

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

« 29 » августа 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Информационная безопасность в банковской системе
(наименование)

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

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

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 10.04.01 Информационная безопасность
(код и наименование направления)

Направленность: Комплексные системы информационной безопасности
(наименование образовательной программы)

1. Общие положения

1.1. Цели и задачи дисциплины

Цель дисциплины – освоение дисциплинарных компетенций по применению комплекса мероприятий по защиты информации на основе реализации требований к информационной безопасности в банковской системе.

Задачи дисциплины:

- изучение основных положений, понятий и категорий теоретических основ функционирования систем информационной безопасности в банковской системе;
- изучение основ и принципов организации современных проблем организационного обеспечения информационной безопасности;
- изучение организации работы и порядка применения терминологии организационного обеспечения информационной безопасности;
- изучение целей систем организационной защиты информации в банковской системе;
- изучение основных направлений и методов организационной защиты информации в банковской системе, формирование умений в разработке проектов функционирования систем организационной защиты информации в банковской системе;
- формирование навыков работы в организации процессов управления системами организационной защиты информации в банковской системе.

1.2. Изучаемые объекты дисциплины

- правовые основы защиты банковской тайны;
- правовая основа и порядок допуска и доступа к информации ограниченного доступа в банковской системе;
- система правовой ответственности за правонарушения в сфере банковского обслуживания;
- правовые основы деятельности подразделений защиты информации в банковской системе;
- порядок организации охраны объектов информатизации, внутриобъектового и пропускного режима в банковской системе;
- организация работы с персоналом по вопросам защиты информации;
- организация защиты информации в автоматизированных банковских системах;
- организация деятельности службы безопасности в банковской системе.

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
ПК-1.2	ИД-1ПК-1.2	Знает нормативные правовые акты в области защиты информации в банковской системе.	Знает нормативные правовые акты в области защиты информации.	Отчёт по практическом у занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-1.2	ИД-2ПК-1.2	Умеет анализировать автоматизированную банковскую систему с целью определения уровня защищенности и доверия	Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия	Защита лабораторной работы
ПК-1.2	ИД-3ПК-1.2	Владеет навыками выработки предложений по устранению выявленных уязвимостей в автоматизированной банковской системе	Владеет навыками выработки предложений по устранению выявленных уязвимостей	Защита лабораторной работы
ПК-3.1	ИД-1ПК-3.1	Знает принципы построения систем защиты информации банковских систем.	Знает принципы построения систем защиты информации компьютерных систем, в том числе антивирусного программного обеспечения; принципы и методы проектирования программно-аппаратного обеспечения.	Отчёт по практическому занятию
ПК-3.1	ИД-2ПК-3.1	Умеет применять отраслевые стандарты Банка России в области защиты информации в банковской системе.	Умеет проводить исследование с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации; Применять отечественные стандарты в области защиты информации для проектирования средств защиты информации компьютерной системы; разрабатывать архитектуру и интерфейсы средств защиты информации, процедуры восстановления работоспособности средств и систем защиты после сбоев.	Защита лабораторной работы
ПК-3.1	ИД-3ПК-3.1	Владеет навыками подборки методических материалов по программным и аппаратным средствам и способам защиты информации, в банковской системе	Владеет навыками подборки общения научно-технической литературы, методических материалов по программным и аппаратным средствам и способам защиты информации, в том числе на английском языке	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		4	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	42	42	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	12	12	
- лабораторные работы (ЛР)	12	12	
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	16	16	
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	102	102	
2. Промежуточная аттестация			
Экзамен			
Дифференцированный зачет	9	9	
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	144	144	

