МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

СТАНДАРТЫ PA/PCI DSS В ФИНАНСОВОЙ ИНДУСТРИИ

Направление подготовки (специальность)
09.04.01 Информатика и вычислительная техника

Направленность (профиль/специализация) программы
Программное обеспечение средств вычислительной техники и автоматизированных систем

Уровень высшего образования - магистратура

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Вычислительной техники и программирования
Курс	1
Семестр	2

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

Рабочая программа рассмотрена и одобрена на заседании кафедры вычислительной техники и программирования
19.02.2020 г. протокол № 5

Зав. кафедрой _____ О.С. Логунова

Рабочая программа одобрена методической комиссией ИЭ и АС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
доцент кафедры ВТ и П, канд. техн. наук _____ Л.Г.Егорова

Рецензент:
Начальник отдела технологических платформ
ООО Компас Плюс , канд. техн. наук _____ Д.С.Сафонов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры вычислительной техники и программирования

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ О.С. Логунова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры вычислительной техники и программирования

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ О.С. Логунова

1 Цели освоения дисциплины (модуля)

Дисциплина Стандарты PA PCI DSS в финансовой индустрии предоставляет практические знания в области знаний о безопасности данных держателях банковских карт и содействовать широкому внедрению унифицированных мер защиты данных. Цель дисциплины состоит в обучении базовым техническим и операционным требованиям, которые разработаны для защиты данных платежных карт. В результате обучения формируется умение использовать современные технологии и инструментальные средства для обеспечения безопасности данных платежных приложений.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Стандарты PA/PCI DSS в финансовой индустрии входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Инновационные технологии современных платежных систем

Современные автоматизированные системы для платежей и розничных банковских процессов

Информационные технологии процессинговых центров

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Инновационные технологии современных платежных систем

Современные автоматизированные системы для платежей и розничных банковских процессов

Программное обеспечение современной перспективной платежной инфраструктуры

Современные розничные финансовые платформы на примере TranzAxis

Автоматизированная система TranzWare для розничных банковских процессов

Конфигурирование на платформе TranzAxis

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Стандарты PA/PCI DSS в финансовой индустрии» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-4 Обладает способностью к разработке компонентов системы управления базами данных, отладке разрабатываемой системы управления базами данных, документированию разработанной системы управления базами данных в целом и ее компонентов и сопровождению созданной системы управления базами данных	
ПК-4.1	Определяет необходимость разработки компонентов системы управления базами данных
ПК-4.2	Оценивает качество разработки компонентов системы управления базами данных

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 37,15 акад. часов:

– аудиторная – 34 акад. часов;

– внеаудиторная – 3,15 акад. часов

– самостоятельная работа – 35,15 акад. часов;

– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Введение и обзор стандарта PCI DSS								
1.1 Стандарт безопасности данных индустрии платежных карт (PCI DSS): общий обзор. Источники информации о PCI DSS.	2	2			5	1. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Устный опрос.	ПК-4.1, ПК-4.2
1.2 Область применения стандарта PCI DSS. Применимость PCI DSS к приложениям, соответствующим стандарту PA-DSS.Применимость стандарта PCI DSS к разработчикам платежных приложений		2	2		5	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
1.3 Область применимости требований стандарта PCI DSS. Сегментация сети. Беспроводные сети. Привлечение сторонних поставщиков услуг (аутсорсинг).		2	2		5	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
Итого по разделу		6	4		15			
2. Требования и процедуры оценки безопасности стандарта PCI DSS								

2.1 Установка и поддержка конфигурации межсетевых экранов для защиты данных держателей карт.	2	2	2/2И		3	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
2.2 Защита хранимых данных держателей карт. Использование паролей и различных параметров безопасности к системам. Шифрование данных держателей карт при передаче через сети общего пользования.		2	2/2И		3	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
2.3 Поддержка программ управления уязвимостями. Защита систем от вредоносного программного обеспечения. Разработка и поддержка безопасных систем и приложений		2	2/2И		3	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
2.4 Меры контроля доступа. Контроль доступа к данным держателей карт. Физический доступ к данным держателе карт. Идентификация и аутентификация доступа к системным компонентам. Мониторинг доступа к сетевым ресурсам и данным держателей карт.		2	2/2И		3	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
2.5 Тестирование системы и процессов безопасности. Поддержка политики информационной безопасности.		2	2		3	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
Итого по разделу		10	10/8И		15			
3. Дополнительные требования PCI DSS								

3.1 Дополнительные требования PCI DSS для поставщиков услуг хостинга с общей средой. Дополнительные требования PCI DSS для организаций, использующих SSL и (или) ранние версии TLS. Дополнительная проверка организаций зоны повышенного риска.	2	1	3		5,15	1. Подготовка к лабораторным занятиям 2. Выполнение лабораторных работ 3. Самостоятельное изучение учебной и научной литературы	1. Беседа - обсуждение 2. Проверка индивидуальных заданий 3. Устный опрос.	ПК-4.1, ПК-4.2
Итого по разделу		1	3		5,15			
Итого за семестр		17	17/8И		35,15		экзамен	
Итого по дисциплине		17	17/8И		35,15		экзамен	

5 Образовательные технологии

1. Традиционные образовательные технологии, ориентированные на организацию образовательного процесса и предполагающие прямую трансляцию знаний от преподавателя к студенту.

Формы учебных занятий с использованием традиционных технологий:

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

Формы учебных занятий с использованием технологий проблемного обучения:

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от студента применения как научно-теоретических знаний, так и практических навыков.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Платежные системы в ракурсе российского законодательства и международной практики: монография / Тамаров П.А. - Москва :ЦИПСиР, 2015. - 280 с. ISBN 978-5-406-03615-0 - Текст : электронный. - URL:
https://znanium.com/catalog/product/556595
(дата обращения: 28.10.2020). – Режим доступа: по подписке.

