МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования«Поволжский государственный университет сервиса»

(ФГБОУ ВО «ПВГУС»)

|  |  |  |  |
| --- | --- | --- | --- |
| УТВЕРЖДЕНО |  | | |
| на заседании Высшей школы интеллектуальных систем и кибертехнологий | | | |
|  | | | |
| Протокол от | 02.12.2022г. | № | 4 |

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

(фонд оценочных средств)

для проведения промежуточной аттестации по дисциплине

|  |
| --- |
| **«Управление информационной безопасностью»** |

наименование дисциплины

|  |  |
| --- | --- |
| по образовательной программе высшего образования – программе | **магистратуры** |
|  | бакалавриата, специалитета, магистратуры |

**«Информационная безопасность интеллектуальных и информационно-аналитических систем»**

|  |
| --- |
|  |

наименование образовательной программы

|  |
| --- |
| **10.04.01 «Информационная безопасность»** |
| шифр, наименование направления подготовки / специальности |

|  |  |
| --- | --- |
| Составитель | Глухова Л.В., профессор, Высшая школа интеллектуальных систем и кибертехнологий, д.э.н., профессор |
|  | ФИО, должность, структурное подразделение,  ученая степень, ученое звание |

Тольятти

2022

**1. Паспорт фонда оценочных средств (далее – ФОС)**

* 1. **Планируемые результаты обучения по дисциплине**

| Код и наименование компетенции | Код и наименование индикатора  достижения компетенции |
| --- | --- |
| УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели | ИУК-3.2. Осуществляет принятие исполнительских решений в условиях спектра мнений, определение порядка выполнения заданий |
| ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание | ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации  ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации |
| ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности | ИОПК-3.1. Применяет нормативные правовые акты, методические документы при подготовке распорядительных документов по обеспечению информационной безопасности, в том числе при разработке ИАС  ИОПК-3.2. Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности |

В результате изучения дисциплины обучающийся должен:

**Владеть:**

* навыками принятия исполнительских решений в условиях спектра мнений и порядка выполнения работ по управлению информационной безопасностью
* навыками проектирования систем обеспечения информационной безопасности
* навыками работы с нормативными документами ФСТЭК при управлении информационной безопасностью.

**Уметь:**

* планировать стратегию членов команды по обеспечению информационной безопасности
* разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации
* разрабатывать проекты информационно-аналитических систем и организационно-распорядительных документов по обеспечению информационной безопасности

**Знать:**

* основные функции организации и управления работой команды исполнителей
* принципы обеспечения информационной безопасности и защиты информации и требования нормативных документов для разработки проекта технического задания
* принципы проектирования и разработки организационно-распорядительных документов по обеспечению информационной безопасности и требования нормативной базы ФСТЭК

**1.2. Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| № | Тема (раздел дисциплины)  (в соответствии с РПД) | Код компетенции и индикаторы достижения компетенций |
| 1 | Тема 1. Основные понятия науки об управлении. Системный, процессный, нормативный подходы | УК-3: ИУК-3.2  ОПК-1: ИОПК-1.1; ИОПК-1.2; |
| 2 | Тема 2. Проектирование системы управления информационной безопасностью на предприятии | ОПК-1: ИОПК-1.1, ИОПК-1.2  ОПК-3: ИОПК-3.1 , ИОПК-3.2 |
| 3 | Тема 3. Оценка рисков информационной безопасности на предприятии | УК-3: ИУК-3.2  ОПК-1: ИОПК-1.1; ИОПК-1.2  ОПК-3: ИОПК-3.1, ИОПК-3.2 |

**1.3. Система оценивания по дисциплине**

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – экзамен.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Шкалы оценки уровня сформированности результатов обучения | | Шкала оценки уровня освоения дисциплины | | |
| Уровневая шкала оценки компетенций | 100 бальная шкала, % | 100 бальная шкала, % | 5-балльная шкала,дифференцированная оценка/балл | недифференцированная оценка |
| допороговый | ниже 61 | ниже 61 | «неудовлетворительно» / 2 | не зачтено |
| пороговый | 61-85,9 | 61-69,9 | «удовлетворительно» / 3 | зачтено |
| 70-85,9 | «хорошо» / 4 | зачтено |
| повышенный | 86-100 | 86-100 | «отлично» / 5 | зачтено |