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
4-й семестр				
Введение в дисциплину	2	0	2	13
Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке специалистов по защите информации. Особенности формирования терминологии научной дисциплины. Взаимосвязь курса с правовыми, историческими, экономическими, социальными, социально-психологическими и техническими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Общие понятия об информационных технологиях	2	2	2	13
Аппаратное и программное обеспечение вычислительной техники, информационные процессы и информационные технологии. Системное и прикладное программное обеспечение, понятие информационных ресурсов (объектов) и пользователей данных ресурсов (субъектов). Основные функции операционной системы ПЭВМ, встроенные возможности разграничения доступа, блокировка доступа к рабочей станции. Идентификация и аутентификация пользователей автоматизированных систем, понятие учетных записей, полномочия администраторов и пользователей систем (привилегии, роли), автоматическая блокировка/разблокировка учетных записей. Использование паролей, понятие структуры пароля, правила выбора стойких паролей, подбор паролей с использованием специализированных программ. Использование локально-вычислительных сетей, понятие сетевых ресурсов, изолированность сегментов локально-вычислительных сетей, разграничение прав доступа к сетевым ресурсам (на примере сети Windows), анализ системных журналов, резервирование и архивирование данных.				
Средства криптографической защиты информации в банковской системе	0	2	2	13
Шифрование данных при хранении и передачи (симметричное/асимметричное шифрование). Понятие электронно-цифровой подписи, цифровых сертификатов, описание механизмов аутентификации. Средства криптографической защиты информации в банковской системе.				
Основные понятия информационной безопасности	2	2	2	13
Политика безопасности в системе, критичные информационные ресурсы. Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия. Понятие целостности и лицензионной чистоты программного обеспечения.				
Исторические аспекты банковского дела	2	0	2	13
Ростовщики. Трапезиты. История банков в России. Виды банков. Функции банков. Правовое регулирование банковской деятельностью.				
Автоматизированные банковские системы	2	2	2	12
Особенности автоматизированных банковских систем, используемых в российских банках. Информационное обеспечение автоматизированных банковских систем.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Техническое оснащение современных автоматизированных банковских систем. Программное обеспечение автоматизированных банковских систем.				
Пластиковые карты, электронные деньги.	0	2	2	12
История развития пластиковых карт. История банковских карт в России. Виды электронных денег и их применение.				
Реализация требований информационной безопасности в системе Банка России.	2	2	2	13
Основные направления политики информационной безопасности и нормативная база Банка России. Стандарты Банка России. Применяемые в ТУ Банка России меры и средства защиты информации, функции администраторов информационной безопасности подразделений. Особенности использования средств защиты информации от несанкционированного доступа. Организация бесперебойного функционирования информационных систем.				
ИТОГО по 4-му семестру	12	12	16	102
ИТОГО по дисциплине	12	12	16	102

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Особенности формирования терминологии учебной дисциплины
2	Управление пользователями и группами в ОС Windows 7/8/.
3	Средства криптографической защиты информации
4	Основные понятия информационной безопасности в банковской системе
5	Исторические аспекты ведения банковского дела.
6	Автоматизированные банковские системы
7	Применение электронных банковских карт и расчетов в электронной форме
8	Реализация требований информационной безопасности в системе Банка России

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Идентификация и аутентификация пользователей автоматизированных систем, блокировка/разблокировка учетных записей.

№ п.п.	Наименование темы лабораторной работы
2	Создание электронной подписи, работа с цифровыми сертификатами.
3	Разграничение доступа к ресурсам, обеспечение целостность и лицензионная чистоты программного обеспечения.
4	Программное обеспечение автоматизированных банковских систем, установка и настройка.
5	Работа с программным обеспечением для электронных банковских карт.
6	Работа с программным обеспечением в должности администратора информационной безопасности.

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

<p>Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой 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 установления связей с ранее освоенным материалом.</p> <p>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.</p> <p>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.</p> <p>При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.</p>
--

5.2. Методические указания для обучающихся по изучению дисциплины

<p>При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:</p> <ol style="list-style-type: none"> 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
1. Основная литература		
1	Автоматизированные информационные технологии в экономике : учебник для вузов / М. И. Семенов [и др.]. - Москва: Финансы и статистика, 2002.	4
2	Васин С. М. Управление рисками на предприятии : учебное пособие для вузов / С.М. Васин, В.С. Шутов. - Москва: КНОРУС, 2010.	7
3	Гамза В. А Безопасность банковской деятельности : учебник для бакалавров / В. А Гамза, И. Б. Ткачук, И. М. Жилкин. - Москва: Юрайт, 2014.	3
4	Деднев М. А. Защита информации в банковском деле и электронном бизнесе / М. А. Деднев, Д. В. Дыльнов, М. А. Иванов. - Москва: КУДИЦ-ОБРАЗ, 2004.	3
5	Экономическая безопасность России. Общий курс : учебник / В. К. Сенчагов [и др.]. - Москва: БИНОМ. Лаб. знаний, 2010.	5
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Информационная безопасность и защита информации : учебное пособие для вузов / Ю. Ю. Громов [и др.]. - Старый Оскол: ТНТ, 2010.	5
2	Ярочкин В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. - Москва: Акад. проект, 2008.	21
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	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	Ю. И. Селиверстов Организация безопасности в банке : Учебное пособие / Ю. И. Селиверстов. - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2013.	http://elib.pstu.ru/Record/iprbooks85956	сеть Интернет; свободный доступ