2. Склярова, Ю. М. Банки и банковское дело: сборник кейс-стади и ситуационных заданий [Электронный ресурс] : учебное пособие / Ю.М. Склярова, И.Ю. Скляров, Т.Г. Гурнович и др.; под общ. ред. Ю.М. Скляровой. - 2-е изд., перераб. и доп. - Ставрополь, 2013. - 128 с. - Текст : электронный. - URL:
https://znanium.com/catalog/product/514841
(дата обращения: 28.10.2020). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Казимагомедов, А. А. Банковское дело: организация деятельности центрального банка и коммерческого банка, небанковских организаций : учебник / А.А. Казимагомедов. - Москва : ИНФРА-М, 2020. - 502 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/25095. - ISBN 978-5-16-012458-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1073953
(дата обращения: 28.10.2020). – Режим доступа: по подписке.

2. Синки, Д. Финансовый менеджмент в коммерческом банке и в индустрии финансовых услуг / Синки Д., Левинзон А.И. - Москва :Альп. Бизнес Букс, 2016. - 1018 с.ISBN 5-9614-0344-0. - Текст : электронный. - URL:
https://znanium.com/catalog/product/926124
(дата обращения: 28.10.2020). – Режим доступа: по подписке.

в) Методические указания:

Представлены в приложении 1.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
Kaspersky Endpoint Security для бизнеса-Стандартный	Д-300-18 от 21.03.2018	28.01.2020
Oracle SQL Developer	свободно распространяемое ПО	бессрочно
Oracle SQL Developer Data Modeler	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp

Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

1. Лекционная аудитория ауд. 282. Мультимедийные средства хранения, передачи и представления информации.

2. Компьютерные классы Центра информационных технологий ФГБОУ ВО «МГТУ». Персональные компьютеры, объединенные в локальные сети с выходом в Internet, оснащенные современными программно-методическими комплексами для решения задач в области информатики и вычислительной техники.

3. Аудитории для самостоятельной работы: компьютерные классы; читальные залы библиотеки. Все классы УИТ и АСУ с персональными компьютерами, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

4. Аудиторий для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Ауд. 282 и классы УИТ и АСУ.

5. Помещения для самостоятельной работы обучающихся, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и наличием доступа в электронную информационно-образовательную среду организации. Классы УИТ и АСУ.

6. Помещения для хранения и профилактического обслуживания учебного оборудования. Центр информационных технологий – ауд. 372.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

Лабораторная работа 1

Установка и поддержка конфигурации межсетевых экранов для защиты ДДК

Межсетевые экраны – это устройства, которые контролируют сетевой трафик, разрешенный между локальными (внутренними) сетями организации и недоверенными (внешними) сетями, а также которые контролируют входящий и исходящий трафик в зонах повышенной критичности, находящихся внутри доверенных сетей организации. Среда ДДК является примером зоны повышенной критичности внутри доверенной локальной сети организации.

Межсетевой экран анализирует весь сетевой трафик и блокирует соединения, которые не удовлетворяют заданным критериям безопасности. Все системы должны быть защищены от несанкционированного доступа из недоверенных сетей, будь то подключение систем электронной торговли к сети через Интернет, доступ работников к Интернету через браузеры, доступ работников к электронной почте, выделенные подключения со сторонними организациями, подключения по беспроводным сетям или иными способами. Зачастую кажущиеся малозначимыми каналы связи с недоверенными сетями могут представлять собой незащищенные пути доступа к ключевым системам.

Межсетевые экраны – важнейшие механизмы обеспечения безопасности любой компьютерной сети. Иные системные компоненты могут обеспечивать функциональные возможности межсетевого экрана, если эти компоненты отвечают минимальным требованиям к межсетевым экранам, приведенным в Требовании 1.

Если иные системные компоненты обеспечивают функциональные возможности межсетевого экрана в составе среды ДДК, они должны быть включены в область оценки и проверены на соответствие с требованием:

Требования PCI DSS	**Проверочные процедуры**
1.1 Разработать и внедрить стандарты конфигурации межсетевых экранов и маршрутизаторов. Стандарты должны включать в себя: 1.1.1 Формализованный процесс утверждения и тестирования всех сетевых соединений и изменений в конфигурациях межсетевых экранов и маршрутизаторов.	1.1 Проверить стандарты конфигурации межсетевых экранов и маршрутизаторов, а также иную указанную ниже документацию, на предмет полноты стандартов и их надлежащего внедрения следующим образом: 1.1.1.а Проверить документированные процедуры на предмет того, что существует формализованный процесс тестирования и утверждения всех: • сетевых соединений; • изменений в конфигурациях межсетевых экранов и маршрутизаторов. 1.1.1.б Для выборки сетевых соединений опросить ответственных работников и проверить записи на предмет того, что сетевые соединения были протестированы и утверждены. 1.1.1.с Определить выборку реальных

	изменений, произведенных в конфигурациях межсетевого экрана и маршрутизатора, сравнить их с записями об изменениях и опросить ответственных работников на предмет того, что изменения были протестированы и утверждены.
1.1.2 Актуальную схему сети, которая указывает все подключения между средой ДДК и другими сетями, включая все беспроводные сети	1.1.2.а Проверить схему (схемы) и конфигурации сети на предмет наличия актуальной схемы сети, а также того, что в схеме отмечены все подключения к ДДК и что она включает все беспроводные сети. 1.1.2.б Опросить ответственных работников на предмет того, что схема поддерживается в актуальном состоянии
1.1.3 Актуальную схему, отображающую все потоки ДДК по системам и сетям.	1.1.3 Проверить схему потоков данных и опросить работников на предмет того, что схема: • отражает все потоки ДДК по системам и сетям; • поддерживается в актуальном состоянии и обновляется, если в среду вносятся изменения
1.1.4 Требования о необходимости межсетевого экранирования каждого Интернет-соединения и соединений между каждой демилитаризованной зоной и внутренней сетью.	1.1.4.а Проверить стандарты конфигурации межсетевого экрана на наличие требований о необходимости межсетевого экранирования каждого Интернет-соединения, а также соединений между каждой демилитаризованной зоной и внутренней сетью. 1.1.4.б Убедиться, что актуальная схема сети соответствует стандартам конфигурации межсетевых экранов. 1.1.4.с Проверить конфигурации сети на наличие межсетевого экрана на каждом Интернет-соединении и между каждой демилитаризованной зоной и внутренней сетью согласно документированным стандартам конфигурации и схемам сети.
1.1.5 Описание групп, ролей и обязанностей по управлению сетевыми компонентами.	1.1.5.а Убедиться, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат описание групп, ролей и обязанностей по управлению сетевыми компонентами.

