

Банк заданий по базовой части вступительного испытания в магистратуру

Задание 1 (5 баллов)

1.1. Понятие «угроза» безопасности информации. Классификация угроз безопасности информации. Что такое модель угроз безопасности информации?

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;

См. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021).

1.2. Понятие «уязвимости информации» в информационных системах. Классификация уязвимостей. Причины возникновения уязвимостей. Информационные источники данных об уязвимостях: назначение, базы уязвимостей, описание уязвимости

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

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

См. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова – Екатеринбург: Изд-во Урал.ун-та, 2019.— 204 с.

1.3. Понятие «риск информационной безопасности». Последовательности обработки рисков информационной безопасности.

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

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.

1.4. Понятие «критическая информационная инфраструктура». Требования к созданию систем безопасности значимых объектов КИИ РФ.

Ответ: См. Федеральный Закон № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации».

См. Приказом ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования».

1.5. Система менеджмента информационной безопасности (СМИБ): назначение, принцип процессного подхода управления.

Ответ: См. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Требования.

Задание 2 (5 баллов)

2.1. Понятие «коммерческая тайна». Основания и методика отнесения сведений к «коммерческой тайне». Требования к защите коммерческой тайны. Охрана конфиденциальности информации при осуществлении трудовых отношений в организации.

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. Права субъектов и обязанности операторов персональных данных.

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

См. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.3. Понятие «служебная тайна». Правовой режим служебной тайны. Порядок передачи служебной информации ограниченного распространения другим органам и организациям.

Ответ: См. Указ Президента РФ №188 от 06.03.1997;

См. 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);

См. Приказ Роскомнадзора от 27.07.2023 № 112 «Об упорядочении обращения со служебной информацией ограниченного распространения в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальных органах» (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения») (Зарегистрировано в Минюсте России 23.10.2023 № 75689).

2.4. Понятие «государственная тайна». Правовой режим «государственной тайны». Перечень сведений, отнесенных к государственной тайне.

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

См. Указа Президента РФ № 1203 1995 года «Об утверждении Перечня сведений, отнесенных к государственной тайне»;

См. Указ Президента РФ от 30 апреля 2008 г. № 654 «О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203».

2.5. КИИ РФ: сфера действия, цели и принципы защиты критической информационной инфраструктуры РФ. Требования по обеспечению безопасности значимых объектов КИИ РФ. Оценка значимости объекта КИИ. Порядок определения мер безопасности для защиты значимого объекта критической информационной инфраструктуры.

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

См. Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ».

Задание 3 (10 баллов)

3.1. Организация системы менеджмента информационной безопасности (СМИБ) на основе процессного подхода. Основное содержание процедур фаз: планирования, обеспечения и поддержки, функционирования, оценивания исполнения и улучшения?

Ответ: См. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Требования;

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.

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. На схеме (Рисунок 1) приведена последовательность деятельности по обработке рисков информационной безопасности. Поясните смысл каждого варианта обработки риска.

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

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.

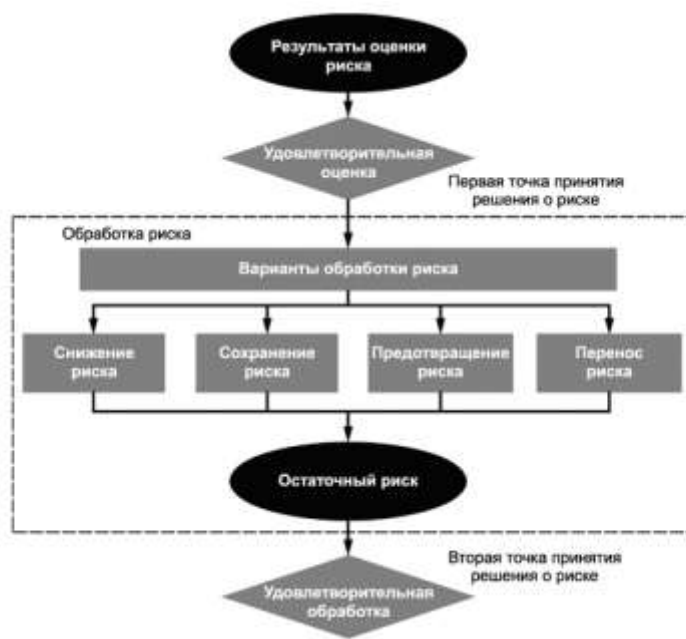


Рисунок 1 – Деятельность по обработке риска

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;

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.

3.5. Назначение, структура, силы и средства ГосСОПКА, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Ответ: См. «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

См. Документ утвержденный Президентом РФ 03.02.2012 №803 «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации»;

См. Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам».

