МЕЖДИСЦИПЛИНАРНОЕ ВСТУПИТЕЛЬНОЕ ИСПЫТАНИЕ В МАГИСТРАТУРУ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (демонстрационный вариант)

Вступительное испытание состоит из двух частей:

1. Тестирование (всего 25 вопросов).
2. Выполнение творческих заданий.

Критерии оценивания:

Положительные ответы	**Количество баллов**
Часть 1. Тестирование	
На каждый отдельный тест	**2**
Максимально количество баллов за часть 1	***50***
Часть 2. Выполнение творческих заданий	
на один вопрос	30
на два вопроса	40
на три вопроса	50
Максимально количество баллов за часть 2	***50***
Общее количество баллов за вступительное испытание	**100**

ДЕМОНСТРАЦИОННЫЙ ВАРИАНТ ЗАДАНИЯ

Часть 1. Тестирование

Укажите один вариант ответа

1. Проектирование это:

- процесс создания в заданных условиях описания несуществующего объекта на базе первичного описания
- первоначальное описание объекта проектирования
- процесс, который заключается в получении и преобразовании исходного описания объекта в конечный описание на основе выполнения комплекса работ исследовательского, расчетного и конструкторского характера
- вторичное описание объекта

2. Первым этапом разработки системы защиты информационной системы является:

- анализ потенциально возможных угроз информации
- изучение информационных потоков
- стандартизация программного обеспечения
- оценка возможных потерь

3. При моделировании надежность системы защиты информации определяется:

- усредненным показателем
- самым слабым звеном
- количеством отраженных атак

- самым сильным звеном

4. При моделировании криптосистемы главным параметром является показатель:

- скорость шифрования
- безошибочность шифрования
- надежность функционирования
- крипто стойкость

5. Основным способом противодействия угрозам «социальной инженерии» при моделировании защиты информации является:

- повышение надежности криптографических алгоритмов
- информационная работа с персоналом предприятия
- страхование информационных рисков
- нет правильного ответа

6. Моделирование функцией защиты информации это совокупность исследовательских отдельных процессов в виде:

- множества действий по проведение функционально однородных мероприятий, осуществляемых на объектах обработки защищаемой информации различными средствами, способами и методами с целью обеспечения заданных уровней обеспечения информационной безопасности;
- однородных, в функциональном отношении, множества задач, обеспечивающих полную или частичную реализацию одной или нескольких целей;
- организованных возможностей средств, методов и мероприятий, используемых на объекте обработки информации с целью осуществления защиты;
- нет правильного ответа

7. Основными функциями службы информационной безопасности автоматизированных систем являются:

- оценка состояния защищенности АС, обновление компонентов системы с глобального сервера, обнаружение сетевых узлов, открытых портов, анализ защищенности web-приложений, координацию расследования инцидентов в информационно-телекоммуникационной сфере
- повышение эффективности продаж компании, анализ эффективности рекламы, управление знаниями компании
- контроль всех каналов коммуникаций с клиентами, визуализация данных всеми популярными диаграммами (гистограммы, секторные диаграммы, воронки и т.д.)
- все ответы правильные

8. Что не входит в меры обеспечения информационной безопасности компьютерных систем?

- Обеспечение четкого регламента хранения данных, фиксация формул расчета данных, обеспечение взаимосвязи данных в области ИБ
- Управление доступом, обеспечение доверенной загрузки, идентификация и аутентификация, управление доступом, ограничение программной среды
- Защита машинных носителей информации, обеспечение целостности данных, регистрация событий, контроль и анализ защищенности данных
- нет правильного ответа

9. Что не является уровнем безопасности?

- Ограничение программной среды, механизм вывода,

пользователь, предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации
- Антивирусное ПО, разграничение доступа, межсетевой экран, политика безопасности
- Система предотвращения (обнаружения) вторжений, контроль физического доступа, осведомлённость пользователей, сертификация
- Все ответы правильные

10. Угрозой безопасности операционной системы (ОС) не является:
- Механизм вывода, интерфейс пользователя, управление политикой безопасности, криптографические функции
- Использование уязвимостей самой ОС, видеокарта, блок преобразования знаний
- Блок формализации, интерфейс естественно-языкового преобразования, анализатор сигналов
- Нет правильного ответа

