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 автоматизированных банковских систем
(наименование)

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

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

Общая трудоёмкость: 288 (8)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем (СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

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

Задачи дисциплины:

- изучение основных положений, понятий и категорий теоретических основ функционирования систем информационной безопасности автоматизированных банковских систем;
- 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 автоматизированных банковских систем;
- изучение основных направлений и методов организационной защиты информации автоматизированных банковских систем, формирование умений в разработке проектов функционирования систем организационной защиты информации автоматизированных банковских систем;
- формирование навыков работы в организации процессов управления системами организационной защиты информации автоматизированных банковских систем.

1.2. Изучаемые объекты дисциплины

- методы правовой защиты информации в автоматизированных банковских системах;
- правовые основы защиты персональных данных в автоматизированных банковских системах;
- правовые основы деятельности подразделений защиты информации автоматизированных банковских систем;
- порядок организации охраны объектов информатизации, внутриобъектового и пропускного режима автоматизированных банковских систем;
- организация работы с персоналом по вопросам защиты информации в банковской сфере;
- организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам в банковской сфере;
- организация деятельности службы безопасности в банковской сфере.

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-2.2	ИД-1ПК-2.2	Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации в автоматизированных банковских системах.	Знает критерии оценки защищенности объекта информатизации; технические средства контроля эффективности мер защиты информации; методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.	Отчёт по практическому занятию
ПК-2.2	ИД-2ПК-2.2	Умеет осуществлять контроль обеспечения уровня защищенности автоматизированных банковских систем	Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации	Защита лабораторной работы
ПК-2.2	ИД-3ПК-2.2	Владеет навыками оценки защищенности автоматизированных банковских систем с помощью типовых программных средств	Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		10	11
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	126	72	54
- лекции (Л)	60	36	24
- лабораторные работы (ЛР)	32	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	30	18	12
- контроль самостоятельной работы (КСР)	4	2	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	126	72	54
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет	9		9
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	288	180	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
10-й семестр				
Введение	2	0	0	0
Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке специалистов по защите информации.				
Общие понятия об информационных технологиях	10	4	4	20
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 использование специализированных программ. Использование локально-вычислительных сетей, понятие сетевых ресурсов, изолированность сегментов локально-вычислительных сетей, разграничение прав доступа к сетевым ресурсам (на примере сети в Windows и Linux), анализ системных журналов, резервирование и архивирование данных.				
Обеспечение информационной безопасности и защита автоматизированных систем	12	8	10	30
Шифрование данных при хранении и передачи (симметричное/асимметричное шифрование). Понятие электронной подписи, цифровых сертификатов, описание механизмов аутентификации. Политика безопасности в системе, критичные информационные ресурсы. Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия. Понятие целостности и лицензионной чистоты программного обеспечения.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Информационная безопасность в системе Банка России. История банковского дела. Автоматизированные банковские системы.	12	4	4	22
Ростовщики. Трапезиты. История банков в России. Виды банков. Функции банков. Правовое регулирование банковской деятельностью. Особенности автоматизированных банковских систем, используемых в российских банках. Информационное обеспечение автоматизированных банковских систем. Техническое оснащение современных автоматизированных банковских систем. Программное обеспечение автоматизированных банковских систем.				
ИТОГО по 10-му семестру	36	16	18	72
11-й семестр				
Информационная безопасности финансовой сферы. Пластиковые карты, электронные деньги. Реализация требований информационной безопасности в системе Банка России.	24	16	12	54
История развития Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (далее – ФинЦЕРТ). Цели и задачи ФинЦЕРТ. Основные направления деятельности центра. Автоматизация информационного обмена. Социальная инженерия. Борьба с СМС-рассылками и колл-центрами мошеннических структур. История развития пластиковых карт. История банковских карт в России. Виды электронных денег и их применение. Банкоматы. Банкоматное мошенничество. Криптовалюта. 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. Аудит информационной безопасности банковской системы. Тестирование на проникновение. Выявление известных уязвимостей ПО. Понятие инцидента, события и мошенничества в сфере банковской безопасности. Классификация нарушений безопасности в банковской сфере и примеры нарушений. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID. Профиль				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
безопасности OpenID API для доступа к сервисам в режиме только для чтения. Профиль безопасности OpenID API для доступа к сервисам в режиме чтения и записи. Дистанционное банковское обслуживание.				
ИТОГО по 11-му семестру	24	16	12	54
ИТОГО по дисциплине	60	32	30	126

