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.17 Информационная безопасность
Направление подготовки:	38.03.05 Бизнес-информатика
Направленность (профиль):	Цифровые решения для бизнеса
Уровень высшего образования:	Бакалавриат
Форма обучения:	очная, заочная, очно-заочная
Разработчики:	Старший преподаватель Мурзинцев С. В.

Санкт-Петербург
2023

1. Цели и задачи дисциплины:

Цель освоения дисциплины:

формирование у студентов методически правильных основ знаний и практических навыков по основам информационной безопасности (ИБ), необходимых выпускникам университета, занимающимся эксплуатацией корпоративных информационных систем.

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

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-2 Способен разрабатывать архитектуру ИС	ПК-2.1 Знает современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM); основы современных операционных систем; архитектуру, устройство и функционирование вычислительных систем; инструменты и методы верификации и проектирования архитектуры ИС; программные средства и платформы инфраструктуры информационных технологий организаций; коммуникационное оборудование; сетевые протоколы.	06.015 Профессиональный стандарт «Специалист по информационным системам»
	ПК-2.2 Умеет проверять (верифицировать) архитектуру ИС; проектировать архитектуру ИС.	
	ПК-2.3 Способен разрабатывать архитектурную спецификацию ИС и согласовывать ее с заинтересованными сторонами.	

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.
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.
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.
ПК-2.1. Знает современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM); основы современных операционных систем; архитектуру, устройство и функционирование вычислительных систем; инструменты и методы верификации и проектирования архитектуры ИС; программные средства и платформы инфраструктуры информационных технологий организаций; коммуникационное оборудование; сетевые протоколы.	Знать современные информационные технологии (ИТ) и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности с учетом требований информационной безопасности.
ПК-2.2. Умеет проверять (верифицировать) архитектуру ИС; проектировать архитектуру ИС.	Уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.
ПК-2.3. Способен разрабатывать архитектурную спецификацию ИС и согласовывать ее с заинтересованными сторонами.	Владеть навыками использования современных информационных технологий (ИТ) и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.

3. Содержание, объем дисциплины и формы проведения занятий

№ п/п	Наименование темы дисциплины	Компетенции	Оценочные средства текущего контроля		
			ЗНАТЬ	УМЕТЬ	ВЛАДЕТЬ
			ПК-2.1 УК-11.1	ПК-2.2 УК-11.2	ПК-2.3 УК-11.3
1	Сетевая безопасность	УК-11 ПК-2	Круглый стол, дискуссия, полемика, дебаты/Эссе №1 (20) Круглый стол, дискуссия, полемика, дебаты/Эссе №2 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №1 (20) Круглый стол, дискуссия, полемика, дебаты/Эссе №2 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №1 (20) Круглый стол, дискуссия, полемика, дебаты/Эссе №2 (20)

№ п/п	Наименование темы дисциплины	Компетенции	Оценочные средства текущего контроля		
			ЗНАТЬ	УМЕТЬ	ВЛАДЕТЬ
			ПК-2.1 УК-11.1	ПК-2.2 УК-11.2	ПК-2.3 УК-11.3
2	Классификация угроз	УК-11 ПК-2	Круглый стол, дискуссия, полемика, дебаты/Эссе №3 (20) Круглый стол, дискуссия, полемика, дебаты/Эссе №4 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №3 (20) Круглый стол, дискуссия, полемика, дебаты/Эссе №4 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №3 (20) Круглый стол, дискуссия, полемика, дебаты/Эссе №4 (20)
3	Классификация типов программно-аппаратных средств защиты информации	ПК-2	Круглый стол, дискуссия, полемика, дебаты/Эссе №5 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №5 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №5 (20)
Количество баллов (100 баллов):			100		

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа

Тема 1: Сетевая безопасность

Введение в информационную безопасность, Правовое обеспечение информационной безопасности, Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности. Информационные технологии в деятельности террористических организаций и современная информационная война. Интернет как сфера распространения идеологии терроризма. Экстремистские материалы: понятие, сущность, разновидности. Интернет как идеологическая площадка для пропаганды, вербовки сторонников терроризма, потенциальных исполнителей террористичесих актов. Общая характеристика террористических сообществ в Интернете. Особенности противодействия вовлечению граждан в экстремистскую деятельность: объективные и субъективные аспекты. Законодательное противодействие распространению террористических и экстремистских материалов в Интернете. Международные стандарты в области предупреждения преступлений в информационно-коммуникационной сфере. Конвенция Совета Европы «О киберпреступлениях» ETS № 185 от 23 ноября 2001 г. Международный опыт противодействия терроризму в сфере информационно-коммуникационных технологий. Законодательное противодействие распространению террористических материалов в Интернете. Предмет, объекты и субъекты антикоррупционной экспертизы. Условия, формирующие и способствующие совершению коррупционных преступлений в информационной сфере.