**2. Перечень оценочных материалов для проведения промежуточной аттестации**

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

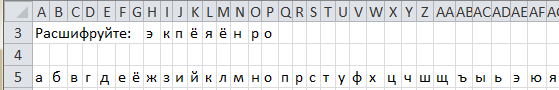
**Перечень вопросов для подготовки к экзамену**

**УК-3. ИУК-3.2:** **Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели**

1. Какой документ регламентирует обеспечение правовых условий использования электронной цифровой подписи в электронных документах?
2. Что является основным документом, обеспечивающим защиту персональных данных?
3. Под какую статью УК РФ попадает такое киберпреступление, как неправомерный доступ к компьютерной информации?
4. Дайте определение понятия «Критерий экономической безопасности - это»
5. Какой государственный стандарт содержит «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»?
6. Дайте определение информационной безопасности.
7. В виде совокупности каких уровней можно представить организационную структуру системы обеспечения информационной безопасности АС организации?
8. Дайте определение понятия «Система защиты информации (СЗИ)»
9. Дайте определение понятия «Профессиональная тайна»
10. В чём разница между служебными и коммерческими секретами?
11. Дайте определение понятия «Персональные данные»
12. Какими факторами могут быть обусловлены информационные угрозы?
13. Запишите виды информационных угроз для государства
14. Запишите виды информационных угроз для компании.
15. Запишите виды информационных угроз для личности (физического лица).
16. Дайте определение Макровируса
17. Дайте определение экономической безопасности
18. Какой документ устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации
19. Какой орган впервые определил критерии установления коммерческого мошенничества.
20. Закончите определение. Согласно Стратегии экономической безопасности РФ до 2030 года угрозы экономической безопасности – это…

**ОПК-1.. ИОПК1-1; ИОПК1-2; Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание**

1. Перечислите функции, выполняемые антивирусом Касперского.
2. Дайте краткую характеристику антивирусам сканерам
3. Дайте краткую характеристику антивирусам мониторам
4. Запишите меры профилактики заражения ПК вирусом.
5. Запишите основные пути проникновения вирусов на компьютер
6. Перечислите вредные действия вирусов.
7. Дайте определение понятия «Персональные данные»
8. Какими факторами могут быть обусловлены информационные угрозы?
9. Запишите виды информационных угроз для государства
10. Запишите виды информационных угроз для компании
11. Запишите виды информационных угроз для личности (физического лица)
12. Дайте определение Макровируса
13. Макровирусы заражают файлы – документы и электронные таблицы офисных приложений. Для анализа макровирусов необходимо получить текст их макросов. При помощи, каких команд можно это сделать для нешифрованных (не-стелс) файлов?
14. Если на компьютере нет антивирусных программ, то каким образом можно восстановить документы Word и Excel заражённых вирусом?
15. Запишите последовательность действий, которые необходимо выполнить для того, чтобы восстановить пораженные документы Word и Excel в случае того, если на компьютере нет антивирусных программ
16. Запишите, какие действия необходимо выполнить, для защиты файлов от макровирусов, если на компьютере нет антивирусных программ.
17. Запишите виды информационных угроз для государства.
18. Какие действия необходимо выполнить в MS Office чтобы зашифровать файл и задать пароль для его открытия?
19. Запишите алгоритм процесса создания архива с паролем в WinRAR. и архив будет создан с паролем.
20. Расшифруйте слово «экпёяёнро», закодированное с помощью шифра Цезаря. Известно, что каждая буква исходного текста заменяется третьей после нее буквой.



**ОПК-3. ИОПК-3.1, ИОПК-3.2.** **Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности**

1. Какие особенности проектирования и разработки организационно-распорядительных документов по обеспечению ИБ регламентированы ГОСТ Р ИСО /МЭК 27005-2010
2. Соотнести между собой процессы системы менеджмента информационной безопасности и процесса менеджмента риска информационной безопасности
3. Что должно быть реализовано в организации при управлении контентом. В соответствии с требованиями ГОСТ Р ИСО/МЭК 27005-2010
4. Перечислить в качестве примера цели менеджмента риска информационной безопасности, которые могут быть указаны в документе «Руководство по реализации» (ГОСТ Р ИСО/МЭК 27005-2010)
5. С учетом чего рекомендовано в организации формировать критерии оценки рисков ИБ?
6. Что такое идентификация риска и какова цель идентификации
7. Роль организационной структуры менеджмента риска информационной безопасности
8. Общее описание оценки риска ИБ
9. Как происходит определение активов организации для их защиты от рисков?
10. Привести пример того, в каких областях деятельности организации могут быть выявлены уязвимости
11. Привести пример последствий, которые могут быть вызваны потерей конфиденциальности, целостности и доступности
12. Привести пример, на основе чего организации могут определять операционные последствия выявленного сценария компьютерного инцидента?
13. В чем заключается управление информационной безопасностью в организации
14. Чем занимается отдел информационной безопасности в организации и что входит в его основные задачи?
15. Каково назначение процесса управления информационной безопасностью организации с точки зрения процессного подхода?
16. Назовите предпосылки разработки политики безопасности предприятия

