

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение  
высшего образования



**Пермский национальный исследовательский  
политехнический университет**

**УТВЕРЖДАЮ**

Проректор по образовательной  
деятельности

 А.Б. Петроченков

« 03 » апреля 20 23 г.

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Дисциплина:** Хранение и защита информации  
(наименование)

**Форма обучения:** очная  
(очная/очно-заочная/заочная)

**Уровень высшего образования:** бакалавриат  
(бакалавриат/специалитет/магистратура)

**Общая трудоёмкость:** 108 (3)  
(часы (ЗЕ))

**Направление подготовки:** 27.03.03 Системный анализ и управление  
(код и наименование направления)

**Направленность:** Информационные технологии и управление в  
нефтегазопереработке и химической промышленности  
(наименование образовательной программы)

## 1. Общие положения

### 1.1. Цели и задачи дисциплины

Цель учебной дисциплины - формирование комплекса знаний, умений и навыков в области основ хранения и защиты информации, необходимых для выполнения видов профессиональной деятельности в рамках обеспечения автоматизированных систем управления химико-технологическими процессами.

Задачи учебной дисциплины:

- изучение
  - понятий, терминов и методологии по хранению и защите информации;
  - получение знаний правовых основ обеспечения безопасности автоматизированных систем;
- формирование умения
  - выполнять анализ защищенности автоматизированных систем;
  - обосновывать выбор средств по хранению и защите информации в автоматизированных системах;
- формирование навыков
  - применения средств по защите информации;
  - работы со средствами хранения и создания резервных копий.

### 1.2. Изучаемые объекты дисциплины

Предметом освоения дисциплины являются следующие объекты: средства хранения и защиты информации в автоматизированных системах.

### 1.3. Входные требования

Не предусмотрены

## 2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
-------------	-------------------	---	--	-----------------

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.3	ИД-1ПК-2.3	Знание требований нормативных правовых актов Российской Федерации, локальных нормативных актов, распорядительных документов и технической документации в области эксплуатации программного обеспечения средств АСУТП; средств защиты программного обеспечения в компьютерных системах; программного обеспечения и платформ инфраструктуры средств АСУТП; требований информационной безопасности программного обеспечения средств АСУТП; методы управления требованиями;	Знает методы управления требованиями; методы моделирования архитектуры программной системы; методы проектирования архитектуры программной системы	Зачет
ПК-2.3	ИД-2ПК-2.3	Умение проверять требования с точки зрения их соответствия архитектуре программной системы; проводить аудит систем безопасности программного обеспечения средств АСУТП с использованием регламентов по защите информации; проводить резервное архивирование баз данных; проверять резервирование серверов операционных систем; проводить диагностику локальной сети и коммутируемых каналов связи; выявлять и осуществлять удаление вредоносного кода в программном обеспечении средств	Умеет проверять требования с точки зрения их соответствия архитектуре программной системы; выявлять требования к архитектуре программной системы путем проведения интервью с заинтересованными сторонами; формулировать архитектурные требования к программной системе.	Защита лабораторной работы

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		АСУТП; выявлять отклонения в работоспособности системы, разграничения прав доступа к ресурсам системы; идентифицировать опасности и оценивать риски при выполнении работ по техническому обслуживанию программного обеспечения средств АСУТП;		
ПК-2.3	ИД-3ПК-2.3	Владение навыками выявления несоответствий требований заказчика к программной системе с точки зрения архитектуры; принятия мер по восстановлению параметров работы программного обеспечения средств АСУТП; создания резервных копий операционных систем и баз данных АСУТП ; восстановления данных из резервных копий программного обеспечения средств АСУТП;	Владеет навыками выявления несоответствий требований заказчика к программной системе с точки зрения архитектуры; описания требований к программной системе с точки зрения архитектуры	Защита лабораторной работы