Практические занятия/самостоятельная работа:

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: Классификация угроз

Классификация сетевых угроз, Файерволлы, Антивирусы, Обновление и настройка операционной системы, шифрование и пароли, архивирование и резервное копирование, социальная инженерия. Злоупотребление высокими технологиями как фактор возникновения кибертерроризма. Кибертерроризм как продукт глобализации. Сущность понятия кибертерроризма. Отличительные признаки кибертерроризма, его характерные проявления. Формы кибератак, хакерства и нанесения ущерба информационным и компьютерным сетям граждан, юридических лиц,государственных учреждений. Способы использования интернета, IT-технологий и телекоммуникационных сетей в террористических целях. Компьютерные игры как способ вовлечения подростков и молодежи в террористическую деятельность при помощи Интернета. Избирательный подход к компьютерным играм.

Практические занятия/самостоятельная работа:

Программная настройка антивирусных систем защиты информации на рабочем месте. Подготовка средств ТЗИ для организации работы персонала на рабочем месте. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа
Лабораторная работа: -
Тема 3: Классификация типов программно-аппаратных средств защиты информации Идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, стеганография, экранирование. **Практические занятия/самостоятельная работа:** Обзор методов построения: 1. Средств, разработанных для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах; 2. Средств, принципиально применимых только в компьютерных сетях и предназначенные для разделения информационных потоков; 3. Средств, принципиально предназначенных для защиты информации от НСД в персональных компьютерах. **Лабораторная работа: -**
Курсовая работа: не предусмотрено учебным планом

Очная форма обучения

Вид учебной работы	Всего часов	Семестр 4
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	Сетевая безопасность	4	6	12	0	18	12
2	Классификация угроз	4	6	12	0	15	12
3	Классификация типов программно-аппаратных средств защиты информации	4	6	12	0	16	12
	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	Сетевая безопасность	5	2	0	0	30	12
2	Классификация угроз	5	0	2	0	30	12
3	Классификация типов программно-аппаратных средств защиты информации	5	2	2	0	31	12
	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	Сетевая безопасность	5	2	2	0	28	12
2	Классификация угроз	5	2	4	0	29	12
3	Классификация типов программно-аппаратных средств защиты информации	5	4	4	0	29	12
	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:

2. ЗАЩИТА ИНФОРМАЦИИ 3-е изд., пер. и доп. Учебное пособие для вузов / Внуков А. А. - Национальный исследовательский университет «Высшая школа экономики» (г. Москва)., 2022 г. - 161 с. - ISBN 978-5-534-07248-8 – Режим доступа: https://urait.ru/book/zaschita-informacii-490277

3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Учебное пособие для вузов / Суворова Г. М. - Ярославский государственный педагогический университет имени К.Д. Ушинского (г.

Ярославль)., 2022 г. - 253 с. - ISBN 978-5-534-13960-0 – Режим доступа: https://urait.ru/book/informacionnaya-bezopasnost-496741

3. 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

Дополнительная литература:

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА 2-е изд., испр. и доп. Учебное пособие для вузов / Чернова Е. В. - Магнитогорский государственный технический университет имени Г.И. Носова (г. Магнитогорск)., 2022 г. - 243 с. - ISBN 978-5-534-12774-4 – Режим доступа: https://urait.ru/book/informacionnaya-bezopasnost-cheloveka-495922

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)., 2022 г. - 325 с. - ISBN 978-5-534-03600-8 – Режим доступа: https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-498844

3. НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебное пособие для вузов / Казарин О. В., Шубинский И. Б. - Российский государственный гуманитарный университет (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2022 г. - 342 с. - ISBN 978-5-534-05142-1 – Режим доступа: https://urait.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-493262

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
6. Oracle VM Virtualbox

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. Connect: IT-технологии : информационная справочная система. - Режим доступа: https://www.connect-wit.ru/. - Текст: электронный

9. it-world.ru [Электронный ресурс] : информационная справочная система . - Режим доступа: https://www.it-world.ru. - Текст: электронный

10. Цифровая экономика [Электронный ресурс] : информационная справочная система . - Режим доступа: https://data-economy.ru/2024. - Текст: электронный

11. Бизнес-информатика: профессиональная база данных . - Режим доступа: https://bijournal.hse.ru/. - Текст: электронный

12. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: профессиональная база данных . - Режим доступа: https://rkn.gov.ru. - Текст: электронный

13. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: профессиональная база данных. - Режим доступа: https://digital.gov.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. Учебная аудитория для проведения занятий семинарского типа - практических занятий – компьютерный класс, оборудованный рабочими местами для обучающихся, оснащенными специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; 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

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

4. 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

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

Круглый стол, дискуссия, полемика, дебаты/Эссе №1

1. Правовое обеспечение информационной безопасности по части статьи УК РФ 272
2. Правовое обеспечение информационной безопасности по части статьи УК РФ 273
3. Правовое обеспечение информационной безопасности по части статьи УК РФ 274
4. Сущность и отличительные признаки кибертерроризма, его характерные проявления.
5. Российское законодательство о противодействии распространению террористических материалов в интернете.
6. Характерные особенности судебной экспертизы материалов экстремистско-террористической направленности.