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

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Adobe Acrobat Reader DC. бесплатное ПО просмотра PDF
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
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечная система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Электронно-библиотечная система ЮРАЙТ	https://biblio-online.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	Количество единиц
Лабораторная работа	Персональный компьютер	10
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный компьютер	10

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**для проведения промежуточной аттестации обучающихся по дисциплине
«Информационная безопасность в банковской системе»
*Приложение к рабочей программе дисциплины***

Направление подготовки: 10.04.01 Информационная безопасность

**Направленность (профиль)
образовательной программы:** Комплексные системы информационной
безопасности

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 2 **Семестр:** 4

Трудоёмкость:

Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:

Зачёт: 3 семестр

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 РПД освоение учебного материала дисциплины запланировано в течение одного семестра (3-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторские лекционные, практические 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 (табл. 1.1).

Контроль уровня усвоенных знаний, усвоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам зачета. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля					
	Текущий		Рубежный		Итоговый	
	С	ТО	ОЛР	Т/КР		Зачёт
Усвоенные знания						
Знать основы законодательства российской банковской системы, организации деятельности центрального банка Российской Федерации по защите информации.	С	ТО1	ПЗ1			КЗ
Знать теоретические основы функционирования систем информационной безопасности в банковской системе, ее современные проблемы и терминологию.	С	ТО2	ПЗ2			КЗ
Знать цели, функции и процессы управления системами информационной безопасности в банковской системе.	С	ТО3	ПЗ3			КЗ
Освоенные умения						
Уметь организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней.	С	ТО1	ПЗ2			КЗ
Уметь разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в банковской системе.	С	ТО2	ПЗ2			КЗ
Уметь организовывать охрану персонала, территорий, зданий, помещений банков.	С	ТО3	ПЗ3			КЗ

Приобретенные владения						
В.1 Владеть навыками организации доступа к объектам информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации в банковской системе.	С	ТО2	ПЗ4			КЗ
Владеть навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности в банковской системе.	С	ТО3	ПЗ5			КЗ

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

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде зачета, проводимая с учётом 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 бланчного 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 материалов 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.

Вопросы для самостоятельного изучения:

Тема 1.1: Перспективы развития законодательства в области информационной безопасности.

Тема 2.1: Шифрование данных при хранении и передаче (симметричное/асимметричное шифрование).

Тема 2.2: Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия.

Тема 3.1: Правовое регулирование банковской деятельностью.

Тема 3.2: Информационное и техническое обеспечение автоматизированных банковских систем.

Тема 3.3: Виды электронных денег и их применение. Банкоматы.

Тема 3.4: Стандарты Банка России.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 5 практических занятий. Темы практических занятий приведены в РПД.

Отчет по выполнению практического задания проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Выполнение комплексного индивидуального задания на самостоятельную работу

Для оценивания навыков и опыта деятельности (владения), как результата обучения по дисциплине, не имеющей курсового проекта или работы, может быть использовано индивидуальное комплексное задание студенту.

Типовые шкала и критерии оценки результатов защиты индивидуального комплексного задания приведены в общей части ФОС образовательной программы.

2.4. 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.

2.4.1. 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.

2.4.2. 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 освоенных 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.

2.4.2.1. Типовые вопросы и задания для зачета по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Понятие операционной системы ПЭВМ
2. Встроенные возможности операционной системы, блокировка доступа к рабочей станции.
3. Идентификация и аутентификация пользователей автоматизированных систем
4. Учетные записи, полномочия администраторов и пользователей систем (привилегии, роли)
5. Специализированные программы по подбору паролей, правила выбора стойких паролей.
6. Разграничение прав доступа к сетевым ресурсам.
7. Анализ системных журналов.
8. Резервирование и архивирование данных.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Управление пользователями и группами в ОС Windows 2000/XP/2003/Vista/7/8/10/11.
2. Система разграничения доступа к локальным и сетевым ресурсам в ОС Windows 2000/XP/2003/Vista/7/8/10/11.
3. Сетевые атаки.
4. Средства защиты информации от несанкционированного доступа (на примере СЗИ от НСД «Аккорд»).
5. Работа «Аккорд» с моделированием случаев НСД, нарушением целостности и запуском несанкционированного ПО.

2.4.2.2. 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.