### 3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		6	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	50	50	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	24	24	
- лабораторные работы (ЛР)	24	24	
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)			
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	58	58	
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
6-й семестр				
Основные понятия из области хранения информации	2	0	0	4
ранение информации. Способы хранения информации. Понятие данных. Понятие базы данных (БД). БД как техническое решение для хранения информации. Документальные, фактографические, мультимедийные БД. Нормативные правовые акты РФ в области хранения и защиты информации.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Средства хранения и резервирования информации	4	8	0	8
Оборудование для хранения данных. Устройства прямого доступа. Иерархия устройств хранения данных. Наборы данных. Понятие файловой системы. Способы организации файловых систем. Записеориентированные файловые системы и файлы прямого доступа. Потокориентированные файловые системы. Многотомные файлы. Иерархические файловые системы. Резервное копирование. Сжатие (упаковка) данных. Архитектура для построения централизованных хранилищ данных большой ёмкости. Особенности архитектуры. Аппаратные средства хранения данных. Понятие RAID-массива. Уровни RAID. Шифрование информации. Аппаратные и программные средства шифрования.				
Угрозы информационной безопасности	2	0	0	8
Виды ущерба в области информационной безопасности. Естественные угрозы информации. Искусственные угрозы информации. Понятие вредоносной программы. Классификация вредоносных программ. Сетевые угрозы.				
Средства защиты информации	4	4	0	10
Защита информации как процесс управления рисками. Виды средств защиты информации. Программное обеспечение для защиты информации. Антивирусы. Системы обнаружения вторжения. Системы предотвращения вторжений. Средства сетевой защиты. Виртуальная частная сеть. Межсетевой экран. Демилитаризованная зона. Сетевые сканеры безопасности.				
Методы выявления уязвимостей	4	4	0	8
Основные приемы выявления уязвимостей. Выявление известных уязвимостей. Системы анализа защищенности. Способы сбора информации о сети. Анализ сетевого трафика. Аудит безопасности. Ведение журнала.				
Организационные меры обеспечения информационной безопасности	4	4	0	8
Понятие системы обеспечения безопасности. Мероприятия для управления информационной безопасностью. Организационная структура системы обеспечения безопасности. Политика безопасности организации. Регламентация работ по защите информации. Аутентификация и идентификация. Технология единого входа. Разграничение доступа. Экономическая оценка затрат на организацию защитных мер.				
Особенности АСУ ТП в области защиты	4	4	0	12

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Понятие информационной системы. Понятие автоматизированных систем управления. Классификация информационных систем. Уязвимости автоматизированных систем управления. Средства защиты автоматизированных систем управления. Требования информационной безопасности в АСУ ТП.				
ИТОГО по 6-му семестру	24	24	0	58
ИТОГО по дисциплине	24	24	0	58

### Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Резервное копирование операционных систем и компьютерной информации
2	Администрирование сети и разграничение прав доступа
3	Анализ журналов работы операционных систем
4	Организация работы виртуальной частной сети (VPN)
5	Организация и настройка системы единого входа (SSO)
6	Анализ сетевого трафика
7	Обнаружение вредоносного программного обеспечения

## 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 принятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

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, лабораторным работам и 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

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
<b>1. Основная литература</b>		
1	Бондарев В. В. Введение в информационную безопасность автоматизированных систем : учебник. Москва : Изд-во МГТУ им. Н. Э. Баумана, 2016. 250 с. 15,75 усл. печ. л.	2
2	От хранения данных к управлению информацией : учебник для вузов пер. с англ. 2-е изд. Санкт-Петербург [и др.] : Питер, 2016. 543 с. 43,86 усл. печ. л.	11

<b>2. Дополнительная литература</b>		
<b>2.1. Учебные и научные издания</b>		
1	Kali Linux. Тестирование на проникновение и безопасность : пер. с англ. / Парасрам Ш., Замм А., Хериянто Т., Али Ш. Санкт-Петербург [и др.] : Питер, 2021. 446 с. 36,120 усл. печ. л.	1
2	Введение в криптографию : учебник / Яценко В. В., Варновский Н. П., Нестеренко Ю. В., Кабатянский Г. А. Санкт-Петербург Москва : Питер : Изд-во МЦНМО, 2001. 287 с.	17
3	Шелупанов А. А., Смолина А. Р. Форензика. Теория и практика расследования киберпреступлений : монография. Москва : Горячая линия-Телеком, 2021. 103 с.	3
<b>2.2. Периодические издания</b>		
1	Безопасность информационных технологий : научный журнал. Москва : Изд-во МИФИ, 1994 - .	
2	Проблемы передачи информации : журнал. Москва : Наука, 1965 - .	
3	Промышленность и безопасность : специализированный журнал. Офиц. изд. Пермь : Горизонт-Прикамье, 2009.	
<b>2.3. Нормативно-технические издания</b>		
	Не используется	
<b>3. Методические указания для студентов по освоению дисциплины</b>		
	Не используется	
<b>4. Учебно-методическое обеспечение самостоятельной работы студента</b>		
	Не используется	