Лабораторная работа2

Использование паролей к системам и другие параметры безопасности

Злоумышленники (внешние и внутренние по отношению к организации) часто используют настройки, учетные записи и пароли по умолчанию, заданные производителем, для компрометации операционных систем, приложений и устройств, на которых они установлены. Поскольку эти настройки по умолчанию хорошо известны и

часто публикуются в хакерских сообществах, их изменение снизит уязвимость систем к атакам. Даже если не планируется использовать учетную запись по умолчанию, изменение пароля по умолчанию на надежный уникальный пароль и последующее отключение учетной записи не позволит злоумышленнику повторно включить ее и получить доступ с помощью пароля по умолчанию.

Если беспроводные сети реализованы без использования достаточно безопасных конфигураций (включая изменение настроек по умолчанию), анализаторы беспроводных сетей могут прослушивать трафик, без труда извлекать пароли и данные, а также легко проникать в сеть и атаковать ее. Кроме того, протокол обмена ключами для ранних версий протокола шифрования 802.11x (Wired Equivalent Privacy, WEP) был взломан, и может сделать шифрование бесполезным. Микропрограммное обеспечение для устройств следует обновить для поддержки более защищенных протоколов.

Требования PCI DSS	**Проверочные процедуры**
1. Всегда изменять параметры по умолчанию, заданные производителями, а также удалять или отключать неиспользуемые учетные записи по умолчанию перед установкой систем в сети. Это требование применимо ко ВСЕМ паролям по умолчанию, включая, в том числе, пароли к операционным системам, защитному программному обеспечению, учетным записям приложений и системным учетным записям, POS-терминалам (терминалы в точках продаж), платежным приложениям, а также строкам доступа SNMP и т. д.	1.1.а Сделать выборку системных компонентов и (с помощью системного администратора) попытаться осуществить вход в устройства и приложения, используя учетные записи и пароли по умолчанию, устанавливаемые производителем, чтобы проверить, что ВСЕ пароли по умолчанию (включая пароли к операционным системам, защитному программному обеспечению, учетным записям приложений и системным учетным записям, POSтерминалам, а также строки доступа SNMP) были изменены. (Используйте руководства от вендоров и Интернет-ресурсы, чтобы узнать учетные записи и пароли по умолчанию, устанавливаемые производителем). 2.1.б Проверить выборку системных компонентов на предмет того, что все неиспользуемые учетные записи по умолчанию (включая учетные записи к операционным системам, POS-терминалам, защитному программному обеспечению, приложениям, устройствам, а также строки доступа SNMP и т. д.) удалены или отключены. 2.1.с Опросить работников и проверить сопроводительную документацию на предмет того, что: • все учетные данные по умолчанию, заданные производителем (включая пароли по умолчанию к операционным системам, POS-терминалам, защитному программному обеспечению, приложениям и системным учетным записям, а также строки доступа SNMP и т. д.) изменяются перед установкой системы в сети; • неиспользуемые учетные записи, настроенные по умолчанию, (включая

	учетные записи к операционным системам, POS-терминалам, защитному программному обеспечению, приложениям и системным учетным записям, а также строки доступа SNMP и т. д.) удаляются или отключаются перед установкой системы в сети.
1.1 Для беспроводных окружений, которые подключены к среде ДДК либо передают ДДК, необходимо изменить ВСЕ параметры по умолчанию, заданные производителем, включая, помимо прочего, ключи шифрования для доступа к беспроводной сети, пароли, строки доступа SNMP.	1.1.1.а Проверить документацию вендора и выполнить вход на беспроводные устройства при содействии системного администратора, чтобы подтвердить, что: • не используются строки доступа SNMP по умолчанию; • не используются пароли и (или) парольные фразы по умолчанию к точкам доступа. 1.1.1.б Проверить документацию вендора и настройки беспроводной конфигурации на предмет того, что микропрограммное обеспечение беспроводных устройств обновлено для того, чтобы поддерживать стойкие алгоритмы шифрования для: • аутентификации в беспроводных сетях; • передачи данных по беспроводным сетям.
1.2 Разработать стандарты конфигурации для всех системных компонентов. Убедиться в том, что стандарты учитывают все известные уязвимости, а также согласуются с положениями отраслевых стандартов безопасной настройки систем. Например, к источникам общепринятых отраслевых стандартов по безопасной настройке систем относятся, среди прочих: • Центр Интернет-безопасности (CIS); • Международная организация по стандартизации (ISO); • Институт системного администрирования, аудита, сетевых технологий и проблем безопасности (SANS); • Национальный институт стандартов и технологий (NIST)	1.2.а Проверить стандарты конфигурации организации для всех типов системных компонентов на предмет того, что эти стандарты согласуются с требованиями отраслевых стандартов безопасной настройки систем. 1.2.б Проверить стандарты системной конфигурации на наличие следующих процедур для всех типов системных компонентов: • изменить все параметры по умолчанию, заданные производителем, и исключить неиспользуемые учетные записи по умолчанию; • реализовать на каждом сервере только одну основную функцию для того, чтобы исключить совмещение на одном и том же сервере функций, требующих различных уровней безопасности; • включать только необходимые службы, протоколы, управляющие программы и т. д., требующиеся для функционирования системы; • реализовать дополнительные защитные меры для любых необходимых служб, протоколов и управляющих программ, которые признаны небезопасными; • настроить параметры безопасности системы таким образом, чтобы исключить

