Частное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ И ЭКОНОМИКИ»

РАССМОТРЕНО И ОДОБРЕНО

На заседании кафедры информационных технологий и математики
Протокол № _9_ от _25.05.2023

УТВЕРЖДАЮ

Первый проректор
Авдашкевич С.В.
28.06.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина:	Б1.Б.14 Информационная безопасность и защита информации
Направление подготовки:	46.03.02 Документоведение и архивоведение"
Направленность (профиль):	«Документоведение и документационное обеспечение управления»
Уровень высшего образования:	бакалавриат
Программа:	Прикладного бакалавриата
Форма обучения:	заочная
Разработчики:	Кандидат экономических наук, доцент Удахина С.В.

Санкт-Петербург
2023

1. Цели и задачи дисциплины:

Цель дисциплины: формирование у студентов методически правильных основ знаний и практических навыков по основам информационной безопасности (ИБ), необходимых выпускникам университета, занимающимся эксплуатацией корпоративных информационных систем. Дисциплина является важной составной частью теоретической подготовки бакалавра и занимает существенное место в его будущей практической деятельности.

Задачи дисциплины:

- получение студентами необходимых для их работы теоретических знаний о современных средствах, методах и технологиях обеспечения информационной безопасности корпоративных информационных систем;
- формирование у студентов практических навыков организации работ по обеспечению основ информационной безопасности и защиты информации на предприятиях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы высшего образования

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Содержание компетенции
ОПК-6	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-17	владением методами защиты информации

Планируемые результаты обучения:

Код компетенции	Основные признаки освоения		
	Знать	**Уметь**	**Владеть**
ОПК-6	основные угрозы и методы обеспечения информационной безопасности; основные методики, направленные на обеспечение информационной безопасности на различных направлениях деятельности современного предприятия; перспективы развития технологий обеспечения информационной безопасности.	анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ; ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности; формулировать задачи по обеспечению ИБ, исходя из поставленных целей.	Владеть: навыками анализа информационной безопасности; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности; приемами анализа степени выполнения задач по обеспечению информационной безопасности.
ПК-17	основные угрозы и методы обеспечения информационной безопасности; основные методики, направленные на обеспечение информационной безопасности на различных направлениях деятельности современного предприятия;	анализировать и выбирать адекватные методы информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ; ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности;	навыками анализа информационной безопасности; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности; приемами анализа степени выполнения задач по обеспечению информационной безопасности.

3. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» входит в Блок 1 «Дисциплины (модуля)» (Базовая часть) образовательной программы высшего образования по направлению 46.03.02 Документоведение и архивоведение направленность (профиль) «Документоведение и документационное обеспечение управления».

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые формируются в процессе изучения следующих дисциплин (практик):

Основы информационной культуры

Знания, умения и навыки, приобретенные в процессе изучения данной дисциплины, будут использованы обучающимся при изучении дисциплин (практик):

Информационные технологии, Конфиденциальное делопроизводство, Производственная практика: технологическая практика, Производственная практика: преддипломная практика

4. Объем дисциплины

Заочная форма обучения:

Вид учебной работы	Всего часов	Курс
		3
Аудиторные занятия (АЗ):	14	14
В том числе:		
Лекционные занятия (Лек)	4	4
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	10	10
Самостоятельная работа студента (СР)	152	152
В том числе:		
Курсовая работа	0	0
Другие виды самостоятельной работы*	152	152
Контроль самостоятельной работы (КСР)	5	5
Контактная работа (КоР)	19	19
Форма промежуточной аттестации		Экзамен
Подготовка к экзамену/зачету и сдача экзамена/зачета (СР, КоР)	9	9
Общая трудоемкость дисциплины, часы/ЗЕТ	180/5	180/5

* - подготовка к аудиторным занятиям.

