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

РАССМОТРЕНО И ОДОБРЕНО	УТВЕРЖДАЮ
На заседании кафедры управления правоохранительной деятельностью Протокол № 11 от 20.06.2023 г.	Первый проректор С.В. Авдашкевич 28.06.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина:	Б1.В.11 Преступления в сфере информационной безопасности
Направление подготовки:	40.03.01 Юриспруденция
Направленность (профиль):	Правоохранительная деятельность
Уровень высшего образования:	Бакалавриат
Форма обучения:	очная, заочная, очно-заочная
Разработчики:	кандидат юридических наук, доцент Далинин А. В.

Санкт-Петербург
2023

1. Цели и задачи дисциплины:

Цель освоения дисциплины:

освоение специалистами актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации

Задачи дисциплины:

1. формирование комплексных знаний об основных тенденциях развития технологий, связанных с обеспечением информационной безопасности;

2. формирование практических навыков применения средств защиты информации при решении профессиональных задач.

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
ПК-1 Способен выявлять операции (сделки), подлежащие контролю в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ)	ПК-1.1 Знает законодательство Российской Федерации, регулирующее отношения в сфере ПОД/ФТ.	08.021 Профессиональный стандарт «Специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма)»
	ПК-1.2 Умеет осуществлять мониторинг деятельности физических и юридических лиц в целях ПОД/ФТ; выявлять необычную или подозрительную деятельность; анализировать финансово-экономическую информацию; подготавливать отчетные материалы о выявлении операций (сделок), подлежащих контролю в целях ПОД/ФТ; применять и разъяснять законодательство, нормативные правовые акты и правила внутреннего контроля в целях ПОД/ФТ; взаимодействовать с другими работниками, осуществляющими контроль и надзор в вопросах ПОД/ФТ.	
	ПК-1.3 Способен осуществлять трудовые действия, направленные на выявление незаконных операций, легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.	
ПК-3 Способен выявлять, пресекать преступления и иные правонарушения	ПК-3.1 Знает понятие, признаки и виды правонарушений, понятие и виды юридической ответственности; уголовно-правовую, криминалистическую, криминологическую характеристику отдельных видов преступлений.	Федеральный закон «О полиции» Федеральный закон «О Прокуратуре Российской Федерации» «Уголовно-процессуальный кодекс Российской Федерации»
	ПК-3.2 Умеет осуществлять проверку сообщений о преступлениях и иных правонарушениях, анализировать и оценивать первичную информацию; обеспечивать сохранность обстановки на месте происшествия, производить неотложные следственные действия и принимать меры к установлению и задержанию правонарушителей.	
	ПК-3.3 Способен осуществлять профессионально-служебную деятельность, направленную на выявление и пресечение правонарушений.	

Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)	Планируемые результаты обучения по дисциплине
ПК-1.1. Знает законодательство Российской Федерации, регулирующее отношения в сфере ПОД/ФТ.	Знать содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных; основные виды угроз безопасности персональных данных в информационных системах персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных; процедуры задания и реализации требований по защите информации в информационных системах персональных данных; меры обеспечения безопасности персональных данных; требования по обеспечению безопасности персональных данных; порядок применения организационных и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.
ПК-1.2. Умеет осуществлять мониторинг деятельности физических и юридических лиц в целях ПОД/ФТ; выявлять необычную или подозрительную деятельность; анализировать финансово-экономическую информацию; подготавливать отчетные материалы о выявлении операций (сделок), подлежащих контролю в целях ПОД/ФТ; применять и разъяснять законодательство, нормативные правовые акты и правила внутреннего контроля в целях ПОД/ФТ; взаимодействовать с другими работниками, осуществляющими контроль и надзор в вопросах ПОД/ФТ.	Уметь планировать мероприятия по обеспечению безопасности персональных данных; разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных; обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных; проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.
ПК-1.3. Способен осуществлять трудовые действия, направленные на выявление незаконных операций, легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.	Владеть навыками работы с правовыми базами данных; определения уровней защищённости персональных данных; определения и оценки угроз безопасности персональных данных в информационных системах персональных данных; разработки и реализации организационных мер, обеспечивающих эффективность системы защиты информации; разработки модели угроз безопасности персональным данным в организации; разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных; применения сертифицированных средств защиты информации.
ПК-3.1. Знает понятие, признаки и виды правонарушений, понятие и виды юридической ответственности; уголовно-правовую, криминалистическую, криминологическую характеристику отдельных видов преступлений.	Знать понятие, виды и признаки преступлений в сфере информационной безопасности и высоких технологий (компьютерная преступность), уголовно-правовую, криминалистическую и криминологическую характеристики преступлений, предусмотренных главой 28 УК РФ (преступления в сфере компьютерной информации).
ПК-3.2. Умеет осуществлять проверку сообщений о преступлениях и иных правонарушениях, анализировать и оценивать первичную информацию; обеспечивать сохранность обстановки на месте происшествия, производить неотложные следственные действия и принимать меры к установлению и задержанию правонарушителей.	Уметь осуществлять первоначальную проверку сообщений о преступлениях, предусмотренных главой 28 УК РФ (преступления в сфере компьютерной информации).

Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)	Планируемые результаты обучения по дисциплине
ПК-3.3. Способен осуществлять профессионально-служебную деятельность, направленную на выявление и пресечение правонарушений.	Владеть навыками выявления и пресечения преступлений, предусмотренных главой 28 УК РФ (преступления в сфере компьютерной информации).

3. Содержание, объем дисциплины и формы проведения занятий

№ п/п	Наименование темы дисциплины	Компетенции	Оценочные средства текущего контроля		
			ЗНАТЬ	УМЕТЬ	ВЛАДЕТЬ
			ПК-1.1 ПК-3.1	ПК-1.2 ПК-3.2	ПК-1.3 ПК-3.3
1	Общие вопросы технической защиты информации	ПК-1 ПК-3	Доклад, сообщение/ Реферат №1 (10)	Деловая и (или) ролевая игра/Кейс-задача №1 (20)	Деловая и (или) ролевая игра/Кейс-задача №1 (20)
2	Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах и мероприятия по обеспечению защиты персональных данных	ПК-1 ПК-3	Круглый стол, дискуссия, полемика, дебаты/Эссе №1 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №1 (20)	Круглый стол, дискуссия, полемика, дебаты/Эссе №1 (20)
3	Организационные и технические мероприятия по защите персональных данных в информационных системах	ПК-1 ПК-3	Задача №1 (10)	Задача №1 (10)	Деловая и (или) ролевая игра/Кейс-задача №2 (20)
4	Основы законодательства РФ в области персональных данных	ПК-1 ПК-3	Коллоквиум/ Проект (групповой проект) №1 (20)	Коллоквиум/ Проект (групповой проект) №1 (20)	Деловая и (или) ролевая игра/Кейс-задача №2 (20)
Количество баллов (100 баллов):			100		

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа
Тема 1: Общие вопросы технической защиты информации Основные понятия и определения. Федеральный закон «Об информации, информационных технологиях и о защите информации». Нормативно-правовое обеспечение защиты персональных данных. Международное и национальное право в области защиты персональных данных. Федеральное законодательство Российской Федерации в области защиты персональных данных. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.Требования к материальным носителям биометрических персональных данных. Содержание и основные положения Федерального Закона Российской Федерации «О персональных данных» № 152-ФЗ. Принципы и условия обработки персональных данных. Принципы обработки персональных данных. Категории персональных данных. Права субъекта персональных данных. Обязанности оператора персональных данных **Практические занятия/самостоятельная работа:** Специальные нормативные документы по технической защите сведений конфиденциального характера. **Лабораторная работа:** -
Тема 2: Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах и мероприятия по обеспечению защиты персональных данных Основные принципы моделирования угроз с использованием методических документов ФСТЭК и ФСБ. Угрозы информационной безопасности. Общая характеристика уязвимостей информационной системы персональных данных. Методология формирования модели угроз с использованием Методических рекомендаций ФСБ. Мероприятия по обеспечению защиты персональных данных. Ответственность оператора персональных данных. **Практические занятия/самостоятельная работа:** Система государственного контроля в области персональных данных **Лабораторная работа:** -
Тема 3: Организационные и технические мероприятия по защите персональных данных в информационных системах Порядок организации защиты персональных данных. Меры по обеспечению безопасности персональных данных. Построение системы защиты персональных данных. Подсистемы в составе СЗПДн. Аттестация, сертификация и лицензирование в области защиты персональных данных.

