Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
Пермский национальный исследовательский политехнический университет
Образовательный центр г. Когалым

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____А.Б. Петроченков
"29" июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Основы информационной безопасности
Форма обучения	Очная
Уровень высшего образования	Специалист
Общая трудоемкость (час., (ЗЕТ))	108 (3)
Специальность	21.05.06 Нефтегазовые техника и технологии

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель - изучение принципов обеспечения информационной безопасности и защиты информации, подходов к анализу угроз безопасности информационных систем и освоение компетенций для решения основных задач защиты информации в информационных системах

Задачи дисциплины:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации;
- приобретение навыков анализа информационной инфраструктуры с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

1.2. Изучаемые объекты дисциплины

– основные понятия, общеметодологические принципы теории информационной безопасности;
– основы государственной информационной политики по обеспечению безопасности информации Российской Федерации;
– виды информации ограниченного доступа;
– угрозы безопасности информации и уязвимости информационных систем;
– информационные войны и информационное оружие;
– методы нарушения конфиденциальности, целостности и доступности информации;
– причины, виды каналы утечки информации и несанкционированного доступа;
– уровни и сервисы защиты информации;
– правовая защита информации;
– способы и средства защиты информации;
– критерии оценки защищенности объектов критической информационной инфраструктуры;
– основы организации защиты информации на предприятиях нефтегазового комплекса.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине	Индикатор достижения	Средства оценки

		(знать, уметь, владеть)	компетенции, с которым соотнесены планируемые результаты обучения	
ПК-4.2	ИД-1ПК-4.2	Знает профили и особенности работы специализированных предприятий по защите информации, оборудование и средства, предназначенные для обеспечения информационной безопасности	Знает профили и особенности работы сервисных компаний, работающих с конкретным предприятием, применяемое оборудование и материалы	Отчёт по практическому занятию
ПК-4.2	ИД-2ПК-4.2	Умеет взаимодействовать со специализированными предприятиями по защите информации при составлении и корректировке регламентов и проектов в области обеспечения информационной безопасности при управлении технологическими процессами и производствами в нефтегазовой отрасли	Умеет взаимодействовать с сервисными фирмами при составлении и корректировке регламентов по взаимодействию компаний, проектов, связанных с исследованием, разработкой, проектированием, конструированием, реализацией и управлением технологическими процессами и производствами в нефтегазовой отрасли, применять современные энергосберегающие технологии	Отчёт по практическому занятию
ПК-4.2	ИД-3ПК-4.2	Владеет навыками применения основных способов и средств защиты информации при проведении работ по сопровождению технологических процессов нефтегазового производства	Владеет навыками работы по сопровождению технологических процессов нефтегазового производства, в том числе на континентальном шельфе, применения современных энергосберегающих технологий	Отчёт по практическому занятию

ПК-1.3	ИД-1ПК-1.3	Знает преимущества и недостатки применяемых современных технологий и эксплуатации технологического оборудования в условиях актуальных угроз безопасности информации	Знает преимущества и недостатки применяемых современных технологий и эксплуатации технологического оборудования	Отчёт по практическому занятию
ПК-1.3	ИД-2ПК-1.3	Умеет интерпретировать результаты исследований технологических процессов применительно к условиям их защищенности от актуальных угроз безопасности информации	Умеет интерпретировать результаты лабораторных и технологических исследований технологических процессов применительно к конкретным условиям	Отчёт по практическому занятию
ПК-1.3	ИД-3ПК-1.3	Владеет навыками участия в основных работах по реализации политики информационной безопасности при эксплуатации отдельных узлов традиционного оборудования.	Владеет навыками совершенствования отдельных узлов традиционного оборудования, в т.ч. лабораторного (по заданию преподавателя).	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	45	45
- лекции (Л)	18	18
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	25	25
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	63	63

2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет		
Зачет	9	9
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	108	108

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
8-й семестр				
Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере Основные составляющие национальных интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Обеспечение региональной информационной безопасности. Проблемы обеспечения информационной безопасности объектов критической инфраструктуры	2	0	2	7
Основные понятия и общеметодологические принципы теории информационной безопасности Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории	2	0	2	7

информационной безопасности				
Понятие и виды защищаемой информации Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты	2	0	2	7
Понятие и виды угроз информационной безопасности Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации. Уязвимости информационных систем и модель нарушителя. Угрозы безопасности информации объектов критической инфраструктуры предприятий нефтегазового комплекса	2	0	2	7
Информационная безопасность и информационное противоборство Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Информационная война как способ воздействия на информационные системы различного назначения и объекты критической информационной инфраструктуры предприятий нефтегазового комплекса	2	0	2	7
Уровни и сервисы защиты информации в информационных системах Единые критерии безопасности информационных технологий.	2	0	4	7