5. Содержание дисциплины

Заочная форма обучения:

№ п/п	Наименование темы дисциплины	Курс	Количество учебных часов				
			В том числе по видам аудиторных занятий			СР	Практическая подготовка*
			Лек	Пр	Лаб		
1	Основные направления формирования информационной безопасности современного предприятия.	3	2	2	0	38	8
2	Защищенная информационная система. Уровни и структура информационной безопасности.	3	0	2	0	38	8
3	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.	3	2	2	0	38	8
4	Технологии и методы обеспечения информационной безопасности. Комплексная защита информационных систем.	3	0	4	0	38	12
	Итого:		4	10	0	152	36

* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и (или) путем выделения часов из часов, отведенных на самостоятельную работу, и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

Наименование разделов и тем	**Содержание учебного материала, лабораторные работы и практические занятия обучающихся, курсовая работа**	**Компетенции**	**Оценочное средство текущего контроля**
1	**2**	**3**	**4**
Тема 1: Основные направления формирования информационной безопасности современного предприятия	Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности. **Практические занятия/Самостоятельная работа:** Основные вопросы информационной безопасности. Международное законодательство в сфере информационной безопасности. Корпоративная концепция информационной безопасности. **Лабораторная работа:** -	ОПК-6 ПК-17	Тестирование №1; Доклад №1
Тема 2: Защищенная информационная система. Уровни и структура информационной безопасности.	Виды защищаемой информации. Модель угроз и модель информационной безопасности. Понятие защищенной информационной системы. Программа информационной безопасности. Организационно-распорядительные документы в сфере информационной безопасности. -Политика информационной безопасности. **Практические занятия/Самостоятельная работа:** Модели угроз и информационной безопасности. Программа и политика информационной безопасности на международном рынке. **Лабораторная работа:** -	ОПК-6 ПК-17	Тестирование №1; Коллоквиум №1
Тема 3: Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.	Управление информационными рисками. Стандартизация в сфере информационной безопасности. **Практические занятия/Самостоятельная работа:** Управление информационными рисками в области международных финансов. **Лабораторная работа:** -	ОПК-6 ПК-17	Тестирование №1; Коллоквиум №2
Тема 4: Технологии и методы обеспечения информационной безопасности. Комплексная защита информационных систем.	Защита информационной инфраструктуры от атак. Антивирусные средства защиты. Оценка эффективности средств защиты информации **Практические занятия/Самостоятельная работа:** Антивирусные средства защиты информационной безопасности. Комплексная защита информационной инфраструктуры и ресурсов в сфере международных финансов. **Лабораторная работа:** -	ОПК-6 ПК-17	Контрольная работа №1
Курсовая работа	Не предусмотрено учебным планом		

6. Формы проведения занятий

При реализации дисциплины применяются инновационные формы учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, принятия решений, лидерские качества.

Заочная форма обучения:

№ п/п	Наименование темы/ лекционного (практического) занятия	Тип занятия	Кол-во часов	Форма проведения занятий
1	Защищенная информационная система. Уровни и структура информационной безопасности: Модели угроз и информационной безопасности. Программа и политика информационной безопасности на международном рынке.	Пр	2	Дискуссия
2	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности: Управление информационными рисками в области международных финансов.	Пр	2	Ролевая игра

7. Способ реализации дисциплины

Без использования онлайн-курса

8. Учебно-методическое обеспечение дисциплины:

Основная литература:

Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2023. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519780

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495922

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998

Дополнительная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844

3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520063

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения

1. Операционная система
2. Пакет прикладных офисных программ
3. Антивирусное программное обеспечение
4. Oracle VM Virtualbox

Дополнительно при применении электронного обучения, дистанционных образовательных технологий используются:

1. LMS Moodle
2. Вебинарная платформа

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», информационных справочных систем и профессиональных баз данных, необходимых для освоения дисциплины

1. ibooks.ru : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://ibooks.ru. - Текст: электронный
2. Электронно-библиотечная система СПбУТУиЭ : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: http://libume.ru. - Текст: электронный
3. Юрайт : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://urait.ru. - Текст: электронный
4. eLibrary.ru : научная электронная библиотека [Электронный ресурс] : профессиональная база данных. - Режим доступа: http://elibrary.ru. - Текст: электронный
5. Архив научных журналов НЭИКОН [Электронный ресурс] : профессиональная база данных. - Режим доступа: arch.neicon.ru. - Текст: электронный
6. КиберЛенинка : научная электронная библиотека [Электронный ресурс] : информационная справочная система. - Режим доступа: http://cyberleninka.ru. - Текст: электронный
7. Лань : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://e.lanbook.com. - Текст: электронный
8. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://rkn.gov.ru/. - Текст: электронный
9. it-world.ru [Электронный ресурс] : информационная справочная система. - Режим доступа: https://www.it-world.ru/. - Текст: электронный
10. Бизнес-информатика [Электронный ресурс] : информационная справочная система. - Режим доступа: https://bijournal.hse.ru/. - Текст: электронный

11. Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа - практических занятий, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованные: рабочими местами для обучающихся, оснащенными специальной мебелью; рабочим местом преподавателя, оснащенного специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской.