11. Что из перечисленного не является вредоносным программным обеспечением?
- QlikView, Klipfolio
- Руткит (rootkit), фишинговая программа
- Ботнеты, онлайновый фишинг
- Все ответы правильные

12. Какое шифрование используется для защиты электронной почты?
- ассиметричное
- симметричное
- асинхронное
- все ответы правильные

13. Основной целью совершенствования нормативно-правового обеспечения информационной безопасности является:
- устранение пробелов в законодательстве, препятствующих организации эффективного противодействия угрозам.
- создание системы сбора и анализа данных об источниках угроз информационной безопасности.
- создание условий для ликвидации, предупреждения и пресечения проявлений угроз безопасности основных объектов национальных интересов
- создание системы сбора и анализа данных об источниках угроз информационной безопасности.

14. К какому виду закрытой информации относится информация с грифом ДСП:
- государственная тайна.
- конфиденциальная информация
- государственная тайн и конфиденциальная информация.
- ни одно из перечисленного.

15. Использование профилей защиты информации связано с задачей?
- стандартизации наборов требований к информационным продуктам, оценке безопасности, проведении сравнительного анализа уровней безопасности различных изделий ИТ
- стандартизации наборов требований к информационным продуктам.
- оценке безопасности.

- проведении сравнительного анализа уровней безопасности различных изделий ИТ.

16. Требования по информационной безопасности зависят от?

- класса защищенности информационных объектов
- результата оценки безопасности
- ценности информации
  развития соответствующих средств защиты в настоящий момент времени

17. С помощью чего осуществляется реализация системы управления информационной безопасности?

- на основании применения необходимых механизмов безопасности.
- на основании политики безопасности
- на основании внедрения 4-х фазной модели PDCA.
- на основании методических указаний.

18. Какую цель преследует стандарт системы менеджмента информационной безопасности?

- Выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон
- Выбор соответствующих мер управления пожарной безопасностью, предназначенных для защиты имущества.
- Выбор соответствующих правовых мер, предназначенных для защиты имущественных активов.
- Ничего из вышеперечисленного.

19. В соответствии с Доктриной информационной безопасности РФ информационная сфера – это совокупность:

- информации, объектов информатизации, информационных систем;
- информации, объектов информатизации, информационных систем, сети "Интернет" и сетей связи;
- информации, объектов информатизации, информационных систем, сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации;
- информации, объектов информатизации, информационных систем, сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, и механизмов регулирования соответствующих общественных отношений .

20. Стандарт ISO 17799 выделяет следующие виды активов:

- информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.)
- сотрудники компании, их квалификация и опыт
- сервисы (поддерживающая инфраструктура)
- все вышеперечисленное

21. Служба защиты информации (СЗИ) – это:

- государственное учреждение по защите информации;
- специализированная организация по физической защите информационных объектов;

- это самостоятельное структурное подразделение в рамках деятельности организации, тесно связана со службами охраны и объектового режима, составляет основу всей системы обеспечения информационной безопасности;
- все ответы правильные.

22. Обеспечение информационной безопасности – это:

- осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных мер по прогнозированию, обнаружению, сдерживанию и предотвращению информационных угроз и ликвидации последствий их проявления;
- осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических мер по прогнозированию, обнаружению, сдерживанию, предотвращению информационных угроз и ликвидации последствий их проявления;
- осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;
- все ответы правильные.

23. Кому непосредственно подчиняется служба информационной безопасности?

- владельцу предприятия;
- владельцу предприятия и лицу которому тот подчиняется;
- руководителю предприятия, либо лицу, которому тот делегировал свои права по руководству ее деятельностью;
- начальнику службы безопасности .

24. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?

- информация;
- запатентованная информация ;
- закрываемая собственником информация;
- коммерческая тайна.

25. При защиты информации укажите как называют взломщиков, которые воруют информацию с помощью компьютера, выкачивая целые информационные банки данных?