	возможность ее некорректного использования; • удалить все неиспользуемые функциональные возможности, такие как, скрипты, драйверы, функции, подсистемы, файловые системы, а также неиспользуемые веб-серверы.
2.1 Реализовать на каждом сервере только одну основную функцию во избежание совмещения на одном и том же сервере функций, требующих различных уровней защиты. (Например, веб-серверы, серверы баз данных и DNS-серверы следует размещать на разных серверах).	2.1.а Сделать выборку системных компонентов и проверить системные конфигурации на предмет того, что выполняется правило «один сервер — одна основная функция». 2.2.1.б Если используются технологии виртуализации, проверить системные конфигурации на предмет того, что на одном виртуальном системном компоненте или устройстве реализована только одна основная функция.
2.2 Включать только необходимые службы, протоколы, управляющие программы и т. д., требующиеся для функционирования системы.	2.2. Сделать выборку системных компонентов и проверить включенные службы, управляющие программы и протоколы на предмет того, что включены только необходимые службы или протоколы.

Лабораторная работа 3

Защита хранимых ДДК

Официальная политика хранения данных определяет, какие данные необходимо хранить и где находятся эти данные, чтобы их можно было безопасно уничтожить или удалить, когда они больше не требуются. После авторизации разрешается хранить только номер карты (PAN) (приведенный в нечитаемый вид), дату истечения срока действия, имя держателя карты и сервисный код. Знание мест хранения ДДК необходимо для их надлежащего хранения или удаления, когда они больше не требуются. Чтобы определить надлежащие требования к хранению, организации сначала следует выяснить свою служебную необходимость, а также любые законодательные или нормативные требования, которые применимы к ее отрасли и (или) к типу хранимых данных.

Обнаружение и удаление хранящихся данных с истекшим сроком хранения позволяет предотвратить хранение данных, которые больше не требуются. Данный процесс можно автоматизировать (полностью или частично) или выполнять вручную. Например, можно запрограммировать процедуру обнаружения и удаления данных (автоматическую или ручную) и (или) проверять места хранения данных вручную. Внедрение методов безопасного удаления данных гарантирует, что данные, когда они больше не требуются, восстановить будет невозможно. Важно! Не хранить данные, если они не нужны!

КАД состоят из полных данных треков, кода или значения проверки подлинности карты и данных ПИН-кода. Хранить КАД после авторизации запрещается! Эти данные представляют большую ценность для злоумышленников, т.к. последние, используя такие данные, могут генерировать поддельные платежные карты и осуществлять мошеннические транзакции.

Эмитенты платежных карт или компании, которые оказывают или поддерживают услуги эмиссии, часто создают и контролируют КАД в рамках процесса эмиссии. Компаниям, которые оказывают, содействуют или поддерживают услуги выпуска карт,

разрешается хранить КАД ТОЛЬКО В ТОМ СЛУЧАЕ, если у них есть в этом обоснованная служебные необходимость. Следует отметить, что все требования стандарта PCI DSS распространяются на эмитентов, и единственное исключение для эмитентов и их процессинговых центров заключается в том, что они могут хранить КАД, если у них в этом есть обоснованная потребность. Под такой потребностью понимается не удобство, а необходимость для выполнения эмитентом своей функции. Любые такие данные должны храниться безопасно, в соответствии с требованиями стандарта PCI DSS и требованиями конкретной международной платежной системы.

Требования PCI DSS	**Проверочные процедуры**
1. Свести хранение ДДК к минимуму с помощью политик, процедур и процессов хранения и уничтожения данных, в которые включены, как минимум, следующие требования для всех хранилищ ДДК: • ограничение количества хранимых данных и сроки хранения до значений, необходимых для выполнения законодательных, нормативных и (или) служебных требований; • конкретные требования к хранению ДДК; • процессы безопасного удаления данных, когда в них уже нет необходимости	1.а Проверить политики, процедуры и процессы хранения и уничтожения данных на предмет наличия в них следующих требований для всех хранилищ ДДК: • ограничение количества хранимых данных и сроков хранения до значений, необходимых для выполнения законодательных, нормативных и (или) служебных требований; • конкретные требования к хранению ДДК (например, ДДК требуется хранить в течение срока X по причинам Y); • процессы безопасного удаления ДДК, если в их хранении больше нет необходимости в соответствии с законодательными, нормативными или служебными требованиями; 1.б Для выборки системных компонентов, которые хранят ДДК: • проверить файлы и системные записи на предмет того, что сроки хранения данных не превышают сроки, определенные политикой хранения данных; • проверить механизм удаления на предмет того, что данные удаляются безопасным образом.
2. Запрещается хранить КАД после авторизации (даже в зашифрованном виде). Если КАД получены, следует сделать все данные невосстановимыми до завершения процесса авторизации.	2. Проверить места хранения данных и системные конфигурации на предмет того, что КАД защищены.
2.1 Запрещается хранить полное содержимое любого трека (магнитной полосы на обратной стороне карты, эквивалентных данных на чипе или в ином месте) после авторизации. Эти данные также называются «полные данные треков», «трек», «трек 1», «трек 2» и «данные магнитной полосы».	2.1 Проверить источники данных в выборке системных компонентов, включая перечисленные ниже, на предмет того, что полные данные любого трека магнитной полосы, находящейся на обратной стороне карты (или ее аналога на чипе), не сохраняются после авторизации: • входящие данные о транзакции; • все журналы (например, журналы транзакций, хронологии, отладки, ошибок); • файлы хронологии; • файлы трассировки;

