Оценочные материалы при формировании программ практик

Направление: 10.04.01 Информационная безопасность
Направленность (профиль): Безопасность информационных систем
Название практики: Преддипломная практика

Формируемые компетенции:

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при защите отчета по практике

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Экзамен или зачет с оценкой
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо

Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

Описание шкал оценивания
Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворитель	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстриро-вать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной	Обучающийся демонстрирует способность к самостоятельно-му применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень контрольных вопросов и заданий на практику

Вопросы к защите отчета по преддипломной практике

Раздел 1. Методология научного исследования.

Основания методологии науки. Характеристика научной деятельности. Средства и методы научного исследования. Организация процесса проведения исследования. Организация коллективного научного исследования.

Вопросы по разделу.

1. Философско-психологические и системотехнические основания.
2. Науковедческие основания.
3. Особенности научной деятельности.
4. Принципы научного познания.
5. Средства научного исследования.
6. Методы научного исследования.
7. Фаза проектирования научного исследования.
8. Технологическая фаза научного исследования.
9. Рефлексивная фаза научного исследования.
10. Методы математического планирования эксперимента.

Литература по разделу.

1. Пижурин А.,Пятков В. Методы и средства научных исследований. - М.: НИЦ ИНФРА-2015. – 264с.
2. Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. -2014. – 280 с.

Раздел 2. Организационно-правовые механизмы обеспечения информационной безопасности.

Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов.

Вопросы по разделу.

1. Информация как объект правового регулирования.
2. Законодательство РФ в области информационной безопасности.
3. Правовой режим защиты государственной тайны.
4. Правовые режимы защиты конфиденциальной информации.
5. Лицензирование и сертификация в информационной сфере.
6. Правовое регулирование оперативно-розыскных мероприятий в оперативно-розыскной и частной детективной и охранной деятельности.
7. Международное законодательство в области защиты информации.
8. Информационная безопасность и современные информационные технологии.
9. Организационные источники и каналы утечки информации.
10. Экономика информационной безопасности. Защита информации в экстремальных ситуациях.
11. Система организационной защиты информации.
12. Цели и задачи организационной защиты информации, ее связь с правовой защитой информации.
13. Средства и методы физической охраны объектов.
14. Порядок проведения аттестации объектов информатизации.
15. Организационные мероприятия по защите конфиденциальной информации.

Литература по разделу.

1. Федеральный закон Российской Федерации "Об информации, информатизации и защите информации" (№ 24-03 от 20.02.1995 г.).

2. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).

3. Березюк Л.П. Организационное обеспечение информационной безопасности: учеб. пособие/ Л. П. Березюк; ДВГУПС. Каф. "Информационные технологии и системы". - Хабаровск: Изд-во ДВГУПС, 2012. - 188 с.:

Раздел 3. Теоретические основы компьютерной безопасности.

Архитектура электронных систем обработки данных; формальные модели; модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; стандарты по оценке защищенных систем; управление процессами функционирования систем защиты; парольные системы.

Вопросы по разделу.

1. Категории информационной безопасности.
2. Систематика методов и механизмов обеспечения компьютерной безопасности.
3. Понятие угроз безопасности, их классификация и идентификация
4. Политика безопасности. Субъектно-объектная модель компьютерной системы в процессах коллективного доступа к информационным ресурсам.
5. Монитор безопасности. Основные типы политик безопасности.
6. Общая характеристика моделей дискреционного доступа. Пятимерное пространство Хартсона.
7. Модели дискреционного доступа на основе матрицы доступа.
8. Модель распространения прав доступа Харрисона-Руззо-Ульмана (HRU).
9. Модель TAKE-GRANT.
10. Общая характеристика модели мандатного доступа.
11. Модель Белла-ЛаПадулы.
12. Понятие и общая характеристика скрытых каналов утечки информации.
13. Дискреционная модель Кларка-Вильсона.
14. Парольные системы. Выбор пароля. Требования к паролю. Количественные характеристики пароля.
15. Методология построения систем защиты информации в АС. Основные этапы разработки защищенных АС. Жизненный цикл АС. ГОСТ 34.601

Литература по разделу.