Учебная аудитория для проведения занятий семинарского типа - практических занятий – компьютерный класс, оборудованный рабочими местами для обучающихся, оснащенными спе-

циальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; рабочим местом преподавателя, оснащенного специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской.

Помещение для самостоятельной работы, оборудованное специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением.

При применении электронного обучения, дистанционных образовательных технологий используются: виртуальные аналоги учебных аудиторий - вебинарные комнаты на вебинарных платформах, рабочее место преподавателя, оснащенное персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному порталу Университета umeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройствами), программным обеспечением; рабочее место обучающегося оснащено персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному порталу Университета umeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройства), программным обеспечением. Авторизация на информационно-образовательном портале Университета umeos.ru и начало работы осуществляются с использованием персональной учетной записи (логина и пароля).

12. Оценочные материалы по дисциплине

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Заочная форма обучения:

Код компетенции	Название дисциплины	Форма промежуточной аттестации	Семестр/курс	Этап формирования компетенции
ОПК-6	Основы информационной культуры	экзамен	1	1
ОПК-6	Информационная безопасность и защита информации	экзамен	3	2
ОПК-6	Информационные технологии	экзамен	4	3
ПК-17	Информационная безопасность и защита информации	экзамен	3	1
ПК-17	Конфиденциальное делопроизводство	экзамен	4	2
ПК-17	Производственная практика: технологическая практика	зачет с оценкой	5	3
ПК-17	Производственная практика: преддипломная практика	зачет с оценкой	5	3

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования в процессе изучения дисциплины, описание шкал оценивания

2.1 Текущий контроль

ТЕСТИРОВАНИЕ

Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Выполнение теста оценивается по следующим показателям:

- Правильность выполнения заданий теста за отведенный промежуток времени.

Критерии и шкала оценивания теста

Выполнение заданий теста оценивается по единой схеме, основанной на вычислении коэффициента результативности (КР) учебных достижений. Для этого подсчитывается количество правильных ответов к заданиям теста (А), при этом каждое тестовое задание оценивается в бинарной шкале «правильно – не правильно». Далее фиксируется максимальное количество заданий данного теста (Amax).

Величина коэффициента результативности учебных достижений студентов в рамках тестирования вычисляется по следующей формуле: КР = А / Amax **(**значения КР изменяются в пределах от 0 до 1**).**

Коэффициент результативности (КР)	КР <0,4	0,4 ≤ КР <0,6	0,6 ≤ КР ≤ 0,8	0,8<КР≤ 1
Баллы в БРС университета	0	6	8	10
Уровень сформированности компетенций	Не сформирована	Пороговый	Высокий	Повышенный

КОНТРОЛЬНАЯ РАБОТА

Самостоятельная письменная аналитическая работа студента, которая способствует закреплению и систематизации знаний по одной или нескольким темам дисциплины. Цель контрольной работы – получить специальные знания и продемонстрировать навыки их практического применения.

Контрольная работа оценивается по следующим показателям:

1. Выполнение работы в полном объеме и без ошибок;
2. Зрелая, творческая, полностью самостоятельная работа;
3. Выполнение работы в соответствии с требованиями к оформлению.