**Вопросы (задания) для подготовки к экзамену**

**с «ключами» правильных ответов**

| № | Содержание вопроса | Правильный ответ | |
| --- | --- | --- | --- |
| **УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели** | | | | |
|  | Какой документ регламентирует обеспечение правовых условий использования электронной цифровой подписи в электронных документах? | Федеральный закон от 06.04.2011 N 63-ФЗ ред. от 23.06.2016 " Об электронной цифровой подписи | |
|  | Что является основным документом, обеспечивающим защиту персональных данных? | Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" | |
|  | Под какую статью УК РФ попадает такое киберпреступление, как неправомерный доступ к компьютерной информации? | Под статью 272 УК РФ неправомерным доступом к компьютерной информации. | |
|  | Дайте определение понятия «Критерий экономической безопасности - это» | Критерий экономической безопасности – это оценка состояния экономики с точки зрения важнейших процессов, отражающих сущность экономической безопасности | |
|  | Какой государственный стандарт содержит «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»? | ГОСТ 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» | |
|  | Дайте определение информационной безопасности. | Информационная безопасность — это набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения. | |
|  | В виде совокупности каких уровней можно представить организационную структуру системы обеспечения информационной безопасности АС организации? | Организационную структуру системы обеспечения информационной безопасности АС организации можно представить в виде, совокупности следующих уровней:   * уровень 1 - Руководство организации * уровень 2 - Подразделение ОИБ * уровень 3 - Администраторы штатных и дополнительных средств защиты * уровень 4 - Ответственные за ОИБ в подразделениях * уровень 5 - Конечные пользователи и обслуживающий персонал | |
|  | Дайте определение понятия «Система защиты информации (СЗИ)» | Система защиты информации (СЗИ) – совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации | |
|  | Дайте определение понятия «Профессиональная тайна» | Профессиональная тайна **—**информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций | |
|  | В чём разница между служебными и коммерческими секретами? | Разница в том, что служебная тайна имеет отношение к государственным органам власти, а коммерческая – к бизнесу | |
|  | Дайте определение понятия «Персональные данные» | Персональные данные — это любая информация, которая относится к конкретному человеку, или субъекту персональных данных. ФИО, мобильный телефон, email, адрес проживания, фотография, паспортные данные | |
|  | Какими факторами могут быть обусловлены информационные угрозы? | Информационные угрозы могут быть обусловлены:  - естественными факторами (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины);  - человеческими факторами | |
|  | Запишите виды информационных угроз для государства | Виды информационных угроз для государства:  - информационная война  - информационные противодействия  - кибератаки  - кибершпионаж  - распространение секретной служебной информации | |
|  | Запишите виды информационных угроз для компании. | Виды информационных угроз для компании:  - разглашение  - утечка  - несанкционированный доступ | |
|  | Запишите виды информационных угроз для личности (физического лица). | Виды информационных угроз для личности (физического лица):  - киберслежка  - онлайновое мошенничество  - фишинг (раскрытие персональных данных: логина, пароля, номера банковской карты)  - фальшивые сайты | |
|  | Дайте определение Макровируса | Макровирус – это такая разновидность компьютерных вирусов, которая заражает офисные документы в прикладных программах, имеющих средства и разрешение на исполнение последовательных макрокоманд | |
|  | Дайте определение экономической безопасности | Экономическая безопасность — состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации | |
|  | Какой документ устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации | ГОСТ Р 51275-2006. Защита информации. | |
|  | Какой орган впервые определил критерии установления коммерческого мошенничества. | Комиссия ООН по праву международной торговли | |
|  | Закончите определение. Согласно Стратегии экономической безопасности РФ до 2030 года угрозы экономической безопасности – это… | состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации. | |
| **ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание** | | | | |
|  | Перечислите функции, выполняемые антивирусом Касперского. | | Функции антивируса Касперского включают защиту в режиме реального времени, обнаружение и удаление вирусов, троянов, червей, шпионских программ, рекламного ПО, кейлоггеров, вредоносных инструментов и автодозвонщиков, а также обнаружение и удаление руткитов. | |