	• несколько схем баз данных; • содержимое баз данных.
2.2 Запрещается хранить код или значение проверки подлинности карты (трех- или четырехзначное число, напечатанное на лицевой или обратной стороне карты, используемые для подтверждения транзакций, выполняемых без предоставления платежной карты) после авторизации. Запрещается хранить ПИН-код или зашифрованный ПИН-блок после авторизации.	2.2 Проверить источники данных в выборке системных компонентов, включая перечисленные ниже, на предмет того, что трех- или четырехзначный код или значение проверки подлинности карты, напечатанные на лицевой стороне карты или на месте для подписи (данные CVV2, CVC2, CID, CAV2), не сохраняются после авторизации. Проверить источники данных в выборке системных компонентов, включая перечисленные ниже, на предмет того, что ПИН-коды, а также зашифрованные ПИН-блоки не сохраняются после авторизации: • входящие данные о транзакции; • все журналы (например, журналы транзакций, хронологии, отладки, ошибок); • файлы хронологии; • файлы трассировки; • несколько схем баз данных; • содержимое баз данных.
2.4 Привести PAN к нечитаемому виду во всех местах их хранения (включая журналы, резервные копии, съемные цифровые носители), используя для этого любой из следующих методов: • однонаправленное хеширование на основе стойкой криптографии (хеш-код должен быть сформирован из целого PAN); • усечение (хеш-код не может использоваться для замены усеченного сегмента PAN); • индексные маркеры и шифровальные блокноты (такие блокноты при хранении должны быть защищены); • стойкая криптография с сопутствующими процессами и процедурами управления ключами	2.4.а Проверить документацию о системе, используемой для защиты PAN, в том числе информацию о ее вендоре, типе системы и (или) процесса, алгоритмах шифрования (при использовании таковых) на предмет того, что PAN приводится к нечитаемому виду с использованием одного из следующих методов: • однонаправленного хеширования на основе стойкой криптографии; • усечения; • индексных маркеров и шифровальных блокнотов, причем такие блокноты при хранении должны быть защищены; • стойкой криптографии с сопутствующими процессами и процедурами управления ключами. 2.4.б Проверить несколько таблиц или файлов из выборки хранилищ данных на предмет того, что PAN приведены к нечитаемому виду (т. е. не хранятся как незашифрованный текст).

Лабораторная работа 4

Шифрование ДДК при передаче через сети общего пользования

Критичная информация должна шифроваться при передаче по сетям общего пользования, потому что злоумышленник без труда может перехватить и (или) изменить их маршрут при передаче. Безопасная передача ДДК требует использования доверенных ключей и (или) сертификатов, безопасного протокола передачи и шифрования надлежащей стойкости для шифрования ДДК.

Не следует принимать запросы на подключение от систем, не поддерживающих требуемую стойкость шифрования, т. к. это приведет к небезопасному подключению. Следует отметить, что некоторые версии протоколов (например, SSL, SSH 1.0 и ранние версии TLS) содержат известные уязвимости, которые могут быть использованы злоумышленником для получения контроля над подверженной этим уязвимостям системой.

Независимо от того, какой протокол используется, следует убедиться, что он настроен на то, чтобы использовать только безопасные конфигурации и версии для предотвращения небезопасного подключения. Например, использовать только доверенные сертификаты и поддерживать только стойкое шифрование (не поддерживать нестойкие, небезопасные протоколы или методы).

Злоумышленники используют свободно распространяемые и широкодоступные средства для прослушивания беспроводного трафика. Использование стойкой криптографии может ограничить раскрытие критичной информации, передаваемой по беспроводным сетям. Чтобы предотвратить доступ злоумышленников к беспроводным сетям или использование беспроводных сетей для получения доступа к другим внутренним сетям или данным, требуется стойкая криптография для аутентификации и передачи ДДК.

Требования PCI DSS	**Проверочные процедуры**
1. Использовать стойкую криптографию и безопасные протоколы, чтобы защитить критичные ДДК при их передаче через открытые общедоступные сети с учетом следующего: • принимаются только доверенные ключи и сертификаты; • используемый протокол поддерживает только безопасные версии и конфигурации; • стойкость шифрования соответствует используемой методологии шифрования.	1.а Выявить все места, где осуществляется прием или передача ДДК через открытые общедоступные сети. Проверить документированные стандарты и сравнить их с системными конфигурациями на предмет того, что во всех местах используются протоколы безопасности и стойкая криптография. 1.б Проверить документированные политики и процедуры на предмет того, что: • принимаются только доверенные ключи и (или) сертификаты; • используемым протоколом поддерживаются только безопасные версии и конфигураций (небезопасные версии или конфигурации не поддерживаются); • применяется шифрование надлежащей стойкости согласно используемой методологии шифрования. 1. с Сделать выборку входящих и исходящих отправок по мере их выполнения (например, отслеживая системные процессы или сетевой трафик) и проверить их на предмет того, что все ДДК передаются в зашифрованном виде с использованием стойкой криптографии. 1.д Проверить ключи и сертификаты на предмет того, что принимаются только доверенные ключи и (или) сертификаты. 1.е Проверить системные конфигурации на предмет того, что протокол реализован таким образом, чтобы использовать только безопасные конфигурации и что он не

	поддерживает небезопасные версии или конфигурации.
2. Убедиться, что при использовании беспроводных сетей, передающих ДДК либо подключенных к среде ДДК, применяется передовой отраслевой опыт, чтобы реализовать стойкое шифрование при аутентификации и передаче данных.	2. Выявить все беспроводные сети, передающие ДДК либо подключенные к среде ДДК. Проверить документированные стандарты и сравнить их с системными конфигурациями на предмет того, что во всех беспроводных сетях: • применяется передовой отраслевой опыт, чтобы реализовать стойкое шифрование при аутентификации и передаче данных; • не используется слабое шифрование (например, WEP, SSL) в качестве защитной меры для аутентификации или передачи данных.