Критерии оценивания контрольной работы

Полное, правильное и обоснованное решение; полностью самостоятельная работа; работа выполнена в соответствии с требованиями к оформлению	10 баллов
Решение в целом правильное и обоснованное, но допущены незначительные ошибки либо решение является неполным, допускается незначительная подсказка со стороны преподавателя; работа выполнена в соответствии с требованиями к оформлению	8 баллов
Решение содержит обоснование, ход рассуждений в целом верный, но при этом допущены существенные ошибки, студент продемонстрировал недостаточное умение правильно применять знания, полученные в процессе изучения дисциплины, либо работа выполнена при существенной помощи преподавателя; работа выполнена с некоторыми нарушениями требований к оформлению	6 баллов
Отсутствует решение задачи, либо отсутствует обоснование решения, либо решение содержит обоснование, но допущены грубые ошибки, приведшие к абсолютно неверной квалификации; работа выполнена без учета требований к оформлению	0 баллов

Шкала оценивания контрольной работы

Зависимость баллов и уровня сформированности компетенций на данном этапе изучения дисциплины представлены в следующей таблице:

Баллы в БРС Университета	10	8	6	0
Уровень сформированности компетенции	Повышенный	Высокий	Пороговый	Не сформированы

ДОКЛАД

Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Показатели и критерии оценивания доклада

№ п/п	Показатели оценки	Критерии оценивания
1	**Структура** (количество слайдов соответствует содержанию и продолжительности выступления, например: для 7-минутного выступления рекомендуется использовать не более 10 слайдов, включая титульный слайд и слайд с выводами)	Каждый из предложенных показателей оценивается по критерию **«выполнен - частично выполнен - не выполнен»,** что соответствует следующему распределению баллов **«2 балла - 1 балл - 0 баллов»**
2	**Наглядность** (иллюстрации хорошего качества, с четким изображением, текст легко читается, например: используются средства наглядности информации в виде таблиц, схем, графиков и т. д.)	
3	**Дизайн и настройка** (оформление слайдов соответствует теме, не препятствует восприятию содержания, для всех слайдов презентации используется один и тот же шаблон оформления)	
4	**Содержание** (презентация отражает основные этапы исследования – проблему, цель, гипотезу, ход выполнения работы, выводы, т. е. содержит полную, понятную информацию по теме доклада при наличии орфографической и пунктуационной грамотности)	
5	**Требования к выступлению** (выступающий свободно владеет содержанием, ясно и грамотно излагает материал, выступающий свободно и корректно отвечает на вопросы и замечания аудитории, выступающий точно укладывается в рамки регламента).	

Шкала оценивания доклада

Зависимость баллов и уровня сформированности компетенции на данном этапе изучения дисциплины за доклад представлены в следующей таблице:

Баллы в БРС Университета	10-9	8-7	6-5	Менее 5
Уровень сформированности компетенции	Повышенный	Высокий	Пороговый	Не сформированы

КОЛЛОКВИУМ

Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.

Коллоквиум оценивается по следующим показателям:

1. Глубокое и прочное усвоение программного материала;
2. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания;
3. Владение разносторонними навыками и приемами выполнения практических работ;
4. Владение профессиональной терминологией;
5. Полный конспект лекционных материалов.

Критерии оценивания коллоквиума

Студент полностью раскрыл содержание материала в объеме, предусмотренном программой, изло-	20

жил материал грамотным языком в определенной логической последовательности, точно используя терминологию и символику; продемонстрировал сформированность и устойчивость полученных знаний. Возможны одна-две неточности при ответе на дополнительные вопросы, которые студент легко исправил по замечанию преподавателя.	баллов
Ответ студента имеет один из недостатков: в изложении вопроса допущены небольшие пробелы, не исказившие содержание ответа; допущены один-два недочета при освещении основного содержания ответа, не исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении дополнительных вопросов, легко исправленные по замечанию преподавателя.	15 баллов
Студент неполно раскрыл содержание вопроса, но показал общее понимание материала и продемонстрировал умения, достаточные для дальнейшего усвоения программного материала; имеет затруднения или допустил ошибки в определении понятий, использовании терминологии и исправил их после нескольких наводящих вопросов преподавателя.	10 баллов
Студент обнаружил полное незнание и непонимание изучаемого учебного материала по дисциплине или не смог ответить ни на один из дополнительных вопросов по изучаемому материалу.	0 баллов

Шкала оценивания коллоквиума

Зависимость баллов и уровня сформированности компетенции на данном этапе изучения дисциплины представлены в следующей таблице:

Баллы в БРС Университета	20	15	10	0
Уровень сформированности компетенции	Повышенный	Высокий	Пороговый	Не сформированы

2.2 Курсовая работа

Не предусмотрено учебным планом

2.3 Промежуточная аттестация в форме зачета

Не предусмотрено учебным планом

2.4 Промежуточная аттестация в форме экзамена

Экзамен проводится в форме группового бланкового тестирования (письменный экзамен). Процедура проведения экзамена изложена в «Положении о текущем контроле успеваемости, промежуточной аттестации и балльно-рейтинговой системе оценки учебных достижений студентов».