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа
Практические занятия/самостоятельная работа: Контроль в области защиты персональных данных **Лабораторная работа:** -
Тема 4: Основы законодательства РФ в области персональных данных Основы законодательства Российской Федерации в области персональных данных. Основы правового регулирования в сфере персональных данных. **Практические занятия/самостоятельная работа:** Оператор персональных данных. **Лабораторная работа:** -
Курсовая работа: не предусмотрено учебным планом

Очная форма обучения

Вид учебной работы	Всего часов	Семестр 4
Аудиторные занятия (АЗ):	32	32
Лекционные занятия (Лек)	16	16
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	16	16
Самостоятельная работа студента (СР)	69	69
Курсовая работа	0	0
Другие виды самостоятельной работы*	69	69
Контроль самостоятельной работы (КСР)	7	7
Контактная работа (КоР)	39	39
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	Общие вопросы технической защиты информации	4	4	4	0	9	4
2	Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах и мероприятия по обеспечению защиты персональных данных	4	4	4	0	20	4
3	Организационные и технические мероприятия по защите персональных данных в информационных системах	4	4	4	0	20	4
4	Основы законодательства РФ в области персональных данных	4	4	4	0	20	4
	Итого:		16	16	0	69	16

* 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 4
Аудиторные занятия (АЗ):	8	8
Лекционные занятия (Лек)	2	2
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	6	6
Самостоятельная работа студента (СР)	91	91
Курсовая работа	0	0
Другие виды самостоятельной работы*	91	91
Контроль самостоятельной работы (КСР)	5	5

Вид учебной работы	Всего часов	Семестр 4
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	Общие вопросы технической защиты информации	4	0	0	0	21	4
2	Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах и мероприятия по обеспечению защиты персональных данных	4	0	2	0	20	4
3	Организационные и технические мероприятия по защите персональных данных в информационных системах	4	2	2	0	30	4
4	Основы законодательства РФ в области персональных данных	4	0	2	0	20	4
	Итого:		2	6	0	91	16

* 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 4
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	Общие вопросы технической защиты информации	4	2	2	0	26	4
2	Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах и мероприятия по обеспечению защиты персональных данных	4	2	2	0	20	4
3	Организационные и технические мероприятия по защите персональных данных в информационных системах	4	2	2	0	20	4
4	Основы законодательства РФ в области персональных данных	4	2	4	0	20	4
	Итого:		8	10	0	86	16

* 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. ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Учебное пособие для вузов / Корабельников С. М. - Всероссийский государственный университет юстиции (РПА Минюста России) (г. Москва)., 2023 г. - 111 с. - ISBN 978-5-534-12769-0 – Режим доступа: https://urait.ru/book/prestupleniya-v-sfere-informacionnoy-bezopasnosti-519079

2. БЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ 2-е изд., пер. и доп. Учебник для вузов / Шульц В. Л., Юрченко А. В., Рудченко А. Д. ; Под ред. Шульца В.Л. - Национальный исследовательский университет «Высшая школа экономики» (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2023 г. - 585 с. - ISBN 978-5-534-12368-5 – Режим доступа: https://urait.ru/book/bezopasnost-predprinimatelskoy-deyatelnosti-518878

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. ИНФОРМАЦИОННОЕ ПРАВО. Учебник для вузов / Под ред. Ковалевой Н.Н. - Саратовская государственная юридическая академия (г. Саратов).; Московский государственный юридический университет имени О.Е. Кутафина (МГЮА) (г. Москва)., 2023 г. - 353 с. - ISBN 978-5-534-13786-6 – Режим доступа: https://urait.ru/book/informacionnoe-pravo-519753

2. ИНФОРМАЦИОННОЕ ПРАВО. ПРАКТИКУМ. Учебное пособие для вузов / Ковалева Н. Н., Жирнова Н. А., Тугушева Ю. М., Холодная Е. В. ; Под ред. Ковалевой Н.Н. - Саратовская государственная юридическая академия (г. Саратов)., 2023 г. - 159 с. - ISBN 978-5-534-12442-2 – Режим доступа: https://urait.ru/book/informacionnoe-pravo-praktikum-518914

3. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ 3-е изд., пер. и доп. Учебник для вузов / Под общ. ред. Кузнецова П.У. - Уральский государственный юридический университет имени В.Ф. Яковлева (г. Екатеринбург)., 2023 г. - 325 с. - ISBN 978-5-534-02598-9 – Режим доступа: https://urait.ru/book/informacionnye-tehnologii-v-yuridicheskoy-deyatelnosti-510646

