГЭУ– opac.unecon.ru

9.2. Материально-техническое обеспечение учебного процесса

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Таблица 9.2.1 – Перечень программного обеспечения (ПО)

№	Наименование ПО
1	Microsoft Windows Professional (КОНТРАКТ № 244/20 «26» июня 2020 г)
2	Microsoft Office Professional (КОНТРАКТ № 244/20 «26» июня 2020 г)
3	7-Zip (freeware)

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

– для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

– для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом и является приложением к рабочей программе дисциплины (модуля).