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 г.

УТВЕРЖДАЮ

Первый проректор
С.В. Авдашкевич
28.06.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина:	Б1.В.11 Информационная безопасность в логистике
Направление подготовки:	38.03.02 Менеджмент
Направленность (профиль):	Логистический менеджмент
Уровень высшего образования:	Бакалавриат
Форма обучения:	очная, заочная, очно-заочная
Разработчики:	Кандидат технических наук, доцент Иванов С.А.

Санкт-Петербург
2023

1. Цели и задачи дисциплины:

Цель освоения дисциплины:

формирование у студентов комплекса знаний, навыков и компетенций в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи дисциплины:

− сформировать у студентов знания о современных тенденциях угроз информационной безопасности, о нормативных правовых документах по защите информации;

− сформировать у студентов устойчивое понимание роли и значения информационной безопасности личности, общества и государства и информационной инфраструктуры общества и государства;

− сформировать у студентов общие представления о современных методах и средствах защиты информации.

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

Планируемые результаты освоения ОП ВО (код и содержание компетенций)	**Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)**	**Примечание**
УК-11 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-11.1 Знает об основных направлениях государственной политики в области противодействия экстремистской деятельности, терроризму, коррупции; международно-правовые основы противодействия экстремистской деятельности, терроризму, коррупции; организационные основы противодействия экстремистской деятельности, терроризму, коррупции.	Наименование категории (группы) компетенций: «Гражданская позиция»
	УК-11.2 Умеет выявлять признаки экстремистской и террористической деятельности, коррупционного поведения; анализировать действующие правовые нормы, обеспечивающие борьбу с экстремизмом, терроризмом, коррупцией в различных областях жизнедеятельности, а также способы профилактики экстремистской и террористической деятельности, коррупции.	
	УК-11.3 Способен осуществлять социальную и профессиональную деятельность на основе развитого правосознания и сформированной правовой культуры, соблюдать правила общественного взаимодействия на основе нетерпимого отношения к проявлениям экстремизма, терроризма, коррупционного поведения.	
ПК-3 Способен организовывать процесс улучшения качества оказания логистических услуг по перевозке грузов в цепи поставок	ПК-3.1 Знает правовые основы транспортно-логистической деятельности; основы гражданского законодательства; коммерческую политику компании; политику компании в области клиентского сервиса; корпоративную структуру компании.	40.049 Профессиональный стандарт «Специалист по логистике на транспорте»
	ПК-3.2 Умеет устанавливать требования клиентов к результату перевозки и ранжировать их по степени значимости для клиентов; профессионально работать с претензионной документацией; оформлять документы на несоответствующую услугу; проводить переговоры с клиентами из различных отраслей экономики; анализировать информацию и формировать отчеты.	

Планируемые результаты освоения ОП ВО (код и содержание компетенций)	Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)	Примечание
	ПК-3.3 Способен выполнять следующие трудовые действия: проводить переговоры с клиентами по претензионным случаям; определять причастных и виновных лиц; определять причины, повлекшие предъявление претензии; взаимодействовать с клиентами по качеству сервиса; организовывать мониторинг эффективности контрагентов, переадресовывать им претензии клиента в случае некачественного сервиса со стороны контрагента; составлять реестр наиболее часто задаваемых клиентами вопросов; разрабатывать инструкции по предотвращению претензий.	

Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)	Планируемые результаты обучения по дисциплине
УК-11.1. Знает об основных направлениях государственной политики в области противодействия экстремистской деятельности, терроризму, коррупции; международно-правовые основы противодействия экстремистской деятельности, терроризму, коррупции; организационные основы противодействия экстремистской деятельности, терроризму, коррупции.	Знать понятия: коррупция, экстремизм, терроризм и их основные признаки. Знать основные принципы и меры по противодействию и профилактике данным явлениям в сфере информационной безопасности в логистике.
УК-11.2. Умеет выявлять признаки экстремистской и террористической деятельности, коррупционного поведения; анализировать действующие правовые нормы, обеспечивающие борьбу с экстремизмом, терроризмом, коррупцией в различных областях жизнедеятельности, а также способы профилактики экстремистской и террористической деятельности, коррупции.	Уметь выявлять признаки экстремизма и терроризма в различных информационных материалах, определять, выявлять и оценивать экстремизм, терроризм и коррупционное поведение в профессиональной деятельности, в области информационной безопасности в логистике.
УК-11.3. Способен осуществлять социальную и профессиональную деятельность на основе развитого правосознания и сформированной правовой культуры, соблюдать правила общественного взаимодействия на основе нетерпимого отношения к проявлениям экстремизма, терроризма, коррупционного поведения.	Владеть навыками выявления причин, способствующих совершению преступлений экстремистской, террористической и коррупционной направленности в области информационной безопасности. Навыками работы с законодательными и другими нормативно-правовыми актами в сфере обеспечения информационной безопасности в логистике.
ПК-3.1. Знает правовые основы транспортно-логистической деятельности; основы гражданского законодательства; коммерческую политику компании; политику компании в области клиентского сервиса; корпоративную структуру компании.	Знать нормативно-правовую базу для организации логистических процессов и обеспечения их безопасности.
ПК-3.2. Умеет устанавливать требования клиентов к результату перевозки и ранжировать их по степени значимости для клиентов; профессионально работать с претензионной документацией; оформлять документы на несоответствующую услугу; проводить переговоры с клиентами из различных отраслей экономики; анализировать информацию и формировать отчеты.	Уметь определять требования информационной безопасности к грузоперевозкам, анализировать потребности клиентов.

Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)	Планируемые результаты обучения по дисциплине
ПК-3.3. Способен выполнять следующие трудовые действия: проводить переговоры с клиентами по претензионным случаям; определять причастных и виновных лиц; определять причины, повлекшие предъявление претензии; взаимодействовать с клиентами по качеству сервиса; организовывать мониторинг эффективности контрагентов, переадресовывать им претензии клиента в случае некачественного сервиса со стороны контрагента; составлять реестр наиболее часто задаваемых клиентами вопросов; разрабатывать инструкции по предотвращению претензий.	Владеет навыками работы с претензионными случаями, определения недостатков в области политики информационной безопасности логистических процессов.

3. Содержание, объем дисциплины и формы проведения занятий

№ п/п	Наименование темы дисциплины	Компетенции	Оценочные средства текущего контроля		
			ЗНАТЬ	УМЕТЬ	ВЛАДЕТЬ
			ПК-3.1 УК-11.1	ПК-3.2 УК-11.2	ПК-3.3 УК-11.3
1	Основные понятия и определения	ПК-3	Деловая и (или) ролевая игра/Кейс-задача №1 (20)	Деловая и (или) ролевая игра/Кейс-задача №1 (20)	Деловая и (или) ролевая игра/Кейс-задача №1 (20)
2	Задачи и угрозы информационной безопасности	ПК-3	Деловая и (или) ролевая игра/Кейс-задача №2 (20)	Деловая и (или) ролевая игра/Кейс-задача №2 (20)	Деловая и (или) ролевая игра/Кейс-задача №2 (20)
3	Понятие и виды защищаемой информации	ПК-3	Деловая и (или) ролевая игра/Кейс-задача №3 (20)	Деловая и (или) ролевая игра/Кейс-задача №3 (20)	Деловая и (или) ролевая игра/Кейс-задача №3 (20)
4	Криптографические методы защиты информации и обеспечение безопасного доступа	ПК-3	Деловая и (или) ролевая игра/Кейс-задача №4 (20)	Деловая и (или) ролевая игра/Кейс-задача №4 (20)	Деловая и (или) ролевая игра/Кейс-задача №4 (20)
5	Программно-аппаратные средства защиты информации	УК-11 ПК-3	Деловая и (или) ролевая игра/Кейс-задача №5 (20)	Деловая и (или) ролевая игра/Кейс-задача №5 (20)	Деловая и (или) ролевая игра/Кейс-задача №5 (20)
Количество баллов (100 баллов):			100		

