Институт ИнЭИ
Направление подготовки 10.04.01 *Информационная безопасность*
Программа направления «*Управление информационной безопасностью*»

Банк заданий по базовой части вступительного испытания в магистратуру

Задание 1 (5 баллов)

1.1. Понятие «угроза» безопасности информации. Как можно классифицировать эти угрозы? Что такое модель угроз?

Ответ: см. ГОСТ Р 50922-2006. Национальный стандарт РФ. Защита информации. Основные термины и определения;

См. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

1.2. Понятие «уязвимость информации» в информационных системах. Способы классификации уязвимостей.

Ответ: См. ГОСТ Р 50922-2006. Национальный стандарт РФ. Защита информации. Основные термины и определения.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

1.3. Понятие «риск информационной безопасности». Опишите условия, при которых отсутствуют риски информационной безопасности.

Ответ: См. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил

1.4. Информационные активы организации: определение, классификация и инвентаризация.

Ответ: См. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

1.5. Система менеджмента информационной безопасности (СМИБ): назначение, принцип управления на основе цикла Деминга-Шухарта.

Ответ: См. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Задание 2 (5 баллов)

2.1. Понятие «коммерческая тайна». Основания отнесения сведений к «коммерческой тайне». Требования к защите коммерческой тайны.

Ответ: См. Федеральный Закон РФ №98-ФЗ 2004 года «О коммерческой тайне».

2.2. Понятие «персональные данные» (ПДН). Классификация ПДН и требования по организации их защиты.

Ответ: См. Федеральный Закон РФ №152-ФЗ 2006 года «О персональных данных».

2.3. Понятие «служебная тайна». Правовой режим служебной тайны.

Ответ: См. Указ Президента РФ №188 от 06.03.1997; Постановление Правительства РФ №1233 от 3.11.1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» (с изменениями и дополнениями).

2.4. Понятие «государственная тайна». Правовой режим «государственной тайны».

Ответ: См. Федеральный Закон РФ №5485-1 1993 года «О государственной тайне».

2.5. Назначение, сфера действия, цели и принципы защиты критической информационной инфраструктуры РФ.

Ответ: См. Федеральный Закон РФ №187 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации».

Задание 3 (10 баллов)

3.1. Система менеджмента информационной безопасности (СМИБ) на основе цикла PDCA. Организация и управление СМИБ. В каких случаях цикл PDCA повторяется?

Ответ: См. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил

3.2. Порядок оценки угроз безопасности информации. Характеристика оценки возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

Ответ: Методический документ. Методика оценки угроз безопасности информации. Утверждена ФСТЭК 5 февраля 2021г.; Банк данных угроз безопасности и уязвимостей информации (https://bdu.fstec.ru/vul).

3.3. Параметрическая модель угроз в системе менеджмента информационной безопасности. Характеристика параметров угроз.

Ответ: См. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. ил

3.4. Цели управления рисками информационной безопасности. Особенность описания рисков для случайных, природных и умышленных угроз. Оценка рисков.

Ответ: См. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил

3.5. Политика информационной безопасности: назначение, содержание, принципы разработки и ее пересмотра.

Ответ: См. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

Задание 4 (10 баллов)

4.1. Алгоритм симметричного блочного шифрования на основе сети Фейстеля. Понятие криптостойкость алгоритма.

Ответ: См. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Изд. «Горячая линия - Телеком», 2005; Хорев П.Б., Методы и средства защиты информации в компьютерных системах. М.: Серия «Учебная литература для ВПО», 2005.

4.2. Принцип реализации ассиметричного блочного шифрования на основе открытого и закрытого ключей.

Ответ: См. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Изд. «Горячая линия - Телеком», 2005; Хорев П.Б., Методы и средства защиты информации в компьютерных системах. М.: Серия «Учебная литература для ВПО», 2005.

4.3. Криптографическая хеш-функция: требования, алгоритм вычисления, область применения.

Ответ: См. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Изд. «Горячая линия - Телеком», 2005; Хорев П.Б., Методы и средства защиты информации в компьютерных системах. М.: Серия «Учебная литература для ВПО», 2005.

4.4. Методы и технологии организации простой электронной подписи в корпоративной информационной системе. Область применения.

Ответ: См. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Изд. «Горячая линия - Телеком», 2005; Хорев П.Б., Методы и средства защиты информации в компьютерных системах. М.: Серия «Учебная литература для ВПО», 2005.