Круглый стол, дискуссия, полемика, дебаты/Эссе №2

Задание 1.

1)Программная настройка антивирусных систем защиты информации на рабочем месте

2)Методы построения:

1. Средств, разработанных для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах;
2. Средств, принципиально применимых только в компьютерных сетях и предназначенные для разделения информационных потоков;
3. Средств, принципиально предназначенных для защиты информации от НСД в персональных компьютерах

Задание 2.

Обоснуйте необходимость избирательного подхода в процессе использования компьютерных игр; приведите соответствующие примеры опасности ряда компьютерных игр для психологии молодых людей

Круглый стол, дискуссия, полемика, дебаты/Эссе №3

Задание 1. Темы для эссе:

1. Файерволлы
2. Антивирусы,
3. Обновление и настройка операционной системы,
4. Шифрование и пароли,
5. Архивирование и резервное копирование,
6. Социальная инженерия

Задание 2.

Составьте перечень признаков, в соответствии с которыми какой-либо сайт может быть однозначно идентифицирован как экстремистский. Какие статьи УК РФ и КОАП РФ могут быть применимы к организаторам и популяризаторам подобных сайтов

Круглый стол, дискуссия, полемика, дебаты/Эссе №4

Задание 1.

Подготовка средств ТЗИ для организации работы персонала на рабочем месте

Задание 2.

Приведите примеры разновидностей экстремистских материалов, с которыми можно столкнуться в сети Интернет. Покажите, каковы общие требовани предъявляются к комплексным психолого-лингвистическим экспертизам, проводимым к отношении подозрительных материалов.

Задание 3.

Покажите основные направления противодействия кибертерроризму, связанные с воздействием на общественное сознание и с решением мировоззренческих проблем молодёжи.

Круглый стол, дискуссия, полемика, дебаты/Эссе №5

1. Основные понятия криптографии
2. Основные понятия стеганографии
3. Типы межсетевых экранов
4. Особенности протоколирования и аудита

9.2. Примерный перечень тем курсовой работы

Не предусмотрено учебным планом

9.3. Типовые контрольные задания для промежуточной аттестации: зачет

Перечень теоретических вопросов к зачёту

№	Задание	Варианты ответа
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 …	Уязвимость проектирования Атака Угроза безопасности информации Тревога
2.	Не относится к уровням обеспечения информационной безопасности:	нормативно-правовой организационный социальный технический
3	Принцип, состоящий в том, что ни один сотрудник организации не должен иметь полномочий, позволяющих ему единолично выполнять критичные операции, называется …	Непрерывность защиты Разделение функций Разумная достаточность Персональная ответственность
4	Не является сервисом безопасности:	экранирование управление доступом туннелирование кодирование
5	Комплекс предупредительных мер по обеспечению ИБ организации, включающий руководящие принципы, правила и процедуры в области безопасности, это …	Программа безопасности Политика безопасности Кодекс безопасности Защита информации

Перечень практических заданий к зачету

Задание 1.

№	Задание	Варианты ответа
1	При моноалфавитной замене получен шифрокод ЗЖРЩ. Расшифровать слово, если известно, что смещение **k** является нечетным числом.	ФЛЭШ БАЙТ ЛОГИН СТЭК
2	Зашифровать сообщение (2,3) методом RSA, если открытый ключ (,N)Æ(7,33).	(27,4) (29,9) (29,4) (29,2)
3	Расшифровать криптограмму (3,1) методом RSA, если секретный ключ (,N)Æ(3,22).	(5, 1) (7, 5) (7, 1) (9,11)
4	Зашифровать методом Виженера сообщение ШИФРЫ ЗАМЕНЫ. Ключ – ХАКЕР (Таблицу см. в приложении).	МИЮФЛЫАЦКЭР МИЮФЛЫАЦЛЭР МИЭХЛЫАШКЭР МИЮХЛЫАЦКЭР
5	Определить ключ слова ТЕХНОЛОГИЯ, шифрокод которого по методу Виженера: ФКЯПУХРИТА.	ТПК ВОЛЬТ ВЕК СТО
6	Получить шифрокод слова УНИВЕРСИТЕТ методом гаммирования, если гаммой шифра является ХЕШИРОВАНИЕ.	БЗПЙЭЦРЗЬОФ БЗСЙЦЭРЗЬОФ БЗПЙЦЭРЗЬОФ БЗСЙЦЭРТЬОФ
7	Определить гамму, если шифрокоду ТЕСТ соответствует информация КРАХ.	ХЦТД ЧЦТД ЧФТД ЧЦРД

Задание 2.

Покажите, как можно эффективно использовантъ специальные информационно-

пропагандистские операции в информационных войнах современно эпохи. Предложите основные пути противодействия информационно-пропагандистским диверсиям.