Законодательный, административный, процедурный уровни информационной безопасности. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.				
Способы и средства защиты информации Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности, DLP, SIEM-системы, SOC-центры. Комплексные решения в обеспечении защиты информации объектов нефтегазового комплекса	2	0	3	7
Правовая защита информации на объектах предприятий нефтегазового комплекса Понятие и структура правовой защиты информации. Основные международные нормы и внутригосударственные нормативно-правовые документы в области обеспечения информационной безопасности. Ответственность за нарушение законодательства в информационной сфере. Основные административные регламенты по обеспечению информационной безопасности объектов информатизации предприятий нефтегазового комплекса	2	0	4	7
Организация защиты информации на объектах информатизации нефтегазового комплекса Сущность организационных мер защиты информации. Организация охраны и режима. Организация работы с персоналом в системе защиты информации. Организация работы с документами. Понятия управления информационной безопасностью. Организация защиты персональных данных и объектов критической информационной инфраструктуры	2	0	4	7

Итого за 8-й семестр	18	0	25	63
Итого по дисциплине	18	0	25	63

Примерная тематика практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере (СЗ)
2	Основные понятия и общеметодологические принципы теории информационной безопасности (СЗ)
3	Определение видов информации ограниченного доступа и состава защищаемой информации (ПЗ)
4	Угрозы безопасности информации и разработка модели угроз информационной безопасности объектов критической информационной инфраструктуры(ПЗ)
5	Информационная безопасность и информационное противоборство (СЗ)
6	Уровни и сервисы защиты информации в информационных системах (СЗ)
7	Применение основных сервисов защиты информации в информационных системах (ПЗ)
8	Способы и средства защиты информации (ПЗ)
9	Особенности правовой защиты информации. Ответственность за нарушение законодательства в информационной сфере (СЗ)
10	Разработка внутренней организационно-распорядительной документации по защите информации на предприятиях нефтегазового комплекса (ПЗ)
11	Организация охраны, режима и работы с персоналом в системе защиты информации объектов нефтегазового комплекса (ПЗ)
12	Организация защиты персональных данных и объектов критической информационной инфраструктуры (ПЗ)

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:
1.Изучение учебной дисциплины должно вестись систематически.
2.После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3.Особое внимание следует уделить выполнению отчетов по практическим занятиям, индивидуальным комплексным заданиям на самостоятельную работу.
4.Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

Не используется

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Основная литература	Ахметова С. Г. Информационная безопасность: учебно-методическое пособие. Пермь: Изд-во ПНИПУ, 2013	https://elib.pstu.ru/Record/RUPNRPUelib3569	сеть Интернет; авторизованный доступ
Основная литература	Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. Москва: Академия, 2008	https://elib.pstu.ru/Record/RUPNRPUelib7500	сеть Интернет; авторизованный доступ
Дополнительная литература	Основы информационной безопасности и защиты информации	https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1	сеть Интернет; авторизованный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения
Лекция	Столы, стулья, стационарный презентационный комплекс
Практическое занятие	Столы, стулья, стационарный презентационный комплекс

8. Фонд оценочных средств дисциплины

Представлен в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
Пермский национальный исследовательский политехнический университет
Образовательный центр г. Когалым

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине "Основы информационной безопасности"

Форма обучения	Очная
Уровень высшего образования	Специалитет
Общая трудоемкость (час., (ЗЕТ))	108 (3)
Специальность	21.05.06 Нефтегазовые техника и технологии
Курс: 4	**Семестр: 8**

Зачет: 8 семестр

Пермь 2023

Общие положения

Фонд оценочных средств (ФОС) для проведения промежуточной аттестации обучающихся по дисциплине "Основы информационной безопасности" является частью (приложением) к рабочей программе дисциплины (РПД). ФОС для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок. ФОС для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД освоение учебного материала дисциплины "Основы информационной безопасности" запланировано в течение одного семестра (8 семестра учебного плана).

Предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций знать, уметь, владеть, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине.

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала и в ходе практических занятий, а также на зачете (табл. 1.1)

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля				
	Текущий		Рубежный		Итоговый
	С	ТО	ОПР	Т	Экзамен
Усвоенные знания					
З.1. Знает профили и особенности работы специализированных предприятий по защите информации, оборудование и средства, предназначенные для обеспечения информационной безопасности	С	ТО	ОПР	Т	ТВ ПЗ КЗ
З.2. Знает преимущества и недостатки применяемых современных технологий и эксплуатации технологического оборудования в условиях актуальных угроз безопасности информации	С	ТО	ОПР	Т	ТВ ПЗ КЗ
Освоенные умения					
У.1. Умеет взаимодействовать со специализированными предприятиями по защите информации при составлении и корректировке регламентов и проектов в области обеспечения информационной безопасности при управлении технологическими процессами и производствами в нефтегазовой отрасли	С	ТО	ОПР	Т	ТВ ПЗ КЗ

У.2. Умеет интерпретировать результаты исследований технологических процессов применительно к условиям их защищенности от актуальных угроз безопасности информации	С	ТО	ОПР	Т	ТВ ПЗ КЗ
Приобретенные владения					
В.1. Владеет навыками применения основных способов и средств защиты информации при проведении работ по сопровождению технологических процессов нефтегазового производства	С	ТО	ОПР	Т	ТВ ПЗ КЗ
В.2. Владеет навыками участия в основных работах по реализации политики информационной безопасности при эксплуатации отдельных узлов традиционного оборудования.	С	ТО	ОПР	Т	ТВ ПЗ КЗ