## 6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	ГОСТ 7.32-2017 СИБИД. Отчет о научно-исследовательской работе. Структура и правила оформления (с Поправками)	<a href="http://docs.cntd.ru/document/1200157208">http://docs.cntd.ru/document/1200157208</a>	сеть Интернет; авторизованный доступ
Дополнительная литература	ГОСТ Р 50922-2006. Защита информации. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	<a href="http://325290.inkip.ru/docs/d?nd=1200058320&amp;point=mark=31FJ9303VVVVVC112GRLQ07B">http://325290.inkip.ru/docs/d?nd=1200058320&amp;point=mark=31FJ9303VVVVVC112GRLQ07B</a>	сеть Интернет; свободный доступ
Дополнительная литература	Ушмаева Н. В. Защита информации : учебно-методическое пособие / Ушмаева Н. В. - Тольятти: ТГУ, 2012	<a href="http://elib.pstu.ru/vufind/Record/lanRU-LAN-BOOK-140164">http://elib.pstu.ru/vufind/Record/lanRU-LAN-BOOK-140164</a>	сеть Интернет; авторизованный доступ
Основная литература	Бондарев В. В. Анализ защищенности и мониторинг компьютерных сетей?. Методы и средства. Москва : МГТУ им. Баумана, 2017. 228 с.	<a href="https://elib.pstu.ru/Record/lanRU-LAN-BOOK-103518">https://elib.pstu.ru/Record/lanRU-LAN-BOOK-103518</a>	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	VMware Workstation Player ( VMware Academic)
Прикладное программное обеспечение общего назначения	Wireshark
Системы управления проектами, исследованиями, разработкой, проектированием, моделированием и внедрением	EVE NG Community Edition (Free Edition)

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

Наименование	Ссылка на информационный ресурс
Научная библиотека Пермского национального исследовательского политехнического университета	<a href="http://lib.pstu.ru/">http://lib.pstu.ru/</a>
Электронно-библиотечная система Лань	<a href="https://e.lanbook.com/">https://e.lanbook.com/</a>
Электронно-библиотечная система IPRbooks	<a href="http://www.iprbookshop.ru/">http://www.iprbookshop.ru/</a>
Информационные ресурсы Сети КонсультантПлюс	<a href="http://www.consultant.ru/">http://www.consultant.ru/</a>
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	<a href="https://техэксперт.сайт/">https://техэксперт.сайт/</a>

### **7. Материально-техническое обеспечение образовательного процесса по дисциплине**

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	Проектор, экран настенный; маркерная доска, компьютерные столы (10 шт.), персональные компьютеры (10 шт.)	1
Лекция	Доска, парты, стол преподавателя, проектор	25

### **8. Фонд оценочных средств дисциплины**

Описан в отдельном документе
------------------------------

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение  
высшего профессионального образования  
«Пермский национальный исследовательский политехнический  
университет»

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**  
для проведения промежуточной аттестации обучающихся по дисциплине  
«Хранение и защита информации»  
*Приложение к рабочей программе дисциплины*

<b>Направление подготовки:</b>	27.03.03 Системный анализ и управление
<b>Направленность (профиль) образовательной программы:</b>	Информационные технологии и управление в нефтегазопереработке и химической промышленности
<b>Квалификация выпускника:</b>	бакалавр
<b>Выпускающая кафедра:</b>	Оборудование и автоматизация химических производств
<b>Форма обучения:</b>	очная/заочная
<b>Курс:</b> <u>3</u>	<b>Семестр(ы):</b> <u>6</u>
<b>Трудоёмкость:</b>	
Кредитов по рабочему учебному плану:	<u>3</u> ЗЕ
Часов по рабочему учебному плану:	<u>106</u> ч
<b>Форма промежуточной аттестации:</b>	
Зачет:	6 семестр

Пермь 2023 г.