4.5. **Методы и технологии организации усиленной электронной подписи в корпоративной информационной системе. Область применения.**

Ответ: См. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Изд. «Горячая линия - Телеком», 2005;

Хорев П.Б., Методы и средства защиты информации в компьютерных системах. М.: Серия «Учебная литература для ВПО», 2005.

Задание 5 (20 баллов)

5.1. На схеме (Рис.1) приведена последовательность обработки рисков информационной безопасности, взятая из ISO/IEK 27005 – 2018.

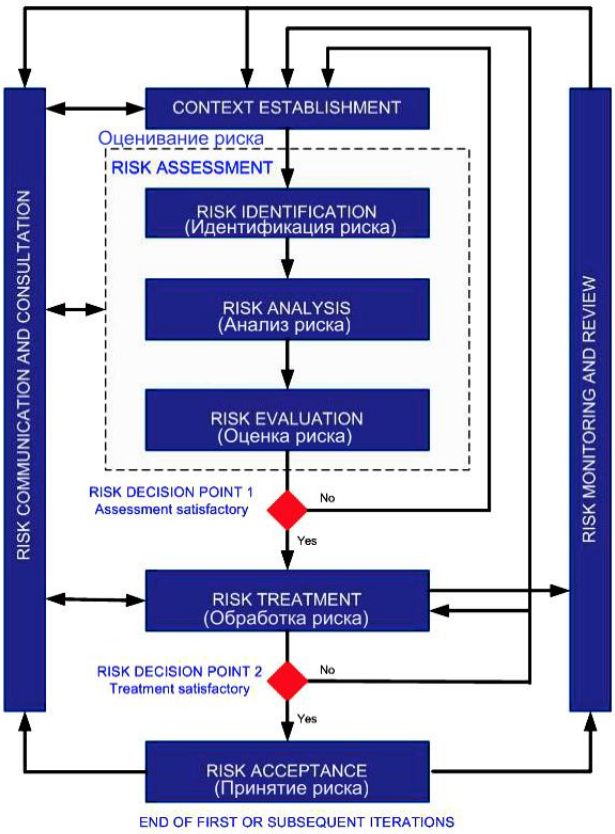

Рис.1. Схема последовательности обработки рисков информационной безопасности

Поясните все этапы обработки рисков на этом рис.1. Дайте письменный ответ, при каких условиях осуществляется перевод управления на блок «Установление контекста» (Context Establishment).

Ответ: См. ISO/IEK 27005 – 2018; ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил

5.2. При каких условиях обработки рисков (Рис.1) управление со второй точки принятия решений (Risk Decision point 2) передается на блок обработки рисков и блок установления контекста (Context Establishment)? Что изменяется в условиях обработки рисков? Надо ли повторить процедуру обработки для уже принятых ранее рисков?

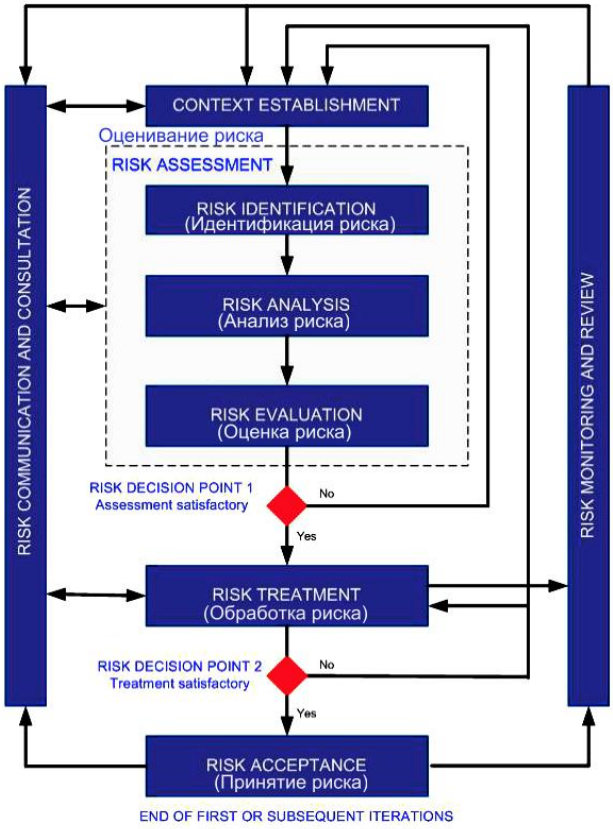

Рис.1. Схема последовательности обработки рисков информационной безопасности

Ответ: См. . ISO/IEK 27005 – 2018; ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил

5.3. Оценка риска информационной безопасности осуществляется путем сложения числовых мер оценок возможности угрозы, оценка значения уязвимости и оценки ценности актива. Числовые значения этих оценок рекомендуется брать в пределах заданных шкал [0, 1, …, 7]. Обоснуйте в каких шкалах необходимо задавать значения угроз, уязвимостей и ценности активов. Какими свойствами обладают эти измерения?