Выполнение теста оценивается по следующим показателям:

- Правильность выполнения заданий теста за отведенный промежуток времени.

Критерии и шкала оценивания теста

Выполнение заданий теста оценивается по единой схеме, основанной на вычислении коэффициента результативности (КР) учебных достижений. Для этого подсчитывается количество правильных ответов к заданиям теста (А), при этом каждое тестовое задание оценивается в бинарной шкале «правильно – не правильно». Далее фиксируется максимальное количество заданий данного теста (Amax).

Величина коэффициента результативности учебных достижений студентов в рамках тестирования вычисляется по следующей формуле: КР = А / Amax **(**значения КР изменяются в пределах от 0 до 1).

Коэффициент результативности (КР)	КР < 0,4	0,4 ≤ КР < 0,6	0,6 ≤ КР ≤ 0,8	0,8< КР ≤ 1
Уровень сформированности компетенций	Не сформирован	Пороговый	Высокий	Повышенный
Оценка за экзамен	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

2.5 Описание показателей и критериев оценивания компетенций, сформированных дисциплиной

После выполнения студентом всех видов оценочных средств, указанных в рабочей программе дисциплины, производится оценка уровня сформированности компетенций по дисциплине:

Код компетенции	Уровень сформированности компетенции	Основные признаки освоения компетенций		
		Знать	**Уметь**	**Владеть**
ОПК-6	Пороговый	основные понятия и определения, используемые при изучении дисциплины; законодательную и нормативную базу информационной безопасности; иметь представление о значение информационной безопасности для современного предприятия.	анализировать и выбирать адекватные модели информационной безопасности; ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности; оценивать состояние организационной защиты информации.	приемами реализации мероприятий по обеспечению на предприятии (в организации) деятельности в области защиты информации; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.
	Высокий	основные виды и источники угроз информации в компьютерных сетях; основные направления формирования информационной безопасности современного предприятия; модели и стандарты в сфере информационной безопасности; перспективы развития технологий обеспечения информационной безопасности.	классифицировать основные угрозы безопасности информации; анализировать и выбирать адекватные модели информационной безопасности; ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности.	навыками анализа информационной безопасности; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.
	Повышенный	основные угрозы и методы обеспечения информационной безопасности; основные методики, направленные на обеспечение информационной безопасности на различных направлениях деятельности современного предприятия; перспективы развития технологий обеспечения информационной безопасности.	анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ; ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности; формулировать задачи по обеспечению ИБ, исходя из поставленных целей.	Владеть: навыками анализа информационной безопасности; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности; приемами анализа степени выполнения задач по обеспечению информационной безопасности.

ПК-17	Пороговый	основные методы защиты информации законодательную и нормативную базу информационной безопасности; иметь представление о значение информационной безопасности для современного предприятия.	анализировать и выбирать адекватные методы информационной безопасности;	приемами реализации методов по обеспечению на предприятии (в организации) деятельности в области защиты информации;
	Высокий	основные виды и источники угроз информации в компьютерных сетях; основные направления формирования информационной безопасности современного предприятия; модели и стандарты в сфере информационной безопасности;	классифицировать основные угрозы безопасности информации; анализировать и выбирать адекватные методы информационной безопасности;	навыками анализа информационной безопасности; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.
	Повышенный	основные угрозы и методы обеспечения информационной безопасности; основные методики, направленные на обеспечение информационной безопасности на различных направлениях деятельности современного предприятия;	анализировать и выбирать адекватные методы информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ; ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности;	навыками анализа информационной безопасности; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности; приемами анализа степени выполнения задач по обеспечению информационной безопасности.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Методика формирования оценки по дисциплине. Успеваемость студента оценивается в баллах и состоит из:

- суммы баллов за выполнение заданий текущего контроля (обучающийся может получить в сумме не более 70 баллов);
- баллов за посещаемость (не более 10 баллов);
- баллов за активность на занятиях (занятия в интерактивной форме – п. 6. Формы проведения занятий), выполнение дополнительных заданий и пр. по усмотрению преподавателя, ведущего дисциплину – премиальные баллы (не более 20 баллов).