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа
Тема 1: Основные понятия и определения Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде. **Практические занятия/самостоятельная работа:** Генерация паролей. Обзор статей УК РФ. ГК РФ, КоАД РФ, ТК РФ. Обзор сайта ФСТЭК, обзор ключевых требований по защите информации ФСТЭК и ФСБ Нормативно-правовая база РФ и организационные аспекты назначения экспертиз информационных материалов, содержащих признаки идеологии терроризма (включая и материалы из интернет) в связи с принятием Федерального закона «О противодействии экстремистской деятельности», «О противодействии террористической деятельности». Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Киберэкстремизм и кибертерроризм. **Лабораторная работа:** -
Тема 2: Задачи и угрозы информационной безопасности

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа
Задача обеспечения конфиденциальности. Задача обеспечения аутентификации. Обеспечение идентификации. Задача обеспечения целостности. Классификация угроз информационной безопасности. Угрозы несанкционированного доступа к данным. Угрозы нарушения целостности данных. Угрозы нарушения конфиденциальности данных. **Практические занятия/самостоятельная работа:** Простейшие криптографические преобразования. **Лабораторная работа:** -
Тема 3: Понятие и виды защищаемой информации Путь конфиденциального документа от создания до уничтожения: решение, разработка проекта, подготовка содержания, реквизитов, передача, получение, исполнение и архивация. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. **Практические занятия/самостоятельная работа:** Режимы применения блочных шифров **Лабораторная работа:** -
Тема 4: Криптографические методы защиты информации и обеспечение безопасного доступа Основные понятия криптографии. Симметричные шифры. Криптография с открытым ключом. Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе. Концепция построения систем разграничения доступа. **Практические занятия/самостоятельная работа:** Открытое распространение ключей **Лабораторная работа:** -
Тема 5: Программно-аппаратные средства защиты информации Аппаратные и программно-аппаратные средства криптозащиты данных. Использование дополнительных плат расширения. Методы “водяных знаков” и методы “отпечатков пальцев”. Защита программ от несанкционированного копирования. Вирусы. **Практические занятия/самостоятельная работа:** Асимметричное шифрование и электронная цифровая подпись **Лабораторная работа:** -
Курсовая работа: не предусмотрено учебным планом

Очная форма обучения

Вид учебной работы	Всего часов	Семестр 5
Аудиторные занятия (АЗ):	54	54
Лекционные занятия (Лек)	18	18
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	36	36
Самостоятельная работа студента (СР)	49	49
Курсовая работа	0	0
Другие виды самостоятельной работы*	49	49
Контроль самостоятельной работы (КСР)	5	5
Контактная работа (КоР)	59	59
Форма промежуточной аттестации	0	Зачет
Подготовка к экзамену и сдача экзамена (СР, КоР)	0	0
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям, подготовка к зачету (при наличии)

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Основные понятия и определения	5	2	4	0	9	4
2	Задачи и угрозы информационной безопасности	5	4	8	0	10	8
3	Понятие и виды защищаемой информации	5	4	8	0	10	8
4	Криптографические методы защиты информации и обеспечение безопасного доступа	5	4	8	0	10	8
5	Программно-аппаратные средства защиты информации	5	4	8	0	10	8

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
	Итого:		18	36	0	49	36

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

Заочная форма обучения

Вид учебной работы	Всего часов	Семестр 5
Аудиторные занятия (АЗ):	8	8
Лекционные занятия (Лек)	4	4
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	4	4
Самостоятельная работа студента (СР)	91	91
Курсовая работа	0	0
Другие виды самостоятельной работы*	91	91
Контроль самостоятельной работы (КСР)	5	5
Контактная работа (КоР)	13	13
Форма промежуточной аттестации	0	Зачет
Подготовка к экзамену/зачету и сдача экзамена/зачета (СР, КоР)	4	4
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Основные понятия и определения	5	2	2	0	12	4
2	Задачи и угрозы информационной безопасности	5	2	2	0	12	8
3	Понятие и виды защищаемой информации	5	0	0	0	20	8
4	Криптографические методы защиты информации и обеспечение безопасного доступа	5	0	0	0	20	8
5	Программно-аппаратные средства защиты информации	5	0	0	0	27	8
	Итого:		4	4	0	91	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.