- фракеры
- хакеры
- нет правильного ответа
- крэкеры

Часть 2. Творческие задания

Сформулируйте ответы на следующие поставленные вопросы (по прогнозируемому направлению исследования магистерской диссертации):

Пример предполагаемой темы магистерской диссертации (решаемая проблема) **«Интеграция системы ИБ в технологию промышленного Интернета для АО «НПК «СПП» («Системы прецизионного приборостроения» г. Москва)**

1. Что предполагается Вами **рассматривать** **как основной объект исследования** ***в предполагаемой магистерской диссертации по информационной безопасности (т.е. необходимо*** **обозначить корпоративное предприятие /организацию, учреждение, фирму/ и сферу его деятельности)?**

Ответ:

Объектом исследования магистерской диссертации выступает региональная промышленная корпорация «НПК» СПП» (далее – Корпорация) самостоятельная группа предприятий, организационно-обособленный хозяйствующий субъект с правами юридического лица, который производит и сбывает товары, выполняет работы, оказывает услуги как на территории России, так и за рубежом.

Предметом исследования выступает процесс обеспечения ИБ Корпорации, которая использует технологию Промышленный интернет.

Гипотеза исследования: качество обеспечения ИБ Предприятия повысится, если внедрить в систему ИБ:

1. Подсистему интеллектуального мониторинга инцидентов, основными функциями которой являются:

– оценка информационной обстановки;

– выявление инцидентов;

– определение наиболее опасных инцидентов;

– выработка целесообразных мер по ИБ;

– целесообразное информационное воздействие на реализуемые угрозы ИБ локальных объектов;

– оповещение должностных лиц.

2. Единую интеллектуальную интеграционную платформу Промышленного интернета, которая имеет:

– продвинутый набор модулей создания и внедрения приложений промышленного Интернета вещей;

– программную платформу и ПО для внедрения подсистемы автоматизированного интеллектуального мониторинга и управления инцидентами и устройствами безопасности;

– гибкую операционную систему для периферийных вычислений и аналитики

– единую основу для IoT сервисов в сетях и облаках

А также:

– обеспечивает автоматическое регистрирование инцидентов;

– способна выделять ложные срабатывания;

– имеет самый широкий спектр оповещений об инцидентах;

– имеет функцию формирования отчетности по результатам аудита;

– имеет самые низкие системные требования;

– обеспечивает создание резервных копий средствами СУБД, без использования внешних средств;

2. Какая подсистема (или структурный компонент, или наиболее существенная /типовая/ локальная система информационной безопасности) для выбранного объекта исследования предполагается Вами рассматривать **как предмет научного исследования** ***магистерской диссертации (т.е.*** **сформулировать предполагаемое уязвимое звено** ***в исследуемой корпоративной системе информационной безопасности)?***

Примерный ответ:

В ходе исследования предполагается решение следующих **задач**:

1. Проанализировать особенности функционирования Предприятия и его существующей системы ИБ.
2. Выявить существующие недостатки в СУИБ Предприятия.
3. Вынести предложения по совершенствованию СУИБ Предприятия.
4.

Научная новизна исследования заключается в использовании нового метода обеспечения ИБ Промышленного интернета Предприятия, путем внедрения в его СУИБ подсистемы автоматизированного интеллектуального мониторинга инцидентов ИБ.

Теоретическая значимость исследования заключается в расширении научных представлений о технологии и организации СУИБ технологии IoT…

Практическая значимость исследования состоит в его ориентированности на выполнение реальных производственных задач по обеспечению ИБ в условиях...

3. Сформулировать в общем виде возможную идею (гипотезу) основы построения прогнозируемого проекта, как **новую (перспективную) технологию по менеджменту (управлению) ИБ** ***для рассматриваемого предмета научного исследования в выбранной корпоративной системе информационной безопасности.***

Примерный ответ:

Теоретико-методологической основой исследования являются идеи, изложенные в статьях и научной литературе зарубежных и российских периодических изданий. Основными источниками, раскрывающими теоретические основы организации СУИБ технологии Интернет вещей, явились работы Барскова А.А., Куприяновского В.П., Намиота Д.Е., Дрожжинова В.И., Иванова М.О. и другие. В данных источниках подробно рассмотрены многие аспекты информационных технологий и походов по обеспечению ИБ Интернета Вещей на промышленных предприятиях, а также принципы…

На защиту могут быть вынесены следующие положения:

1. Проведенный анализ позволит выявить существующие проблемы обеспечения ИБ Корпорации, использующего технологию Промышленного интернета. Решение..
2. Таким образом, предложенная система автоматизации процессов управления инцидентами ИБ позволит повысить…
3. Вариант оценки эффективности, предложенной СУИБ IIoT и её документационное обеспечение управления: …