1. Грушо А.А. и др. Теоретические основы компьютерной безопасности. –М: Академия, 2011, - 271 с.
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: http://e.lanbook.com/view/book/5150/
3. Шестухина, В.И. Теоретические основы компьютерной безопасности: учеб.пособие / В.И. Шестухина. – Хабаровск: Изд-во ДВГУПС, 2012. – 174с.

Раздел 4. Безопасность систем баз данных.

Общие принципы построения баз данных: реляционная, иерархическая и сетевая модели; распределенные базы данных. Средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС. Журнализация, средства создания резервных копии и восстановления баз данных. Технологии удаленного доступа к системам баз данных. Аспекты информационной безопасности баз данных. Угрозы информационной безопасности баз данных. Политика безопасности. Контроль доступа к базе данных.

Вопросы по разделу.

1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных.
2. Критерии качества баз данных.
3. Сущность понятия безопасности баз данных.
4. Архитектура систем управления базами данных.
5. Источники угроз информации баз данных.

6. Классификация угроз информационной безопасности баз данных.
7. Угрозы, специфичные для систем управления базами данных.
8. Аутентификация и идентификация пользователей.
9. Методы дискреционного разграничения доступа.
10. Реализация мандатной модели доступа.
11. Обеспечение согласованности данных в многопользовательском режиме обработки.
12. Типы блокировок.
13. Аудит систем баз данных.
14. Концептуальное моделирование: недостатки реляционной модели данных для моделирования предметной области, определение концептуальной модели и способы представления.
15. Характеристики эффективной базы данных.

Литература по разделу.

1. Смирнов С.Н. Безопасность систем баз данных. Учебное пособие М. Гелиос 2011 г.- 352 с.
2. Гурвиц Г.А. Microsoft Access 2010. Разработка приложений на реальном примере. СПб.: БХВ-Петербург, 2010 – 496 с. – ил.

Раздел 5. Криптографические методы защиты информации.

История криптографии; характер криптографической деятельности; шифры и их свойства; композиции шифров; системы шифрования с открытыми ключами; виды информации, подлежащие закрытию, их модели и свойства; криптографическая стойкость шифров; модели шифров; основные требования к шифрам; совершенные шифры; теоретико-информационный подход к оценке криптостойкости шифров; вопросы практической стойкости; имитостойкость и помехоустойчивость шифров; принципы построения криптографических алгоритмов; криптографические хеш-функции; электронная цифровая подпись.

Вопросы по разделу.

1. Криптография. Основные термины и определения.
2. Классификация криптографических систем. Симметричные шифры.
3. Шифры замены. Шифры перестановки. Шифры гаммирования. Основные методы шифрования.
4. Схемы режима шифрования DES-ECB, DES-CBC, DES-CPB и DES-OFB.
5. Шифрование с открытым ключом. Основные понятия.
6. Алгоритм шифрования RSA.
7. Хэш-функции. Основные понятия и разновидности.
8. Криптографические протоколы. Протоколы обмена ключами.
9. Протоколы аутентификации. Разновидности и краткая характеристика.
10. Парольная идентификация/аутентификация.
11. Идентификация/аутентификация с помощью биометрических данных.
12. Электронная цифровая подпись. Общие сведения и разновидности.
13. Электронные платежи.
14. Основные сведения о криптоанализе и атаки на криптосистемы.
15. Компьютерная стеганография.

Литература по разделу.

1. Федеральный закон Российской Федерации "Об информации, информатизации и защите информации" (№ 24-03 от 20.02.1995 г.).
2. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).
3. Федеральный закон Российской Федерации "О персональных данных" (№ 152 от 27.07.2006 г.).
4. Федеральный закон Российской Федерации "Об электронной цифровой подписи" (№ 1-ФЗ от 26.12.2001 г.).
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2012 – 816 с. – ил.

Раздел 6. Обеспечение безопасности современных серверов баз данных.