Очно-заочная форма обучения

Вид учебной работы	Всего часов	Семестр 5
Аудиторные занятия (АЗ):	18	18
Лекционные занятия (Лек)	8	8
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	10	10
Самостоятельная работа студента (СР)	86	86
Курсовая работа	0	0
Другие виды самостоятельной работы*	86	86
Контроль самостоятельной работы (КСР)	4	4
Контактная работа (КоР)	22	22
Форма промежуточной аттестации	0	Зачет
Подготовка к экзамену и сдача экзамена (СР, КоР)	0	0
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям, подготовка к зачету (при наличии)

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Основные понятия и определения	5	2	2	0	12	4
2	Задачи и угрозы информационной безопасности	5	2	2	0	12	8
3	Понятие и виды защищаемой информации	5	2	2	0	12	8
4	Криптографические методы защиты информации и обеспечение безопасного доступа	5	2	2	0	22	8
5	Программно-аппаратные средства защиты информации	5	0	2	0	28	8
		Итого:	8	10	0	86	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.

4. Способ реализации дисциплины

Без использования онлайн-курса.

5. Учебно-методическое обеспечение дисциплины:

Основная литература:

1. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЛОГИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ТОРГОВЫХ КОМПАНИЙ. Учебное пособие для вузов / Новиков В. Э. - Национальный исследовательский университет «Высшая школа экономики» (г. Москва)., 2023 г. - 184 с. - ISBN 978-5-534-01012-1 – Режим доступа: https://urait.ru/book/informacionnoe-obespechenie-logisticheskoy-deyatelnosti-torgovyh-kompaniy-511280

2. ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Учебник и практикум для вузов / Под ред. Поляковой Т. А., Стрельцова А. А. - Всероссийский государственный университет юстиции (РПА Минюста России) (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2023 г. - 325 с. - ISBN 978-5-534-03600-8 – Режим доступа: https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-511239

3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Учебное пособие для вузов / Суворова Г. М. - Ярославский государственный педагогический университет имени К.Д. Ушинского (г. Ярославль)., 2023 г. - 253 с. - ISBN 978-5-534-13960-0 – Режим доступа: https://urait.ru/book/informacionnaya-bezopasnost-519780

Дополнительная литература:

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ. Учебное пособие для вузов / Зенков А. В., 2023 г. - 104 с. - ISBN 978-5-534-14590-8 – Режим доступа: https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-520063

2. Прохорова О. В. — Информационная безопасность и защита информации: учебник для вузов - Издательство Лань, 2023 г. - 124 с. - ISBN 978-5-507-46010-6 – Режим доступа: https://e.lanbook.com/book/293009

3. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебник и практикум для вузов / Казарин О. В., Забабурин А. С. - Российский государственный гуманитарный университет (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2023 г. - 312 с. - ISBN 978-5-9916-9043-0 – Режим доступа: https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-513300

6. 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. LMS Moodle
5. Вебинарная платформа

7. 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. Развитие бизнеса.РУ [Электронный ресурс] : Информационная справочная система. - Режим доступа: https://www.devbusiness.ru. - Текст: электронный
9. it-world.ru [Электронный ресурс] : информационная справочная система . - Режим доступа: https://www.it-world.ru. - Текст: электронный
10. Компьютерра : информационная справочная система . - Режим доступа: https://www.computerra.ru/. - Текст: электронный
11. Бизнес-информатика: профессиональная база данных . - Режим доступа: https://bijournal.hse.ru/. - Текст: электронный
12. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: профессиональная база данных. - Режим доступа: https://digital.gov.ru. - Текст: электронный
13. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: профессиональная база данных . - Режим доступа: https://rkn.gov.ru. - Текст: электронный
14. Executive.ru: профессиональная база данных . - Режим доступа: https://www.e-xecutive.ru. - Текст: электронный

8. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа, семинарского типа - практических занятий, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованная: рабочими местами для обучающихся, оснащенными специальной мебелью; рабочим местом преподавателя, оснащенным специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; техническими средствами

обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской; лицензионным программным обеспечением

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

3. 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). Авторизация на информационно-образовательном портале Университета umeos.ru и начало работы осуществляются с использованием персональной учетной записи (логина и пароля). Лицензионное программное обеспечение

9. Оценочные материалы по дисциплине

Описание оценочных средств (показатели и критерии оценивания, шкалы оценивания) представлено в приложении к основной профессиональной образовательной программе «Каталог оценочных средств текущего контроля и промежуточной аттестации».