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
2	Управление пользователями и группами в ОС Windows 2000/XP/2003/Vista/7/8/10.
3	Сетевые атаки.
3	Система разграничения доступа к локальным и сетевым ресурсам в ОС Windows 2000/XP/2003/Vista/7/8/10.
4	Средства защиты информации от несанкционированного доступа (на примере СЗИ от НСД «Аккорд»).
4	Автоматизированная система «Фид-АнтиФрод».
4	Угрозы, возникающие при эксплуатации систем ДБО и потенциальные нарушители.
4	Проверка возможности подбора паролей к интерфейсам управления систем.
4	Защита от банкоматного мошенничества.
4	Работа «Аккорд» с моделированием случаев НСД, нарушением целостности и запуском несанкционированного ПО.

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
2	Работа с параметрами реестра Windows на виртуальной машине. Редактор реестра. Работа с параметрами разделов HKEY_CURRENT_USER, HKEY_ LOCAL_MACHINE.
3	Идентификация и аутентификация (RSA, схемы Шнорра и Фейге-Фиата-Шамира).
3	Лицензионные и свободно распространяемые программные продукты. Организация обновления программного обеспечения с использованием сети Интернет.
4	Современные стандарты идентификации: OpenID API.
4	Подбор данных аутентификации (имен пользователей, паролей, ключей) для доступа к сетевым службам на основе словарей стандартных и часто встречающихся значений.
4	Информационные технологии в банковской деятельности. Система Дистанционного Банковского Обслуживания BS-Client.
4	Социальная инженерия.
4	Дистанционная работа банка с клиентами.

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.

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
1. Основная литература		
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	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

3	Информационные системы и технологии в экономике и управлении : учебник для вузов / Трофимов В. В., Ильина О. П., Трофимова Е. В., Кияев В. И., Приходченко А. П. 3-е изд., перераб. и доп. Москва : Юрайт, 2011. 521 с.	2
4	Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов. 2-е изд. Москва : Горячая линия-Телеком, 2004. 146 с.	7
5	Партыка Т. Л., Попов И. И. Информационная безопасность : учебное пособие для среднего профессионального образования. 3-е изд., перераб. и доп. Москва : ФОРУМ, 2008. 431 с.	1
6	Чипига А.Ф. Информационная безопасность автоматизированных систем : учебное пособие для вузов. Москва : Гелиос АРВ, 2010. 335 с.	2
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Мельников Д. А. Информационная безопасность открытых систем : учебник. Москва : Флинта : Наука, 2013. 442 с. 27,44 усл. печ. л.	11
2	Михайлов С. Ф., Петров В. А., Тимофеев Ю. А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции : учебное пособие. Москва : Изд-во МИФИ, 1995. 110 с.	1
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	Безопасность финансовых (банковских) операций. Защита информации	https://files.stroyinf.ru/Data2/1/4293744/4293744380.pdf	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)

Вид ПО	Наименование ПО
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
База данных научной электронной библиотеки (eLIBRARY.RU)	https://elibrary.ru/
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	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 автоматизированных банковских систем»
Приложение к рабочей программе дисциплины

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация (профиль) образовательной программы:	Безопасность открытых информационных систем
Квалификация выпускника:	Специалист
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	Очная

Курс: 1**Семестр**: 2

Трудоёмкость:

Кредитов по рабочему учебному плану:	8 ЗЕ
Часов по рабочему учебному плану:	288 ч.