Лабораторная работа 5

Защита систем от вредоносного программного обеспечения

Мейнфреймы, компьютеры среднего уровня (например, AS/400) и подобные системы в данное время не подвержены заражению вредоносным ПО или не являются его мишенью. Однако тенденции в области вредоносного ПО могут быстро меняться, а значит, организациям важно знать о новых видах вредоносного ПО, которые могут быть опасны для их систем (например, отслеживая сообщения о безопасности от вендоров ПО и новостных групп антивирусов, чтобы узнать, угрожают ли их системам новые виды и формы вредоносного ПО).

В процесс выявления новых уязвимостей в системе безопасности следует включить тенденции в области вредоносного ПО. Порядок реагирования на новые тенденции организации следует по необходимости включить в стандарты конфигурации и защитные меры.

Даже у лучших антивирусов снижается эффективность, если за ними не следить и не поддерживать в актуальном состоянии с помощью последних обновлений безопасности, антивирусных баз или защитных мер от вредоносного ПО.

Журналы регистрации событий предоставляют возможность мониторинга активности вирусов и вредоносного ПО, и реагирования на эту активность. Поэтому следует настроить средства защиты от вредоносного ПО на генерацию журналов регистрации событий и управлять этими журналами в соответствии с требованием.

Требования PCI DSS	Проверочные процедуры
1.1 Развернуть антивирусное ПО на всех системах, обычно подверженных воздействию вредоносного ПО	1.1. Проверить, что антивирусное ПО развернуто в выборке системных компонентов, включая все типы ОС, обычно подверженных воздействию вредоносного ПО, при наличии применимой антивирусной технологии.
1.2 Убедиться, что антивирусное ПО способно обнаруживать и устранять все известные типы вредоносного ПО, а также обеспечивать защиту от них.	1.2. Проверить документацию вендора и конфигурации антивирусов на предмет того, что антивирусные программы: - обнаруживают все известные типы вредоносного ПО; - удаляют все известные типы вредоносного ПО; - защищают от всех известных типов

	вредоносного ПО.
1.3 Проверить, что все антивирусные механизмы: - поддерживаются в актуальном состоянии; - выполняют периодическое сканирование; - создают журналы регистрации событий, которые хранятся согласно требованию 10.7 стандарта PCI DSS.	1.3.а Проверить политики и процедуры на предмет того, что они предписывают поддерживать антивирусные ПО и базы в актуальном состоянии. 1.3.б Проверить конфигурацию антивирусов, включая установочные образы, на предмет того, что антивирусные механизмы: - настроены на автоматическое обновление; - настроены на периодическое сканирование. 1.3.с Проверить выборку системных компонентов, включая все типы операционных систем, подверженных воздействию вредоносного ПО, на предмет того, что: - антивирусное ПО и базы актуальны; - выполняется периодическое сканирование.
1.4 Убедиться, что антивирусные механизмы постоянно запущены, и пользователи не могут их ни отключить, ни изменить без явного разрешения, которое выдается руководством на каждый конкретный случай и на ограниченный период времени.	1.4 а Проверить конфигурацию антивирусов, включая установочные образы ПО и выборку системных компонентов, на предмет того, что антивирусное ПО постоянно запущено. 1.4 б Проверить конфигурацию антивирусов, включая установочные образы ПО и выборку системных компонентов, на предмет того, что антивирусное ПО не может быть отключено или изменено пользователями.

Лабораторная работа 6

Разработка и поддержка безопасных систем и приложений

Цель данного требования состоит в том, чтобы организации были постоянно в курсе новых уязвимостей, которые могут воздействовать на ее среду.

Источники информации об уязвимостях должны быть достоверными. Зачастую к таковым относятся веб-сайты вендоров, отраслевые новостные группы, почтовые рассылки или RSS-ленты.

Как только организация выявляет уязвимость, которая может оказать негативное влияние на среду организации, необходимо оценить критичность уязвимости. Следовательно, в организации должен быть метод оценки уязвимостей и уровня их критичности на постоянной основе. Для этого недостаточно провести сканирование авторизованным поставщиком услуг сканирования (ASV) или внутреннее сканирование на наличие уязвимостей; для этого необходим процесс активного мониторинга отраслевых источников информации об уязвимостях.

Ранжируя риски (например, «высокий», «средний» или «низкий» уровни), организация может быстрее идентифицировать наиболее высокие риски, устанавливать им приоритет и управлять ими, а также минимизировать вероятность использования злоумышленниками уязвимостей, которые представляют наиболее высокий риск для организации.

Данное требование распространяется на применимые обновления для всего установленного ПО, включая платежные приложения, как прошедшие проверку на соответствие стандарту PA-DSS, так и не проходившие данной проверки.

Требования PCI DSS	Проверочные процедуры
1.1 Наладить процесс выявления уязвимостей с помощью авторитетных внешних источников информации об уязвимостях, а также процесс оценки критичности (например, «высокая», «средняя» или «низкая») для недавно обнаруженных уязвимостей.	1.1.а Проверить политики и процедуры на предмет того, что в процессах требуется: - идентифицировать новые уязвимости; - оценивать критичность уязвимостей, в т. ч. идентифицировать все уязвимости с «высоким» и «критичным» уровнями; - использовать авторитетные внешние источники информации об уязвимостях.
1.2 Гарантировать, что все системные компоненты и ПО защищены от известных уязвимостей путем установки применимых обновлений безопасности, которые выпускает производитель. Устанавливать критичные обновления безопасности в течение одного месяца с момента их выпуска.	1.2 а Проверить политики и процедуры, относящиеся к установке обновлений безопасности, на наличие процессов, которые требуют: - устанавливать применимые критичные обновления безопасности, которые выпускает производитель, в течение месяца после их выхода; - устанавливать все применимые обновления безопасности, которые выпускает производитель, в течение соответствующего срока с момента их выхода (например, в течение трех месяцев). 1.2 б Сравнить перечень обновлений безопасности, которые установлены на каждой системе из выборки системных компонентов и связанного с ними ПО, с перечнем последних обновлений безопасности, которые выпускает производитель, на предмет того, что: - применимые критичные обновления безопасности, которые выпускает производитель, устанавливаются в течение месяца с момента выпуска; - все применимые обновления безопасности, которые выпускает производитель, устанавливаются в течение надлежащего срока с момента выпуска (например, в течение трех месяцев).
1.3. Удалять все учетные записи разработчиков, тестовые учетные записи и (или) учетные записи заказного приложения, идентификаторы пользователей и пароли перед передачей ПО заказчикам или переводом его в производственный режим.	1.3 Проверить документированные процедуры разработки ПО на предмет того, что все допроизводственные учетные записи и (или) учетные записи заказного приложения, идентификаторы пользователей и (или) пароли удаляются перед передачей ПО заказчикам или переводом его в производственный режим.
1.4 Контролировать разрабатываемый код на наличие потенциальных уязвимостей	1.4 Проверить документированные процедуры разработки ПО и опросить