Рекомендации по защите баз данных. Формирование защищенной среды. Предоставление разрешений через учетные записи служб. Защита файлов баз данных. Обеспечение безопасности сети.

Шифрование данных на диске. Защищенная среда баз данных. Защита от инсайдерских атак.

Вопросы по разделу.

1. Обзор возможностей MS SQL Server 2014.
2. Серверы баз данных. Административные задачи управления сервером баз данных.
3. Архитектура вычислительной среды MS SQL Server, установка и настройка компонентов.
4. Основные задачи администрирования серверов баз данных. Объекты администрирования.
5. Структура базы данных в MS SQL Server. Системные и пользовательские таблицы. Назначение системных таблиц, хранимых процедур.
6. Архитектура информационной безопасности сервера баз данных. Режимы аутентификации в MS SQL Server: проверка подлинности Windows, проверка средствами MS SQL Server, цифровые сертификаты.
7. Защита данных. Использование ролевой модели. Роли пользователей на уровне сервера баз данных. Инструменты управления ролями пользователей.
8. Создание и управление пользовательскими базами данных. Резервное копирование.
9. Пользователь и схема MS SQL Server. Встроенные пользователи.
10. Хранимые процедуры MS SQL Server. Пользовательские функции MS SQL Server.
12. Настройка MS SQL Server с помощью утилиты MS SQL Server Management Studio.
13. Субъекты безопасности. Роли пользователей на уровне базы данных. Инструменты управления ролями пользователей на уровне базы данных.
14. Средства мониторинга и анализа работы MS SQL Server. Журналы транзакций, их назначение.
15. Резервное копирование и восстановление данных. Модели восстановления данных MS SQL Server, их особенности.

Литература по разделу.

1. Бондарь А. Microsoft SQL Server 2014 в подлиннике. СПб.: БХВ-Петербург, 2014 – 592 с. – ил.
2. Dewson R. Beginning SQL Server for Developers. Apress, 2014 – 684 с. – ил.

Раздел 7. Обеспечение безопасности корпоративных систем.

Структура корпораций и предприятий; архитектура корпоративных ин-формационных систем. Создание концептуального плана защиты сетевой инфраструктуры. Проектирование логической инфраструктуры защиты сети. Проектирование физической инфраструктуры защиты сети. Проектирование безопасного управления сетью. Проектирование инфраструктуры обновления системы безопасности. Проектирование защиты межсетевого взаимодействия.

Вопросы по разделу.

1. Состав корпоративной информационной системы.
2. Бизнес-факторы, влияющие на проект защиты корпоративной информационной системы.
3. Проектирование защиты сети путем разбиения ее на сегменты.
4. Проектирование репликации Active Directory через брандмауэры.
5. Проектирование защиты данных внутри сети.
6. Источники угроз информации корпоративной системы.
7. Реализация принципа наименьших привилегий при обеспечении информационной безопасности.
8. Действия при проектировании безопасного администрирования.
9. Разработка стратегии аутентификации. Проектирование модели доверия для леса и домена.
10. Проектирование проверки подлинности в гетерогенной сети.

Литература по разделу.

1. Лецкий Э.К., Яковлев В.В. Корпоративные информационные системы на железнодорожном транспорте, 2014. — 256 с.
2. Хомоненко А.Д. и др. Модели информационных систем: учеб. пособие. 2015. — 188 с.
3. Корниенко А.А. Информационная безопасность и защита информации на железнодорожном транспорте. Ч.1. 2014. — 440 с.
4. Корниенко А.А. (под ред.). Информационная безопасность и защита информации на железнодорожном транспорте. Ч.2. 2014. — 448 с.

3. Оценка ответа обучающегося на контрольные вопросы, задания по практике.

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворитель	Удовлетворитель	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам.	Значительные погрешности.	Незначительные погрешности.	Полное соответствие.
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать	Полное несоответствие критерию.	Значительное несоответствие критерию.	Незначительное несоответствие критерию.	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер.
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.