**Фонд оценочных средств** для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств 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. Фонд оценочных средств 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 рабочей программы дисциплины (РПД) освоение учебного материала дисциплины запланировано в течение одного семестра (6-го семестра учебного плана) и разбито на 7 учебных модуля. В каждом модуле предусмотрены аудиторские лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (таблица 1).

Контроль уровня усвоенных знаний, усвоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, выполнении заданий на практических занятиях, сдаче отчетов по лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.

Таблица 1 – Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля					
	Текущий		Рубежный		Итоговый	
	С	ТО	ОЛР	Т/КР		Зачёт
<b>Усвоенные знания</b>						
<b>З1.</b> Знание требований нормативных правовых актов Российской Федерации, локальных нормативных актов, распорядительных документов и технической документации в области эксплуатации программного обеспечения средств АСУТП;		+				ТВ
<b>З1.</b> знать средств защиты программного обеспечения в компьютерных системах;	+			+		ТВ
<b>З3.</b> знать программное обеспечение и платформы инфраструктуры средств АСУТП;	+					ТВ
<b>З4.</b> знать требований информационной безопасности программного обеспечения средств АСУТП;		+		+		ТВ
<b>З5.</b> знать методов управления требованиями;	+					ТВ
<b>Освоенные умения</b>						
<b>У.1</b> Умение проверять требования с точки зрения их соответствия архитектуре программной системы;			+			ОЛР
<b>У.2</b> уметь проводить аудит систем безопасности программного обеспечения средств АСУТП с использованием регламентов по защите информации;			+			ОЛР

У.3. уметь проводить резервное архивирование баз данных;			+			ОЛР
У.4. уметь проверять резервирование серверов операционных систем;			+			ОЛР
У.5. уметь проводить диагностику локальной сети и коммутируемых каналов связи;			+			ОЛР
У.5. уметь выявлять и осуществлять удаление вредоносного кода в программном обеспечении средств АСУТП;			+			ОЛР
У.6. уметь выявлять отклонения в работоспособности системы, разграничения прав доступа к ресурсам системы;			+			ОЛР
У.7. уметь идентифицировать опасности и оценивать риски при выполнении работ по техническому обслуживанию программного обеспечения средств АСУТП			+			ОЛР
<b>Приобретенные владения</b>						
В.1 владеть навыками выявления несоответствий требований заказчика к программной системе с точки зрения архитектуры;			+			ОЛР
В.2 владеть навыками принятия мер по восстановлению параметров работы программного обеспечения средств АСУТП;			+			ОЛР
В.3 владеть навыками создания резервных копий операционных систем и баз данных АСУТП ;			+			ОЛР
В.4 владеть навыками восстановления данных из резервных копий программного обеспечения средств АСУТП;			+			ОЛР

*С – собеседование по теме; ТО – теоретический опрос; ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование/контрольная работа; ТВ – теоретический вопрос; ПЗ – практическое задание;*

Итоговой оценкой освоения дисциплинарных компетенций (результатов обучения по дисциплине) является промежуточная аттестация по дисциплине в виде 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 обучаемых, 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, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;

- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение 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 проводится по каждой теме в форме собеседования или выборочного теоретического опроса студентов. Результаты по 4-х 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, усвоенных умений и приобретенных владений (таблица 1) проводится в форме выполнения и защиты лабораторных работ и рубежных контрольных работ (после изучения каждого модуля учебной дисциплины).

### **2.2.1 Выполнение и защита лабораторных работ**

Всего запланировано 7 лабораторных работ. Темы лабораторных работ приведены в РПД. Защита лабораторной работы проводится индивидуально каждым студентом.