(вручную или автоматически) перед передачей готовых приложений заказчикам или переводом их в производственный режим с соблюдением как минимум следующих требований: - контролировать изменения программного кода лицами, которые не являются авторами этого кода, и лицами, которые знают методики контроля кода и методы безопасного программирования; - контролируя программный код, убедиться, что он разработан в соответствии с рекомендациями безопасного программирования; - вносить все необходимые корректировки до выпуска ПО; - результаты контроля кода рассматриваются и утверждаются руководством до выпуска ПО.	ответственных работников на предмет того, что все изменения разрабатываемого программного кода обязательно контролируются (вручную или автоматически) с учетом следующих требований: - контролировать изменения программного кода лицами, которые не являются авторами этого кода, и лицами, которые знают методики контроля кода и методы безопасного программирования; - контролируя программный код, убедиться, что он разработан в соответствии с рекомендациями безопасного программирования (см. Требование 6.5 PCI DSS); - вносить все необходимые корректировки до выпуска ПО; - результаты контроля кода рассматриваются и утверждаются руководством до выпуска ПО.

Лабораторная работа 7

Ограничение доступа к ДДК в соответствии со служебной необходимостью

Для того чтобы доступ к ДДК ограничивался только теми лицами, которым он необходим, сначала нужно определить:

— необходимые права доступа для каждой роли (например, системного администратора, работника колл-центра, продавца),

— системы, устройства и данные, доступ к которым необходим для каждой роли,

— уровень прав доступа, необходимых каждой роли для реального выполнения своих должностных обязанностей.

Как только роли и необходимые им права доступа определены, лицам могут быть предоставлены соответствующие права доступа.

Назначая привилегированные идентификаторы, важно предоставлять лицам только те права, которые им минимально необходимы для выполнения должностных обязанностей («минимально необходимый набор прав»). Например, администратор баз данных или администратор резервного копирования не должны иметь те же полномочия, что и администратор всей системы.

Назначая минимально необходимый набор прав, можно предотвратить ошибочное или случайное изменение конфигурации приложения, или его настроек безопасности со стороны пользователей, не обладающих достаточными знаниями о приложении. Устанавливая минимально необходимые права доступа, можно также свести к минимуму ущерб, если постороннее лицо получит доступ к идентификатору пользователя.

Требования PCI DSS	**Проверочные процедуры**
1.1 Ограничить доступ к системным компонентам и ДДК только теми лицами, которым такой доступ требуется в соответствии с их служебными обязанностями.	1.1 Проверить документированную политику контроля доступа на предмет того, что она отражает требования - определением прав доступа и назначением привилегий для каждой роли; - ограничением доступа

	привилегированных учетных записей только тем набором прав, который им минимально необходим для выполнения своих должностных обязанностей; - назначением прав доступа согласно роли и должностным обязанностям конкретного работника; - документированным утверждением (в письменной или электронной форме) всех прав доступа уполномоченными сторонами с указанием списка конкретных утвержденных привилегий.
1.2 Определить необходимые права доступа для каждой роли, включая: - системные компоненты и информационные ресурсы, доступ к которым необходимо предоставить каждой роли для выполнения должностных обязанностей; - необходимый уровень привилегий (например, пользовательский, администраторский и т. д.) для доступа к ресурсам.	1.2 Сделать выборку ролей и проверить их на предмет того, что потребности в правах доступа для каждой роли определены и включают: - системные компоненты и информационные ресурсы, доступ к которым необходимо предоставить каждой роли для выполнения должностных обязанностей; - список прав доступа, необходимых каждой роли для выполнения должностных обязанностей.
1.3 Ограничить права доступа идентификаторам привилегированных пользователей только тем набором прав, который минимально необходим им для выполнения своих должностных обязанностей.	1.3 Сделать выборку учетных записей привилегированных пользователей и опросить руководящих работников на предмет того, что назначенные полномочия: - необходимы для выполнения этим лицом своих должностных обязанностей; - ограничен только тем набором прав, который минимально необходим для выполнения должностных обязанностей.
1.4 Установить систему (или системы) контроля доступа к системным компонентам, которая ограничивает доступ в соответствии со служебной необходимостью пользователя и которая настроена запрещать все, что явным образом не разрешено.	1.4 Проверить настройки системы и документацию вендора на предмет того, что система (или системы) контроля доступа реализована следующим образом: - проверить, что системы контроля доступа внедрены на всех системных компонентах; - проверить, что системы контроля доступа настроены так, чтобы права доступа пользователей назначались согласно их ролям и должностным обязанностям; - контроля доступа настроены так, чтобы по умолчанию запрещать любой доступ.

Лабораторная работа 8

Идентификация и аутентификация доступа к системным компонентам

Назначение уникального идентификатора каждому лицу, имеющему доступ, обеспечивает однозначную подотчетность каждого лица в его действиях. Если такая подотчетность реализована, то действия, производимые с критичными данными и

системами, производятся известными и авторизованными пользователями, и процессами и связь между такими действиями и совершившими их пользователями или процессами может быть отслежена.