|  | Дайте краткую характеристику антивирусам сканерам | | Антивирусы сканеры умеют находить и лечить известные им вирусы в памяти и на диске, используют базы данных вирусов и выполняют ежедневное обновление баз данных через интернет | |
|  | Дайте краткую характеристику антивирусам мониторам | | Антивирусы мониторы выполняют постоянную защиту, в том числе от «фишинга» и спама, перехват подозрительных действий, а также проверку файлов, флеш-дисков и данных из интернета | |
|  | Запишите меры профилактики заражения ПК вирусом. | | для профилактики заражения компьютерными вирусами возможно применение действий:  - Периодическое обновление операционной системы и программного обеспечения  - Использование антивирусного ПО и программ с комплексной защитой от вредоносных файлов и постоянно обновлять их базы  - Внимательное и осторожное пользование сетью Интернет и скачивание файлов  - Периодическое резервное копирование важных данных  - По возможности пользоваться проверенными дистрибутивами  - Ограничить круг людей, имеющих доступ к ПК | |
|  | Запишите основные пути проникновения вирусов на компьютер | | Основные пути проникновения вирусов:  - дискета, на которой находятся зараженные вирусом файлы  - компьютерная сеть, в том числе система электронной почты и Internet  - жесткий диск, на который попал вирус в результате работы с зараженными программами  - вирус, оставшийся в оперативной памяти после предшествующего пользователя | |
|  | Перечислите вредные действия вирусов. | | Компьютерный вирус может выполнять следующие вредные действия:  - удаление или искажение файлов;  - изменение (порча) таблицы размещения файлов на диске, которая отвечает за целостность данных;  - засорение оперативной памяти и памяти диска пустой информацией;  - замедление работы компьютера или его полная остановка (зависание) | |
|  | Дайте определение понятия «Персональные данные» | | Персональные данные — это любая информация, которая относится к конкретному человеку, или субъекту персональных данных. ФИО, мобильный телефон, email, адрес проживания, фотография, паспортные данные | |
|  | Какими факторами могут быть обусловлены информационные угрозы? | | Информационные угрозы могут быть обусловлены:  - естественными факторами (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины);  - человеческими факторами | |
|  | Запишите виды информационных угроз для государства | | Виды информационных угроз для государства:  - информационная война  - информационные противодействия  - кибератаки  - кибершпионаж  - распространение секретной служебной информации | |
|  | Запишите виды информационных угроз для компании | | Виды информационных угроз для компании:  - разглашение  - утечка  - несанкционированный доступ | |
|  | Запишите виды информационных угроз для личности (физического лица) | | Виды информационных угроз для личности (физического лица):  - киберслежка  - онлайновое мошенничество  - фишинг (раскрытие персональных данных: логина, пароля, номера банковской карты)  - фальшивые сайты | |
|  | Дайте определение Макровируса | | Макровирус – это такая разновидность компьютерных вирусов, которая заражает офисные документы в прикладных программах, имеющих средства и разрешение на исполнение последовательных макрокоманд. | |
|  | Макровирусы заражают файлы – документы и электронные таблицы офисных приложений. Для анализа макровирусов необходимо получить текст их макросов. При помощи, каких команд можно это сделать для нешифрованных (не-стелс) файлов? | | Чтобы получить текст макросов можно воспользоваться командами меню.  Например, При помощи команд: Меню/Сервис/Макрос | |
|  | Если на компьютере нет антивирусных программ, то каким образом можно восстановить документы Word и Excel заражённых вирусом? | | Для восстановления документов Word и Excel заражённых вирусом достаточно сохранить пораженные файлы в текстовом формате RTF, содержащем практически всю информацию из первоначальных документов и не содержащем макросы | |
|  | Запишите последовательность действий, которые необходимо выполнить для того, чтобы восстановить пораженные документы Word и Excel в случае того, если на компьютере нет антивирусных программ | | Для этого нужно выполнить следующие действия:  1. Выберите пункты меню «Файл» – «Сохранить как».  2. В открывшемся окне в поле «Тип файла» выберите «Текст в формате RTF».  3. Выберите команду «Сохранить», при этом имя файла оставьте прежним.  4. В результате появится новый файл с именем существующего, но с другим расширением.  5. Далее удалите все зараженные документы.  6. Восстановите документы из RTF-файлов в соответствующий формат файла | |
|  | Запишите, какие действия необходимо выполнить, для защиты файлов от макровирусов, если на компьютере нет антивирусных программ. | | меню: «Сервис» – «Макрос» – «Безопасность». В открывшемся окне на вкладке «Уровень безопасности» отметьте пункт «Очень высокая» | |