*Типовые шкалы и критерии оценки приведены в общей части ФОС образовательной программы.*

### **2.2.2 Рубежная контрольная работа**

Согласно РПД запланировано три рубежные контрольные работы после освоения студентами учебных модулей дисциплины. Контрольная работа по разделам 2, 4 (КР1), контрольная работа по разделу 6 (КР2). Некоторые типовые вопросы к контрольным работам приведены ниже.

*Типовые вопросы к КР1:*

1. Какие методы защиты информации, использовались в древнее время и в Средние века?
2. Каковы отличия формального и неформального подходов к проблемам защиты информации?
3. Каковы основные принципы построения систем защиты информации?
4. Какова взаимосвязь различных средств защиты информации? Есть ли среди них приоритетные?

5. Каковы основные средства реализации комплексной системы защиты информации?
6. Приведите примеры формальных и неформальных средств защиты?

*Типовые вопросы к КР 2:*

1. Какова структура государственной системы защиты информации?
2. Кто несет ответственность за нарушение режима защиты информации?
3. Каковы основные цели защиты информации?
4. Перечислите основные организационные меры по защите информации на промышленных предприятиях.

*Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.*

### **2.3 Промежуточная аттестация (итоговый контроль)**

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

#### **2.3.1. Процедура промежуточной аттестации без дополнительного аттестационного испытания**

Промежуточная аттестация проводится в форме зачета. Зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине.

Критерии выведения итоговой оценки за компоненты компетенций при проведении промежуточной аттестации в виде зачета приведены в общей части ФОС образовательной программы.

#### **2.3.2. Процедура промежуточной аттестации с проведением аттестационного испытания**

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде зачета по дисциплине может проводиться с проведением аттестационного испытания по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки усвоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности *всех* заявленных компетенций.

##### **2.3.2.1. Типовые вопросы и задания для зачета по дисциплине**

**Типовые вопросы для контроля усвоенных знаний:**

1. Сформулируйте понятия и основные составляющие информационной безопасности

2. Обоснуйте важность проблемы компьютерной информационной безопасности
3. Наиболее распространенные угрозы, пути и каналы утечки информации
4. Сформулируйте понятие «Вредоносные программы (вирусы)». Классификация компьютерных вирусов
5. Сформулируйте понятие законодательного уровня информационной безопасности
6. Обоснуйте важность законодательного уровня информационной безопасности
7. Критерии безопасности компьютерных систем
8. Основные понятия в области лицензирования и сертификации
9. Сформулируйте текущее состояние российского законодательства в области информационной безопасности
10. В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?
11. Объясните порядок оформления и получения лицензий в области информационной безопасности
12. Обоснуйте причины отказа в получении лицензии
13. Назовите методы защиты информации
14. Сформулируйте понятие «Идентификация пользователей». Классификация методов идентификации пользователей
15. Сформулируйте понятия и дайте характеристику «аутентификация пользователей», «парольная аутентификация»
16. Дайте определение понятиям «Управление доступом, ограничение, разграничение, разделение доступа к информации» и сформулируйте их основные характеристики
17. Сформулируйте преимущества и недостатки метода криптографического преобразования информации
18. Экранирование. Классификация межсетевых экранов
19. Основные технологии построения защищенных информационных систем
20. Обеспечение информационной безопасности в АСУ

### **Типовые вопросы и практические задания для контроля приобретенных умений**

1. Назовите основные правила защиты от компьютерных вирусов
2. Сформулируйте достоинства и недостатки современных антивирусных программ
3. Сформулируйте виды противников или «нарушителей» информационной безопасности
4. Виды возможных нарушений информационной системы в АСУ
5. Назовите методы защиты информации

### **Типовые задания для контроля приобретенных владений:**

1. Произведите расчет времени подбора пароля брутфорсом, с предложенными требованиями
2. Проведите анализ защищенности предложенной системы на возможные организационные уязвимости
3. Проведите анализ защищенности предложенной системы на возможные программные уязвимости

### **2.3.2.2. Шкалы оценивания результатов обучения на зачете**

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания.

Типовые шкала и критерии оценки результатов обучения при сдаче зачета 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 в рамках выборочного контроля при зачете считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины.*

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

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

При формировании итоговой оценки промежуточной аттестации в виде зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.