Эффективность пароля во многом зависит от устройства и реализации системы аутентификации, в частности от того, насколько часто злоумышленник может пытаться ввести пароль и какие меры безопасности предпринимаются для защиты паролей пользователей в точке ввода, в момент передачи и во время хранения.

Уникально идентифицируя каждого пользователя – вместо использования одного идентификатора для нескольких работников – организация может устанавливать индивидуальную ответственность работников за их действия и эффективно вести журнал регистрации событий по каждому из них. Это поможет ускорить разрешение проблем и противодействие им, когда обнаруживаются случаи некорректного использования или злого умысла.

Если механизм блокировки учетных записей не реализован, злоумышленник может непрерывно пытаться подобрать пароль вручную или с использованием автоматизированных средств (программ перебора паролей) до тех пор, пока ему это не удастся, и он не получит доступ к учетной записи пользователя. Если учетная запись пользователя блокируется в результате непрекращающихся попыток подбора пароля, защитные меры в виде задержки активации заблокированных учетных записей помогут остановить злоумышленника от непрерывного подбора пароля (он будет вынужден остановиться, по крайней мере, на 30 минут до автоматической активации учетной записи). Кроме того, если будет запрошена повторная активация, администратор или специалист технической поддержки может установить, действительно ли ее запросил владелец учетной записи.

Требования PCI DSS	**Проверочные процедуры**
1.1 Назначить всем пользователям уникальные учетные записи, прежде чем предоставить им доступ к системным компонентам или ДДК.	1.1 В выборке учетных записей привилегированных и обычных пользователей проверить связанные с ними авторизации и проверить настройки системы на предмет того, что каждая учетная запись обычного и привилегированного пользователей наделена только теми полномочиями, которые указаны в утверждающем документе.
1.2 Отзывать доступ у каждого уволенного пользователя.	1.2 Сделать выборку пользователей, уволенных за прошедшие шесть месяцев, и проанализировать текущие списки доступа – как *локального, так и удаленного, на предмет того, что учетные записи таких пользователей заблокированы или удалены из списков доступа.* Убедиться, что все физические средства аутентификации (например, смарт-карты, токены и т. д.) были возвращены или деактивированы.
1.3 Блокировать идентификатор пользователя не более чем после шести неудачных попыток входа подряд.	1.4 Проверить настройки системной конфигурации в выборке системных компонентов на предмет того, что в параметрах аутентификации установлено требование, чтобы учетная запись пользователя блокировалась не более чем

	после шести неудачных попыток входа.
1.4 Установить период блокировки идентификатора пользователя равным 30 минутам или до тех пор, пока его не разблокирует администратор.	1.4 Проверить настройки системной конфигурации в выборке системных компонентов на предмет того, что учетная запись пользователя блокируется не менее чем на 30 минут, либо до тех пор, пока его не разблокирует администратор.
1.5 Привести все учетные данные для аутентификации (например, пароли и (или) парольные фразы) к нечитаемому виду с использованием стойкой криптографии, когда они передаются или хранятся на любых системных компонентах.	1.5 а Проверить документацию вендора и настройки системной конфигурации на предмет того, что пароли защищены с использованием стойкой криптографии во время их передачи и хранения. 1.5 б Проверить файлы паролей в выборке системных компонентов на предмет того, что пароли хранятся в нечитаемом виде. 1.5 с Проверить передачу данных в выборке системных компонентов на предмет того, что пароли передаются в нечитаемом виде.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-4: Обладает способностью к разработке компонентов системы управления базами данных, отладке разрабатываемой системы управления базами данных, документированию разработанной системы управления базами данных в целом и ее компонентов и сопровождению созданной системы управления базами данных		
ПК-4.1	Определяет необходимость разработки компонентов системы управления базами данных	***Перечень теоретических вопросов*** 1. Защита вычислительной сети. 2. Конфигурация компонентов информационной инфраструктуры. 3. Защита хранимых данных о держателях карт. 4. Защита передаваемых данных о держателях карт. 5. Антивирусная защита информационной инфраструктуры. 6. Разработка и поддержка информационных систем. 7. Управление доступом к данным о держателях карт. 8. Механизмы аутентификации. 9. Физическая защита информационной инфраструктуры. 10. Протоколирование событий и действий. 11. Контроль защищенности информационной инфраструктуры. 12. Управление информационной безопасностью.
ПК-4.2	Оценивает качество разработки компонентов системы управления базами данных	***Практические задания*** 1. Для оценки соответствия требованиям PCI DSS именно поставщиков услуг хостинга с общей средой: — сделать выборку серверов (под управлением Microsoft Windows и Unix (Linux) из репрезентативной выборки размещенных ТСП и поставщиков услуг; — выполнить проверки, на предмет того, что эти поставщики защищают среду и данные размещенных у них организаций (ТСП и поставщиков услуг). 2. Проверить, что поставщик услуг хостинга с общей средой обеспечивает ведение журналов регистрации событий следующим образом:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		- журналы для распространенных приложений сторонних производителей включены; - журналы активны по умолчанию; - журналы доступны владеющей организации для изучения; - месторасположения журналов доведены до сведения владеющей организации. ***Задания на решение задач из профессиональной области, комплексные задания*** Проверить результаты тестирования на проникновение на предмет того, что: - тест на проникновение для проверки средств сегментации осуществляется, как минимум, каждые 6 месяцев и после любого изменения средств и (или) методов сегментации; - тест на проникновение распространяется на все используемые средства и (или) методы сегментации; - тест на проникновение проверяет, действительно ли механизмы и (или) методы сегментации эффективно работают и изолируют все системы, находящиеся в среде ДДК, от остальных.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Экзамен по данной дисциплине проводится в устной форме по экзаменационным билетам, каждый из которых включает 2 теоретических вопроса и одно практическое задание.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.