|  | Запишите виды информационных угроз для государства. | | Виды информационных угроз для государства  - информационная война  - информационные противодействия  - кибератаки  - кибершпионаж  - распространение секретной служебной информации | |
|  | Какие действия необходимо выполнить в MS Office чтобы зашифровать файл и задать пароль для его открытия? | | Чтобы зашифровать файл и задать пароль для его открытия, выполните действия:  1. Нажмите кнопку MS Office , наведите указатель мыши на пункт «Подготовить» и выберите пункт «Зашифровать документ».  2. В диалоговом окне «Шифрование документа» введите пароль в поле «Пароль» и нажмите кнопку «ОК».  3. В диалоговом окне «Подтверждение пароля» введите пароль еще раз в поле «Подтверждение» и нажмите кнопку «ОК». Чтобы сохранить пароль, сохраните файл | |
|  | Запишите алгоритм процесса создания архива с паролем в WinRAR и архив будет создан с паролем | | Для создания архива с паролем в WinRAR нужно кликнуть по документу правой кнопкой мыши и выбрать пункт «Добавить в архив». В окне создания архива, нажать кнопку «Установить пароль», и дважды ввести его (при необходимости включить шифрование имен файлов). После этого нажмите «ОК» | |
|  | Расшифруйте слово «экпёяёнро», закодированное с помощью шифра Цезаря. Известно, что каждая буква исходного текста заменяется третьей после нее буквой. | | Правильный ответ: антивирус | |
| **ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности** | | | | |
|  | Какие особенности проектирования и разработки организационно-распорядительных документов по обеспечению ИБ регламентированы ГОСТ Р ИСО /МЭК 27005-2010 | | Особенностью ГОСТ Р ИСО/МЭК 27005-2010 является то, что в нем прописано из чего состоит процесс менеджмента риска.  Процесс менеджмента риска ИБ состоит из:  - установления контекста;  - оценки риска;  - обработки риска;  - принятия риска;  - коммуникаций риска;  - мониторинга риска;  - переоценки риска информационной безопасности.  Для этого разрабатывается модель компетенций персонала по управлению рисками ИБ. | |
|  | Соотнести между собой процессы системы менеджмента информационной безопасности и процесса менеджмента риска информационной безопасности | | Процессы системы менеджмента информационной безопасности (СМИБ) можно соотнести с процессами управления рисками информационной безопасности так, как показано в таблице | |
|  | Что должно быть реализовано в организации при управлении контентом. В соответствии с требованиями ГОСТ Р ИСО/МЭК 27005-2010 | | При организации управления контентом как процессом должно быть учтено:  1) входные данные;  2) действия;  3) руководство по реализации;  4) выходные данные.  Действия должны включать определение основных критериев, необходимых для менеджмента риска ИБ, определение области применения и границ, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ.  Руководство по реализации обязательно включает цель управления рисками ИБ | |
|  | Перечислить в качестве примера цели менеджмента риска информационной безопасности, которые могут быть указаны в документе «Руководство по реализации» (ГОСТ Р ИСО/МЭК 27005-2010) | | Документ «Руководство по реализации» может иметь, например, такие цели управления:  - поддержка СМИБ;  - исполнение законодательно-нормативных требований и подтверждение проявленной организацией разумной предосторожности;  - подготовка плана обеспечения непрерывности бизнеса;  - подготовка плана реагирования на инциденты;  - описание требований ИБ для продукта, услуги или механизма. | |
|  | С учетом чего рекомендовано в организации формировать критерии оценки рисков ИБ? | | Критерии оценки рисков должны быть разработаны с учетом:  - стратегической ценности обработки бизнес-информации;  - критичности затронутых информационных активов;  - законодательно-нормативных требований и договорных обязательств;  - оперативного значения и значения для бизнеса доступности, конфиденциальности и целостности;  - ожидания и реакции причастных сторон, а также негативных последствий для нематериальных активов и репутации.  Кроме того, критерии оценки рисков могут использоваться для определения приоритетов при обработке рисков. | |
|  | Что такое идентификация риска и какова цель идентификации | | Цель идентификации риска - определить, что могло бы произойти при нанесении возможного ущерба, и получить представление о том, как, где и почему мог иметь место этот ущерб. | |