Ответ: См. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил

5.4. В стандарте ГОСТ Р ИСО/МЭК 27002-2012 года одним из условий создания защищенной информационной системы является планирование, внедрение и управление непрерывностью бизнеса. По каким параметрам оцениваются риски непрерывности бизнеса и какие при этом планируются меры контроля и управления?

Ответ: См. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

5.5. Как оценивается величина возможного ущерба при проведении оценки рисков? Как определить погрешность возможного общего предотвращенного ущерба для разработанного плана обработки рисков?

Ответ: См. Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Банк заданий по специальной части вступительного испытания в магистратуру

Задание 6 (5 баллов)

6.1. Как определяется требуемый уровень защищенности информационной системы персональных данных (ИСПДН) и для каких целей разрабатывается модель нарушителя?

Ответ: См. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

6.2. Порядок определения класса защищенности информационных систем для обработки данных в государственных информационных системах.

Ответ: См. Приказ ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

6.3. Понятие «непрерывность бизнеса» в системах управления информационной безопасность. В чем различие механизмов «доступности» и «непрерывности» в СМИБ?

Ответ: См. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

6.4. Как определить способ обработки рисков информационной безопасности?

Ответ: См. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил

6.5. С какими целями разрабатывается ключевой документ системы менеджмента информационной безопасности «Положение о применимости»? Какое содержание этого документа?

Ответ: См. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Задание 7 (5 баллов)

7.1. Понятие системы резервного копирования и требования, предъявляемые к ней. Политика резервного копирования.

Ответ: См. Хорев П.Б. Программно-аппаратная защита информации. - М.: Высшее образование. Инфра-М, 2009; Зайцев А.П., Голубятников И.В. Программно-аппаратные средства обеспечения информационной безопасности. - М.: Машиностроение, 2006;

Семененко В. А., Федоров Н. В. Программно-аппаратная защита информации. М.: Изд. Московского государственного индустриального университета, 2007;

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М.: Издательство Юрайт, 2018.

7.2. Понятие, принцип действия и основные возможности DLP-систем по предотвращению утечки информации в информационной системе организации.

Ответ: См. https://www.infowatch.ru/; https://searchinform.ru/.

7.3. Общая характеристика механизмов защиты информации, встроенных в современную отечественную **операционную систему** ASTRA LINUX

См. материалы https://www.astralinux.ru/.

7.4. Характеристика процессов аутентификации, авторизации и аудита.

Ответ: См. Хорев П.Б. Программно-аппаратная защита информации. - М.: Высшее образование. Инфра-М, 2009;

Зайцев А.П., Голубятников И.В. Программно-аппаратные средства обеспечения информационной безопасности. - М.: Машиностроение, 2006;

Семененко В. А., Федоров Н. В. Программно-аппаратная защита информации. М.: Изд. Московского государственного индустриального университета, 2007;

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018.

7.5. Характеристика функциональных возможностей и области использования технологии VPN.

Ответ: См. Хорев П.Б. Программно-аппаратная защита информации. - М.: Высшее образование. Инфра-М, 2009;

Зайцев А.П., Голубятников И.В. Программно-аппаратные средства обеспечения информационной безопасности. - М.: Машиностроение, 2006;

Семененко В. А., Федоров Н. В. Программно-аппаратная защита информации. М.: Изд. Московского государственного индустриального университета, 2007;

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018.

Задание 8 (10 баллов)

8.1. Порядок практического использования электронной подписи в соответствии с отечественным стандартом ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

См. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

8.2. Содержание программы аудита системы менеджмента информационной безопасности и этапы ее реализации.

См. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

ГОСТ Р ИСО 19011 – 2012 года. Руководящие указания по аудиту систем менеджмента.