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. Наука права [Электронный ресурс] : информационная справочная система . - Режим доступа: https://naukaprava.ru. - Текст: электронный

9. Официальный Интернет-портал правовой информации [Электронный ресурс] : информационная справочная система. - Режим доступа: http://pravo.gov.ru. - Текст: электронный

10. Конституционный Суд РФ [Электронный ресурс] : информационная справочная система . - Режим доступа: http://www.ksrf.ru. - Текст: электронный

11. Государственная автоматизированная система РФ «Правосудие»: профессиональная база данных. - Режим доступа: https://sudrf.ru. - Текст: электронный

12. Гарант: профессиональная база данных . - Режим доступа: https://www.garant.ru/. - Текст: электронный

13. Министерство юстиции Российской Федерации: профессиональная база данных. - Режим доступа: https://minjust.gov.ru/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

Доклад, сообщение/Реферат №1

1. Федеральный закон «Об информации, информационных технологиях и о защите информации».

2. Нормативно-правовое обеспечение защиты персональных данных.

3. Международное и национальное право в области защиты персональных данных.

4. Федеральное законодательство Российской Федерации в области защиты персональных данных.

5. Требования к защите персональных данных при их обработке в информационных системах персональных данных.

6. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

7. Требования к материальным носителям биометрических персональных данных.

8. Содержание и основные положения Федерального Закона Российской Федерации «О персональных данных» № 152-ФЗ.

9. Принципы и условия обработки персональных данных. Принципы обработки персональных данных.

10. Категории персональных данных.

11. Права субъекта персональных данных.

12. Обязанности оператора персональных данных.

13. Специальные нормативные документы по технической защите сведений конфиденциального характера.

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

Мероприятия по обеспечению защиты персональных данных

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

Составление Положения о защите персональных даннных в организации

Задача №1

Заполните таблицу "Меры по обеспечению безопасности персональных данных":

п/н	Состав мер по обеспечению безопасности персональных данных	Содержание мер по обеспечению безопасности персональных данных
1.		
2.		
3.		
….		

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

Дать полную характеристику конкретного признака состава преступления либо полный сравнительный анализ с указанием всех признаков сходства и различия нескольких составов преступлений данной группы.

1. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан.
2. Публичное распространение заведомо ложной общественно значимой информации, повлекшее

тяжкие последствия.

3. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей Преступления в сфере незаконного оборота наркотических средств, психотропных веществ или их аналогов, совершаемые с использованием средств массовой информации или электронных или информационно-телекоммуникационных сетей.
4. Неправомерный доступ к компьютерной информации.
5. Создание, использование и распространение вредоносных компьютерных программ.
6. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Коллоквиум/Проект (групповой проект) №1

1. Информационная безопасность: понятие, основные задачи и методы ее обеспечения;
2. Угрозы информационной безопасности.
3. Государственная политика в сфере информационной безопасности.
4. Источник угрозы информационной безопасности и его виды.
5. Субъект информационной безопасности: понятие, виды.
6. Государственное управление в информационной сфере.
7. Влияние современных условий политического и социально-экономического развития страны на обеспечение информационной безопасности.
8. Основные задачи по обеспечению информационной безопасности.
9. Права граждан в информационной сфере.
10. Государственная тайна.
11. Основные этапы развития преступности в информационной сфере.
12. Понятие и виды преступлений в информационной сфере.
13. Уголовно-правовая характеристика преступлений в информационной сфере.
14. Уголовная ответственность за преступления, совершенные в информационной сфере.
15. Причинный комплекс факторов преступности в информационной сфере.
16. Особенности мотивации преступного поведения в информационной сфере.
17. Условия, формирующие и способствующие совершению преступлений в информационной сфере.
18. Криминологический анализ международного и зарубежного опыта предупреждения преступности в информационной сфере;
19. Меры предупреждения преступности в информационной сфере в современной России;
20. Повышение эффективности предупредительного воздействия уголовного законодательства в отношении преступлений в информационной сфере.
21. Основные направления международного сотрудничества в области обеспечения информационной безопасности.
22. Проблемы взаимодействия Российской Федерации иными с государствами в области

обеспечения информационной безопасности.