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приводятся в соответствующих методических материалах и локальных нормативных актах Университета.

Для оценивания учебных достижений студентов в Университете действует балльно-рейтинговая система.

Если оценка, соответствующая набранной в семестре сумме рейтинговых баллов, удовлетворяет студента, то она является итоговой оценкой по дисциплине при проведении промежуточной аттестации в форме экзамена/зачета с оценкой/зачета.

Условием сдачи экзамена/зачета с оценкой/зачета с целью повышения итоговой оценки по дисциплине является сдача студентом экзамена, за который он получает экзаменационные баллы без учета баллов, полученных за текущий контроль:

Шкала оценивания учебных достижений по дисциплине,завершающейся зачетом без оценки

Баллы по дисциплине	60 и менее		61-73		74-90		91-100
Итоговая оценка по дисциплине	Незачет		Зачет				
Баллы в международной шкале ECTS с буквенным обозначением уровня	50 и менее	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
Уровень сформированности компетенций	Не сформированы		Пороговый		Высокий		Повышенный

Шкала оценивания учебных достижений по дисциплине, завершающейся экзаменом/ зачетом с оценкой

Баллы по дисциплине	60 и менее	61-73	74-90	91-100
Итоговая оценка по дисциплине	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

Баллы в международной шкале ECTS с буквенным обозначением уровня	<50	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
Уровень сформированности компетенций	Не сформированы		Пороговый		Высокий		Повышенный

9.1. Типовые контрольные задания для текущего контроля

Деловая и (или) ролевая игра/Кейс-задача №1

1) Разработать программу на языке С++, реализующую следующие функции:
– генерация строки с заданной пользователем длиной, состоящей из символов алфавита в соответствии с вариантом задания (использовать функции rand( ), srand( ) и инициализацию от таймера);
– поверка равномерности распределения символов путем визуализации частотного распределения;
– вычисление среднего времени подбора пароля, выбираемого из сгенерированной строки.
2) Построить график зависимости среднего времени подбора пароля от его длины.
3) Дать практические рекомендации по выбору пароля исходя из предположений об алфавите пароля; ценности информации, доступ к которой защищается с помощью этого пароля; производительности вычислительного средства атакующего и времени атаки.
Варианты алфавита для генерации пароля: 1) Латиница строчные. 2) Латиница строчные и прописные. 3) Буквы русского языка строчные. 4) Буквы русского языка строчные и прописные. 5) Арабские цифры. 6) Латиница строчные и арабские цифры. 7) Латиница строчные, прописные и арабские цифры. 8) Буквы русского языка строчные и арабские цифры. 9) Буквы русского языка строчные, прописные и арабские цифры. 10) Все символы таблицы ASCII.
Вариант выбирается в соответствии с номером студента в рамках группы. Если студентов в группе больше, чем вариантов в списке, то варианты снова повторяются начиная с единицы.

Деловая и (или) ролевая игра/Кейс-задача №2

1) Реализовать в виде программы шифр (зашифрование и расшифрование) в соответствии с вариантом. Язык исходного текста русский или английский по выбору исполнителя.
2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.
3) Оценить криптографическую стойкость реализованного шифра.
4) Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.
Варианты для реализации. 1) Шифр Цезаря. 2) Шифр Виженера. 3) Шифр Скитала. 4) Шифр перестановки, использующий простые (прямоугольные) таблицы.
Вариант выбирается в соответствии с номером студента в рамках группы. Если студентов в группе больше, чем вариантов в списке, то варианты снова повторяются, начиная с единицы.

Деловая и (или) ролевая игра/Кейс-задача №3

1) Зашифровать предложенные преподавателем изображения всеми возможными алгоритмами во всех возможных режимах. Результаты шифрования отразить в отчете в виде скриншотов.
2) Оценить полученные результаты и объяснить их причины.
3) Дать рекомендации по применению алгоритмов шифрования и их режимов в зависимости от типов изображения, шифрования и особенностей применения.
4) Дать ответ на вопрос: как влияет размер блока шифра на результат шифрования и почему?