Полученные итоговые баллы по дисциплине переводятся в оценку по традиционной пятибалльной шкале оценивания и по 100-балльной шкале оценок Европейской системы перевода и накопления баллов (ECTS) в соответствии с таблицами, представленными в п. Таблицами. 1, 2. Оценки в пятибалльной шкале выставляются в ведомости и зачетные книжки, в 100-балльной – в ведомости.

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приводятся в соответствующих методических материалах и локальных нормативных актах Университета (Положение «О текущем контроле успеваемости, промежуточной аттестации и балльно-рейтинговой системе оценки учебных достижений студентов», Положение «Об оценочных средствах», Положение «О контроле самостоятельности выполнения письменных работ обучающимися университета с использованием системы «Антиплагиат ВУЗ» и др.).

Уровень сформированности компетенции № 1 (№ N) определяется перечнем оценочных средств:

Оценочное средство *(в том числе экзамен, зачет с оценкой при наличии)*	**Уровень сформированности компетенции***			**Средний уровень сформированности компетенций по каждому оценочному средству**
	Студент №1	**…**	**Студент № N**	
……	…….			
Итоговый уровень:	……			

* *пороговый, высокий или повышенный*

Итоговый (общий/средний) уровень рассчитывается как среднее арифметическое с округлением в сторону более высокого уровня.

Далее делается вывод об общем уровне освоения компетенций студентами в ходе изучения дисциплины:

Оценочный лист по дисциплине

ФИО студента	**Уровень сформированности компетенций**								
	Общекультурные компетенции			**Общепрофессиональные компетенции**			**Компетенции по видам деятельности**		
	№ 1	**№ N**	**Уровень сформированности общекультурных компетенций**	**№ 1**	**№ N**	**Уровень сформированности общепрофессиональных компетенций**	**№ 1**	**№ N**	**Уровень сформированности компетенций по виду деятельности № 1**
Студент № 1									
Студент № 2									
……									

4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Примерные задания для контрольных работ №1 (в форме реферата)

1. Классификация угроз информационной безопасности по базовым признакам.
2. Угрозы нарушения конфиденциальности.
3. Угрозы нарушения целостности данных.
4. Угрозы отказа служб (угрозы отказа в доступе).
5. Понятие политики безопасности информационных систем. Назначение политики безопасности.
6. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
7. Законодательный уровень обеспечения информационной безопасности.
8. Основные законодательные акты РФ в области защиты информации.
9. Асимметричные методы шифрования данных.
10. Основные угрозы безопасности данных и их классификация.
11. Симметричные методы шифрования данных.

12. Каналы утечки данных и их классификация.
13. Идентификация, аутентификация пользователей. Классификация методов идентификации пользователей.
14. Уязвимые места информационных систем.
15. Обеспечение доступности данных.
16. Основные методы защиты данных и их классификация.
17. Защита информации в системах управления базами данных.
18. Основные средства защиты данных и их классификация.
19. Формальные средства защиты информации.
20. Программно-технический аспект информационной безопасности.
21. Неформальные средства защиты информации.
22. Организационный аспект информационной безопасности.
23. Мероприятия по защите информации от несанкционированного доступа.
24. Управленческий аспект информационной безопасности.
25. Мероприятия по защите информации от потерь.
26. Законодательный аспект информационной безопасности.
27. Мероприятия по защите информации от вредоносных программ.
28. Вредоносные программы (вирусы) и их классификация.