8.3. Общая характеристика системы антивирусной защиты информации. Современные методы обнаружения компьютерных вирусов и защиты от них.

Ответ: См. Хорев П.Б. Программно-аппаратная защита информации. - М.: Высшее образование. Инфра-М, 2009; Зайцев А.П., Голубятников И.В. Программно-аппаратные средства обеспечения информационной безопасности. - М.: Машиностроение, 2006;

Семененко В. А., Федоров Н. В. Программно-аппаратная защита информации. М.: Изд. Московского государственного индустриального университета, 2007;

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018.

8.4. Интегрированные антивирусные решения и их общая характеристика: защита от спама, межсетевое экранирование, защита от использования опасных сетевых ресурсов.

Ответ: См. Хорев П.Б. Программно-аппаратная защита информации. - М.: Высшее образование. Инфра-М, 2009; Зайцев А.П., Голубятников И.В. Программно-аппаратные средства обеспечения информационной безопасности. - М.: Машиностроение, 2006;

Семененко В. А., Федоров Н. В. Программно-аппаратная защита информации. М.: Изд. Московского государственного индустриального университета, 2007;

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018.

8.5. Общая характеристика интегрированной системы технических средств охраны по предупреждению, обнаружению и ликвидаций угроз безопасности.

Ответ: См. Невский А.Ю., Баронов О.Р. Технические средства охраны. М.: ВНИИгеосистем, 2015;

Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. М.: Горячая линия-Телеком, 2014;

ГОСТ Р 51558-2008. Национальный стандарт Российской Федерации. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

Задание 9 (10 баллов)

9.1. Основные требования и содержание политики информационной безопасности организации. Какие исходные данные необходимы для её разработки и как оценить ее корректность?

Ответ: См. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

9.2. Системы управления событиями информационной безопасности (SIEM): назначение, решаемые задачи и общая структура системы.

Ответ: См. Минзов А.С., Баронов О.Р., Минзов С.А., Осипов П.А.

Управление событиями информационной безопасности: Учебное пособие / Под редакцией профессора, д-ра техн. наук А.С. Минзова. — М. : ВНИИгеосистем, 2020. — 97 с. : ил.

9.3. Каналы утечки конфиденциальной акустической информации: классификации каналов, краткие характеристики и среда распространения информативного сигнала, технические средства обнаружения и защиты.

Ответ: См. Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное *пособие.* М.: Горячая линия-Телеком, 2005.

9.4. Побочные электромагнитные излучения и наводки (ПЭМИН): краткая характеристика канала утечки конфиденциальной информации, технические средства обнаружения и защиты.

Ответ: См. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. М.: Горячая линия-Телеком, 2014. Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное *пособие.* М.: Горячая линия-Телеком, 2005.

9.5. Организация инженерно-технической защиты территорий и помещений с использованием технических средств охраны.

Ответ: Невский А.Ю., Баронов О.Р. Технические средства охраны. М.: ВНИИгеосистем, 2015;

ГОСТ Р 53195.1-2008 Национальный стандарт Российской Федерации. Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения;

ГОСТ Р 53709-2009. Национальный стандарт Российской Федерации. Системы безопасности комплексные и интегрированные. Общие технические требования;

ГОСТ Р 51241-2008. Национальный стандарт Российской Федерации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний;

ГОСТ Р 51558-2008. Национальный стандарт Российской Федерации. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

Задание 10 (20 баллов)

10.1. Цель, задачи и общая характеристика мероприятий специального обследования защищаемого помещения.

Ответ: См. Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное *пособие.* М.: Горячая линия-Телеком, 2005.

10.2. Цель, задачи и общая характеристика мероприятий специальной проверки технического средства приема, обработки, хранения и передачи информации.

Ответ: См. Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное *пособие.* М.: Горячая линия-Телеком, 2005.

10.3. Какие цели и задачи решаются при разработке плана обработки рисков информационной безопасности и как они связаны с конечными целями организации и ограничениями? Методы и способы реализации этих задач.

Ответ: См. Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

10.4. Что является общим и в чем различаются между собой концепции защиты информации, изложенные в стандартах COBIT 5.0 и ГОСТ Р ИСО/МЭК 27001?

Ответ: См. Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил.

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

10.5. Определить перечень исходных данных при оценке актуальных угроз информационной безопасности как при проектировании систем и сетей, так и в ходе их эксплуатации. В какой логической последовательности проводится анализ и оценка угроз?

Ответ: См. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)