Форма промежуточной аттестации:

Экзамен:	10 семестр
Зач. без оценки	11 семестр

Пермь 2023

Фонд оценочных средствдля проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины.Фонд оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает системуоценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средствдля 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 двух семестров (10, 11-го семестров учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные 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 (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим заданиям и экзамена. 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**	**ПЗ**	**Т/КР**		**Экзамен**
Усвоенныезнания						
З.1знать основные факторы, определяющие величину ущерба, нанесенного банковской системе вследствие отсутствия или недостаточной надёжности систем защиты информации, теоретические основы функционирования систем информационной безопасности в банковской системе, ее современные проблемы и терминологию.	С	ТО1	ПЗ1			ТВ
Освоенные умения						
У.1уметь анализировать эффективность систем информационной безопасности в банковской системе,разрабатывать нормативно-методические материалы по регламентации системы информационной безопасности в банковской системе.	С	ТО2	ПЗ 2 ПЗ 3			ТВ
Приобретенные владения						
В.1владетьнавыками выбора метода определения ущерба, наносимого владельцу информации в результате противоправного ее использования, навыками работы с персоналом,принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения	С	ТО3	ПЗ 4 ПЗ 5			ТВ

информационной безопасности в банковской системе.						

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

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, 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 в форме собеседования или выборочного теоретического опроса в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в журнал преподавателя и учитываются в виде интегральной оценки при проведениипромежуточной аттестации.

Вопросы для самостоятельного изучения:

Тема 1.1: Перспективы развития законодательства в области информационной безопасности.

Тема 2.1: Шифрование данных при хранении и передачи (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 5практических 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. Промежуточная аттестация (итоговый контроль)

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

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

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

2.3.1. Типовые вопросы и задания для экзаменапо дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Системное и прикладное программное обеспечение, понятие информационных ресурсов (объектов) и пользователей данных ресурсов (субъектов).
2. Основные функции операционной системы ПЭВМ, встроенные возможности разграничения доступа, блокировка доступа к рабочей станции.
3. Идентификация и аутентификация пользователей автоматизированных систем.

4. Понятие учетных записей, полномочия администраторов и пользователей систем (привилегии, роли).
5. Автоматическая блокировка/разблокировка учетных записей.
6. Использование паролей, понятие структуры пароля, правила выбора стойких паролей, подбор паролей с использование специализированных программ.
7. Понятие сетевых ресурсов, изолированность сегментов локально-вычислительных сетей, разграничение прав доступа к сетевым ресурсам.
8. Шифрование данных при хранении и передачи (симметричное/асимметричное шифрование).
9. Понятие электронной подписи, цифровых сертификатов, описание механизмов аутентификации.
10. Средства криптографической защиты информации в банковской системе.
11. Политика безопасности в системе, критичные информационные ресурсы.
12. Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия.
13. Понятие целостности и лицензионной чистоты программного обеспечения.
14. История банков в России. Виды банков. Функции банков.
15. Правовое регулирование банковской деятельностью.
16. Особенности автоматизированных банковских систем, используемых в российских банках.
17. Информационное обеспечение автоматизированных банковских систем.
18. Техническое оснащение современных автоматизированных банковских систем.
19. Программное обеспечение автоматизированных банковских систем.
20. История развития пластиковых карт.
21. История банковских карт в России. Виды электронных денег и их применение.
22. Основные направления политики информационной безопасности и нормативная база Банка России.
23. Стандарты Банка России.
24. Применяемые в ТУ Банка России меры и средства защиты информации, функции администраторов информационной безопасности подразделений.
25. Особенности использования средств защиты информации от несанкционированного доступа.
26. Организация бесперебойного функционирования информационных систем.

Типовые 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.

2.3.2. Шкалы оценивания результатов обучения наэкзамене

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

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть*приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов икомпетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете 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, 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 экзаменаиспользуются типовые критерии, приведенные в общей части ФОС образовательной программы.