Типовые задания для тестирования №1

1) Что входит в понятие “безопасность информации”
   a) исключение ознакомления с информацией сотрудников АСОИ
   b) предотвращение ознакомления с информацией лиц к ней не допущенных
   c) исключение изменений информации
   d) исключение утечки информации за счет излучений и наводок
2) Конфиденциальность информации обеспечивается путем
   a) содержания критической информации в секрете
   b) ограничения доступа в специальные помещения
   c) организации мониторинга сети
3) Информационная безопасность информации достигается обеспечением
   a) конфиденциальности
   b) доступности
   c) комплексирования средств ЗИ
   d) целостности информации
4) Защита целостности потоков данных осуществляется с использованием
   a) дополнительных форм нумерации
   b) меток времени
   c) повтором сообщений
   d) включением дополнительных признаков к сообщению
5) Для обеспечения защиты от анализа трафика могут быть использованы
   a) механизм заполнения текста
   b) генерация фиктивных сообщений
   c) ограничение доступа в выделенные помещения
6) Если сеть централизованная, то защита должна
   a) централизованной
   b) распределенной
7) При схеме управления защитой информации ***"длинные руки"*** полномочия пользователей

на каждом компьютере устанавливаются
   a) администратором удаленно со своего рабочего места
   b) самим пользователем системы
   c) пользователем системы после действий администратора безопасности

8) Схема отложенного централизованного управления доступом требует, чтобы компьютеры пользователей на момент изменения полномочий были
   a) включены
   b) выключены
   c) безразлично

9) Для облегчения работы администратора безопасности по контролю за состоянием безопасности АС необходимо предусмотреть следующие возможности
   a) селекцию определенных событий из системных журналов
   b) ограничение перечня событий, регистрируемых СЗИ
   c) семантическое сжатие данных в журналах регистрации
   d) автоматическую подготовку отчетных документов

10) Реальные возможности нарушителя определяются
   a) психологическим состоянием нарушителя
   b) состоянием объекта защиты,
   c) наличием потенциальных каналов утечки информации,
   d) качеством средств защиты информации

11) В качестве показателя эффективности системы защиты информации может быть использованы
   a) вероятность обнаружения нарушения
   b) своевременность реакции на каждый вид нарушения
   c) доказуемость нарушения

12) Для осуществления несанкционированного доступа в информационную систему требуется провести подготовительные действия
   a) собрать сведения о системе
   b) выполнить пробные попытки вхождения в систему
   c) выявить организационную структуру предприятия

13) Программы ЦП характеризуются следующими параметрами
   a) криптостойкостью
   b) количеством операторов
   c) временем работы
   d) функциональными возможностями

14) Время работы алгоритма ЦП складывается из времени
   a) набора текста
   b) генерации ключей
   c) проверки подписи
   d) постановки подписи

15) С увеличением криптостойкости системы ЦП временные характеристики
   a) падают
   b) увеличиваются

Примерная тематика докладов №1

1. Понятие политики безопасности организации.
2. Сертификация средств защиты информации.
3. Категорирование информационных объектов по степени важности и конфиденциально-

сти защищаемой информации.
4. Программы внутренней защиты. Программы ядра системы безопасности.
5. Интегральная безопасность информационных систем.
6. Комплексная защита объектов.
7. Механические системы защиты.
8. Системы оповещения.

Типовые вопросы для коллоквиума №1

1. Классификация угроз информационной безопасности по базовым признакам.
2. Угрозы нарушения конфиденциальности.
3. Угрозы нарушения целостности данных.
4. Угрозы отказа служб (угрозы отказа в доступе).
5. Понятие политики безопасности информационных систем. Назначение политики безопасности.
6. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
7. Законодательный уровень обеспечения информационной безопасности.
8. Основные законодательные акты РФ в области защиты информации
9. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем.
10. Основные направления и способы защиты информации.
11. Понятия идентификации и аутентификации.
12. Требования к парольной защите.
13. Основные направления технической защиты информации.
14. Понятие технического канала утечки информации

Типовые вопросы для коллоквиума №2

1. Основные понятия и определения информационной безопасности. Виды информации ограниченного доступа.
2. Цели и задачи защиты информации.
3. Угрозы утечки информации по техническим каналам.
4. Характеристики объектов информатизации.
5. Побочные электромагнитные излучения и наводки.
6. Классификация технических каналов утечки информации.