|  | Роль организационной структуры менеджмента риска информационной безопасности | | Для процесса менеджмента риска ИБ необходимо устанавливать и поддерживать организационную структуру и распределение обязанностей.  Основные роли и области ответственности, присущие этой организационной структуре:  - разработка процесса менеджмента риска ИБ, подходящего для данной организации;  - выявление и изучение причастных сторон;  - определение ролей и обязанностей всех сторон, как внутренних, так и внешних по отношению к организации;  - установление требуемых взаимосвязей между организацией и причастными сторонами, а также взаимодействия с высокоуровневыми функциями менеджмента риска организации (например, менеджмента операционного риска), а также взаимодействия с другими значимыми проектами и видами деятельности;  - определение путей передачи принятия решений на более высокий уровень и/или другим специалистам;  - определение подлежащих ведению документов.  Эта организационная структура должна одобряться соответствующим руководством организации. | |
|  | Общее описание оценки риска ИБ | | Риск представляет собой комбинацию последствий, вытекающих из нежелательного события и вероятности возникновения события. Оценка риска количественно или качественно характеризует риски и дает возможность руководителям назначать для них приоритеты в соответствии с осознаваемой ими серьезностью или другими установленными критериями.В общем виде оценка риска включает: анализ риска и оценку риска. | |
|  | Как происходит определение активов организации для их защиты от рисков? | | Активом является что-либо, имеющее ценность для организации и, следовательно, нуждающееся в защите.  При определении активов следует иметь в виду, что информационная система состоит не только из аппаратных и программных средств, но и из документов.  Определение активов следует проводить с соответствующей степенью детализации, обеспечивающей информацию, достаточную для оценки риска. Для этого в отношении каждого актива должен быть определен владелец. Владелец актива может не обладать правами собственности на актив, но он несет ответственность за его получение, разработку, поддержку, использование и безопасность. | |
|  | Привести пример того, в каких областях деятельности организации могут быть выявлены уязвимости | | Уязвимости могут быть выявлены в следующих областях:  - организация работ;  - процессы и процедуры;  - установившийся порядок управления;  - персонал;  - физическая среда;  - конфигурация информационной системы;  - аппаратные средства, программное обеспечение и аппаратура связи;  - зависимость от внешних сторон. | |
|  | Привести пример последствий, которые могут быть вызваны потерей конфиденциальности, целостности и доступности | | В результате потерями активов конфиденциальности, целостности и доступности возникают негативные последствия.  Последствием может быть снижение эффективности, неблагоприятные операционные условия, потеря бизнеса, ущерб, нанесенный репутации, и т.д. | |
|  | Привести пример, на основе чего организации могут определять операционные последствия выявленного сценария компьютерного инцидента? | | Организации должны определять операционные последствия сценариев инцидентов на основе:  - времени на расследование и восстановление;  - потерь (рабочего) времени;  - упущенной возможности;  - охраны труда и безопасности;  - финансовых затрат на приобретение специфических навыков, необходимых для устранения неисправности;  - репутации и иного "неосязаемого капитала". | |
|  | В чем заключается управление информационной безопасностью в организации | | Управление информационной безопасностью заключается в планировании, развертывании и поддержании комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности. | |
|  | Чем занимается отдел информационной безопасности в организации и что входит в его основные задачи? | | Отдел информационной безопасности в организации создается с целью обеспечения защиты информационных ресурсов организации от намеренного и ненамеренного разглашения, утери, искажения, похищения.  В задачи Отдела входит разработка и внедрение системы безопасности, а также контроль за ее работой и анализ эффективности используемых средств защиты информации. | |
|  | Каково назначение процесса управления информационной безопасностью организации с точки зрения процессного подхода? | | Процесс управления информационной безопасностью в организации — это циклический процесс, включающий:  осознание степени необходимости защиты информации и постановку задач;  сбор и анализ данных о состоянии информационной безопасности в организации;  оценку информационных рисков;  планирование мер по обработке рисков;  реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий;  мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия | |
|  | Назовите предпосылки разработки политики безопасности предприятия | | Основными предпосылками разработки политики безопасности являются:  1. Требования законодательства и государственных органов;  2. Требования международных и иных стандартов;  3. Объективная необходимость обеспечения безопасности. | |