С - собеседование по теме; ТО - коллоквиум (теоретический опрос); КЗ - кейс-задача (индивидуальное задание); ОЛР - отчет по лабораторной работе; ОПР - отчет по практической работе; Т/КР - рубежное тестирование (контрольная работа); ТВ - теоретический вопрос; ПЗ - практическое задание; КЗ - комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в форме зачета, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучающихся, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с "Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, специалитета и магистратуры в ПНИПУ" предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

– входной контроль с целью контроля исходного уровня подготовленности обучающегося и его соответствия предъявляемым требованиям для изучения данной дисциплины;

– текущий контроль усвоения материала (уровня освоения компонента "знать" заданных компетенций) на каждом аудиторном занятии и контроль посещаемости лекционных занятий;

– промежуточный и рубежный контроль освоения обучающимися отдельных компонентов "знать" и "уметь" заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), рефератов, эссе и т.д.

– рубежный контроль по дисциплине, проводимый на следующей неделе после прохождения каждого теоретического раздела дисциплины, и промежуточный, осуществляемый во время каждого контрольного мероприятия внутри тематического раздела дисциплины;

– межсессионная аттестация с целью единовременного подведения итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

– контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме тестирования или проверки рубежных контрольных работ после изучения каждого тематического модуля учебной дисциплины.

2.2.1 Защита отчетов по практическим занятиям

Всего запланировано 12 практических занятий. Типовые темы практических занятий приведены в РПД.

2.2.2. Рубежное тестирование

Запланировано 2 рубежных тестирований после освоения студентами каждого модуля дисциплины:

– Модуль 1. Методологические основы обеспечения информационной безопасности;

– Модуль 2. Сервисы, способы и средства защиты информации в информационных системах;

– Модуль 3. Основы организации и обеспечения информационной безопасности

1.

Типовые шкалы и критерии оценки результатов рубежной контрольной работы приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль по дисциплине)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются положительная интегральная оценка по результатам текущего и рубежного контроля, а также успешная защита отчетов по всем практическим занятиям.

Промежуточная аттестация в форме зачета по дисциплине проводится по билетам. Билет содержит теоретический вопрос для проверки усвоенных знаний, практическое задание для проверки освоенных умений и комплексное задание для контроля уровня приобретенных владений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали теоретические вопросы и практические задания, контролирующие уровень сформированности всех заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.2. Шкалы оценивания результатов обучения на зачете

Оценка результатов обучения по дисциплине в форме оценки уровня сформированности компонентов "знать", "уметь" и "владеть" заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля в процессе промежуточной аттестации.

Типовые шкала и критерии оценки результатов обучения в процессе промежуточной аттестации для компонентов "знать", "уметь" и "владеть" приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1 Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций путем выборочного контроля в процессе промежуточной аттестации считается, что полученная оценка за компонент проверяемой компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

Правильный ответ	Содержание вопроса	Компетенция
Информационно-телекоммуникационная сеть	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это: 1. База данных 2. Информационная технология 3. Информационная система 4. Информационно-телекоммуникационная сеть 5. Медицинская информационная система	ПК-1.3
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это: 1. Электронное сообщение 2. Распространение информации 3. Предоставление информации 4. Конфиденциальность информации 5. Доступ к информации	ПК-1.3
Распространение информации	Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это: 1. Уничтожение информации 2. Распространение информации 3. Предоставление информации 4. Конфиденциальность информации 5. Доступ к информации	ПК-1.3
Доступ к информации	Возможность получения информации и ее использования это: 1. Сохранение информации 2. Распространение информации 3. Предоставление информации 4. Конфиденциальность информации 5. Доступ к информации	ПК-1.3
Электронное сообщение	Информация, переданная или полученная пользователем информационно-телекоммуникационной сети: 1. Электронное сообщение 2. Информационное сообщение 3. Текстовое сообщение 4. Визуальное сообщение 5. Sms-сообщение	ПК-1.3
«О персональных данных»	Понятие защиты информации определяется федеральным законом: 1. «Об информационной безопасности и защите информации» 2. «О персональных данных» 3. «Об информации, информационных технологиях и	ПК-4.2

	защите информации» 4. «О конфиденциальной информации» 5. «Об утверждении перечня сведений конфиденциального характера»	
Идентификация	Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом: 1. Авторизация 2. Аутентификация 3. Обезличивание 4. Деперсонализация 5. Идентификация	ПК-4.2
Аутентифика́ция	Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации: 1. Авторизация 2. Обезличивание 3. Деперсонализация 4. Аутентифика́ция 5. Идентификация	ПК-4.2
Login	Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название: 1. Токен 2. Password 3. Пароль 4. Login 5. Смарт-карта	ПК-4.2
Шифрование	Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет: 1. Идентификация 2. Аутентификация 3. Авторизация 4. Экспертиза 5. Шифрование	ПК-4.2