Примерный перечень теоретических и практических заданий для экзамена

№	Задание	Варианты ответа	Кол-во баллов
1.	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее, это …	а) Уязвимость проектирования б) Атака в) Угроза безопасности информации г) Тревога	1
2.	Не относится к уровням обеспечения информационной безопасности:	а) нормативно-правовой б) организационный в) социальный г) технический	1
3	Принцип, состоящий в том, что ни один сотрудник организации не должен иметь полномочий, позво-	а) Непрерывность защиты б) Разделение функций	1

<table>
<tr><td></td><td>ляющих ему единолично выполнять критичные операции, называется …</td><td>в) Разумная достаточность
г) Персональная ответственность</td><td></td></tr>
<tr><td>4</td><td>Не является сервисом безопасности:</td><td>а) экранирование
б) управление доступом
в) туннелирование
г) кодирование</td><td>1</td></tr>
<tr><td>5</td><td>Комплекс предупредительных мер по обеспечению ИБ организации, включающий руководящие принципы, правила и процедуры в области безопасности, это …</td><td>а) Программа безопасности
б) Политика безопасности
в) Кодекс безопасности
г) Защита информации</td><td>1</td></tr>
<tr><td>6</td><td>Зашифровать слово БЕЗОПАСНОСТЬ перестановкой согласно таблице.
1 2 3 4 5 6 7 8 9 10 11 12
5 8 6 11 1 10 9 4 3 12 2 7</td><td>а) ПНАТБСООЗЬЕС
б) ПНАСБТООЗЬЕС
в) ПОАТБСНОЗЬЕС
г) ПНАТЬБСООЗЕС</td><td>2</td></tr>
<tr><td>7</td><td>При моноалфавитной замене получен шифрокод ЗЖРЩ. Расшифровать слово, если известно, что смещение k является нечетным числом.</td><td>а) ФЛЭШ
б) БАЙТ
в) ЛОГИН
г) СТЭК</td><td>2</td></tr>
<tr><td>8</td><td>Зашифровать слово HAIFспособом простой замены, используя таблицу.
A B C D E F G H I J
F I L O R U X A D Q</td><td>а) FOID
б) AFDX
в) FOAD
г) AFDU</td><td>2</td></tr>
<tr><td>9</td><td>Зашифровать сообщение (2,3) методом RSA, если открытый ключ (K_0 ,N)➡(7,33).</td><td>а) (27,4)
б) (29,9)
в) (29,4)
г) (29,2)</td><td>2</td></tr>
<tr><td>10</td><td>Расшифровать криптограмму (3,1) методом RSA, если секретный ключ (K_c ,N)➡(3,22).</td><td>а) (5, 1)
б) (7, 5)
в) (7, 1)
г) (9,11)</td><td>2</td></tr>
<tr><td>11</td><td>Зашифровать методом Виженера сообщение ШИФРЫ ЗАМЕНЫ. Ключ – ХАКЕР (Таблицу см. в приложении).</td><td>а) МИЮФЛЫАЦКЭР
б) МИЮФЛЫАЦЛЭР
в) МИЭХЛЫАШКЭР
г) МИЮХЛЫАЦКЭР</td><td>3</td></tr>
<tr><td>12</td><td>Определить ключ слова ТЕХНОЛОГИЯ, шифрокод которого по методу Виженера: ФКЯПУХРИТА.</td><td>а) ТПК
б) ВОЛЬТ
в) ВЕК
г) СТО</td><td>3</td></tr>
<tr><td>13</td><td>Зашифровать сообщение ИНТЕРНЕТ способом Гронсфельда.
№ позиции | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8
Ключ | 5 | 2 | 4 | 8 | 1 | 3 | 6 | 7</td><td>а) МОХЛРПЙШ
б) МОЧЛРСЙШ
в) НПЦМСРКЩ
г) НПЦМКРКЩ</td><td>3</td></tr>
<tr><td>14</td><td>Получить шифрокод слова УНИВЕРСИТЕТ методом гаммирования, если гаммой шифра является ХЕШИРОВАНИЕ.</td><td>а) БЗПЙЭЦРЗЬОФ
б) БЗСЙЦЭРЗЬОФ
в) БЗПЙЦЭРЗЬОФ
г) БЗСЙЦЭРТЬОФ</td><td>3</td></tr>
<tr><td>15</td><td>Определить гамму, если шифрокоду ТЕСТ соответствует информация КРАХ.</td><td>а) ХЦТД
б) ЧЦТД
в) ЧФТД
г) ЧЦРД</td><td>3</td></tr>
</table>