23. Количественные показатели преступности в информационной сфере в Уральском федеральном округе и России.
24. Качественные показатели преступности в информационной сфере в Уральском федеральном округе и России
25. Перспективные направления развития в области информационной безопасности

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. Информационная безопасность: понятие, основные задачи и методы ее обеспечения
2. Угрозы информационной безопасности.
3. Государственная политика в сфере информационной безопасности.
4. Источник угрозы информационной безопасности и его виды.
5. Субъект информационной безопасности: понятие, виды.
6. Государственное управление в информационной сфере.
7. Влияние современных условий политического и социально-экономического развития страны на обеспечение информационной безопасности.
8. Основные задачи по обеспечению информационной безопасности.
9. Права граждан в информационной сфере.
10. Государственная тайна.
11. Основные этапы развития преступности в информационной сфере.
12. Понятие и виды преступлений в информационной сфере.
13. Уголовно-правовая характеристика преступлений в информационной сфере.
14. Уголовная ответственность за преступления, совершенные в информационной сфере.
15. Причинный комплекс факторов преступности в информационной сфере.
16. Особенности мотивации преступного поведения в информационной сфере.
17. Условия, формирующие и способствующие совершению преступлений в информационной сфере.
18. Криминологический анализ международного и зарубежного опыта предупреждения преступности в информационной сфере;
19. Меры предупреждения преступности в информационной сфере в современной России;
20. Повышение эффективности предупредительного воздействия уголовного законодательства в отношении преступлений в информационной сфере.
21. Основные направления международного сотрудничества в области обеспечения информационной безопасности.
22. Проблемы взаимодействия Российской Федерации иными с государствами в области

обеспечения информационной безопасности.

23. Количественные показатели преступности в информационной сфере в Уральском федеральном округе и России.
24. Качественные показатели преступности в информационной сфере в Уральском федеральном округе и России.
25. Перспективные направления развития в области информационной безопасности
26. Система и виды преступлений против информационной безопасности.
27. Общая характеристика преступлений против информационной безопасности.
28. Клевета, ее признаки, виды. Отграничение от смежных составов.
29. Посягательство на неприкосновенность частной жизни.
30. Нарушение тайны переписки, телефонных переговоров, почтовых отправлений или иных сообщений.
31. Отказ в предоставлении гражданину информации.
32. Нарушение авторских и смежных прав.
33. Нарушение изобретательских и патентных прав.
34. Разглашение тайны усыновления (удочерения).
35. Мошенничество с использованием электронных средств платежа. Отграничение от смежных составов.
36. Мошенничество в сфере компьютерной информации.
37. Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую, либо банковскую тайн, его виды, отграничение от смежных составов.
38. Злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах.
39. Манипулирование рынком. Его виды.
40. Неправомерное использование инсайдерской информации.

Примерный переченьпрактических заданий к зачету

Заадние 1.
Составить схему методов обеспечения информационной безопасности РФ.
Задание 2.
Дать краткий анализ федеральных законов в области информационной безопасности.
Задание 3.
Подготовьте примерную инструкцию о порядке проведения внутреннего расследования по фактам незаконного получения и разглашения сведений, составляющих коммерческую тайну, нарушения порядка конфиденциального делопроизводства.
Задание 4.
Опишите процедуру получения допуска к сведениям, составляющим государственную тайну.
Задание 5.
Романов П.С. совместно с Носовым М.П. и Козловым Н.П. осуществил установку на банкомате нештатного электронного устройства, предназначенного для негласного получения информации. Устройство способно считывать информацию с магнитных полос пластиковых платежных карт, в том числе индивидуальных номеров банковских карт, т.е. информацию, вводимую посредством

клавиатуры пользователем банкомата, в том числе о ПИН-кодах платежных пластиковых карт.
Является информация, полученная злоумышленниками банковской тайной?
Каковы способы защиты от подобных преступных действий?

Задание 6.

Организация (исполнитель) и банк (абонент) заключили договор о предоставлении услуг сети передачи данных и услуг телематических служб, в частности для подключения банка к сети Интернет. Договором предусмотрено, что абонент не освобождается от оплаты услуг или какой-либо их части исполнителю в случае, если оказание этих услуг вызвано несанкционированным доступом к оборудованию банка третьими лицами. Банк считает, что указанный пункт должен быть признан недействительным, поскольку законодательно абонент не может быть ответственным за неисполнение условий договора по вине третьей стороны.
Правомерна ли позиция банка?