Деловая и (или) ролевая игра/Кейс-задача №4
Для заданного простого P (в соответствии с вариантом) найти g – примитивный элемент конечного поля GF(P) и выполнить генерацию общего секрета. Для нахождения g воспользуйтесь методом перебора по возрастанию, возведения в степень по модулю P и проверки того факта, что все степени принимают значения от 0 до P – 1.
Варианты: 1) 5717 11) 3877 21) 4877 2) 9721 12) 1877 22) 2957 3) 2111 13) 1973 23) 2971 4) 3917 14) 4937 24) 3137 5) 4231 15) 7237 25) 1123 6) 9001 16) 9011 26) 9679 7) 8699 17) 8233 27) 8329 8) 8447 18) 8581 28) 7351 9) 7489 19) 7573 29) 7673 10) 7759 20) 7883 30) 6823
Вариант выбирается в соответствии с порядковым номером студента в рамках группы. Если студентов в группе больше, чем вариантов в списке, то варианты снова повторяются, начиная с единицы.
Отчет должен содержать:
1) Листинги программ: а) для проверки g (первообразный корень по модулю P); б) для вычисления Ba mod P = gab mod P и Ab mod P = gab mod P.
2) Описание шагов, выполняемых участниками протокола – Алисой и Бобом для вычисления общего секрета.
3) Выводы, содержащие: а) модель атакующего и оценки длины ключа; б) возможные угрозы протоколу и предложения по защите от них.

Деловая и (или) ролевая игра/Кейс-задача №5
Разработать программное обеспечение, реализующее функции генерации секретного и открытого ключей, шифрования и цифровой подписи для алгоритма RSA.
Обмен входными и выходными данными должен осуществляться через файлы:
– открытого ключа;
– секретного ключа;
– исходного сообщения;
– зашифрованного сообщения.
Для повышения скорости шифрования использовать метод последовательного возведения в квадрат и умножения. Выполнить тестирование разработанного программного обеспечения на 10 наборах тестовых данных. Длина чисел p и q должна быть не менее 1024 бит.

9.2. Примерный перечень тем курсовой работы
Не предусмотрено учебным планом

9.3. Типовые контрольные задания для промежуточной аттестации: зачет

Примерный перечень теоретических вопросов к зачету
1. Определение информационной безопасности.
2. Критические данные.
3. Признаки компьютерных преступлений в интернет технологиях.
4. Основные технологии и методы компьютерных преступлений.
5. Уровня защиты компьютерных (интернет технологий) и информационных ресурсов.
6. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
7. Концепция обеспечения безопасности информационных систем.
8. Избирательная политика управления доступом.
9. Организационные меры безопасности информационных систем.
10. Матрица доступа в АСОИ.
11. Полномочное управление доступом.

12. Избирательное управление доступом.
13. Оценочные стандарты и технические спецификации.
14. Угрозы безопасности данных
15. Источники нарушений безопасности
16. Аутентификация
17. Авторизация пользователей
18. Методы парольной аутентификации. Недостатки методов аутентификации с запоминаемым паролем.
19. Аутентификация с помощью биометрических характеристик.
20. Принципы работы биометрических систем.
21. Реализация биометрических систем.
22. Поведенческие биометрические характеристики.
23. Атаки на биометрические системы.
24. Правовое обеспечение информационной безопасности по части статьи УК РФ 272
25. Правовое обеспечение информационной безопасности по части статьи УК РФ 273
26. Правовое обеспечение информационной безопасности по части статьи УК РФ 274
27. Сущность и отличительные признаки кибертерроризма, его характерные проявления.
28. Российское законодательство о противодействии распространению террористических материалов в интернете.
29. Характерные особенности судебной экспертизы материалов экстремистско-террористической направленности.

Примерный перечень практических заданий к зачету

1) Создать папку с общим доступом на одной из виртуальных машин.
2) Настроить брандмауэр, применив различные политики:
а) доступ к разделяемому ресурсу разрешен только компьютеру с данным IP-адресом;
б) доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp);
в) доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp) и только компьютерам с данным IP-адресом (адресами);
г) доступ к внешним ресурсам разрешен только конкретным программам;
д) конкретной программе разрешен доступ к ресурсам удаленного компьютера с данным IP-адресом по заданному порту;
е) запретить запрос входящего эха (ICMP).
3) Оформить отчет, подтверждающий применение указанных политик.