Задание 4 (10 баллов)

4.1. Алгоритм симметричного блочного шифрования на основе сети Фейстеля. Понятие криптостойкость алгоритма. Последовательность и режимы алгоритмов симметричного блочного шифрования «Магма» и «Кузнечик».

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;

См. ГОСТ Р 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».

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;

См. 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;

См. 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;

См. 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;

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

Задание 5 (10 баллов)

5.1. На схеме (Рисунок 1) приведена схема последовательности менеджмента рисков информационной безопасности, взятая из ГОСТ Р ИСО/МЭК 27005-2010.



Рисунок.1 – Процесс менеджмента риска информационной безопасности

Поясните все этапы процесса менеджмента рисков информационной безопасности представленные на рисунке 1. Дайте письменный ответ, при каких условиях осуществляется перевод управления на блок «Установление контекста».

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

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.

5.2. Непрерывный мониторинг каких факторов должен быть обеспечен организацией в процессе менеджмента риска информационной безопасности (Рисунок 1). Поясните содержание мероприятий по руководству реализацией действия процесса менеджмента риска ИБ по постоянному мониторингу, анализу и улучшению?

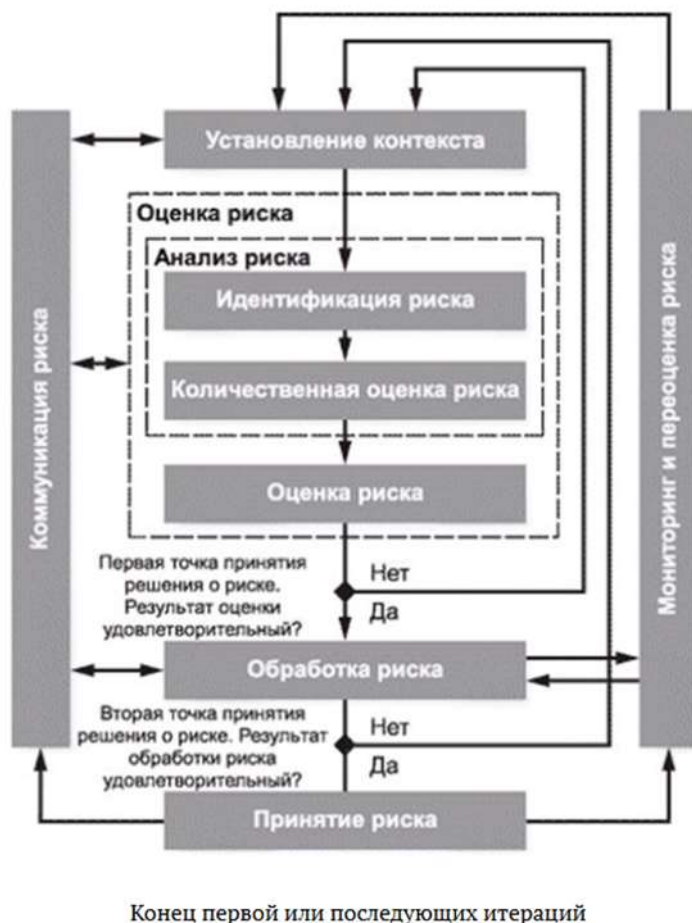


Рисунок.1 – Процесс менеджмента риска информационной безопасности

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

5.3. Высокоуровневая и детальная оценка риска информационной безопасности. Поясните порядок определения меры ценности активов и степени вероятности сценария инцидента на основе использования шкалы от 0 до 8.

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

5.4. В стандарте ГОСТ Р ИСО/МЭК 27002-2021 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 27002-2021. 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 разрабо-
танного 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.;

См. 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 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состав 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 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

6.3. Порядок организации деятельности по защите информации оператором (обладателем информации) в государственных информационных системах.

Ответ: См. Приказ от 11.04.2025 года № 117 Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений.

6.4. Кто организует защиту информации в государственных информационных системах и какие документы должны быть разработаны оператором (обладателем информации) и утверждены руководством для этого? Краткое содержание документов по организации защиты информации.

Ответ: См. Приказ от 11.04.2025 года № 117 Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений.

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 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Требования;

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

Задание 7 (5 баллов)

7.1. Назначение, характеристика функциональных возможностей программных и программно-аппаратных межсетевых экранов. Механизмы защиты информации. Отличия

средств традиционных решений от межсетевых экранов нового поколения (NGFW).

Ответ: См. Р.Р. Фаткиева. Основы построения защищенных компьютерных сетей. Межсетевое экранирование. СПбГЭТУ «ЛЭТИ», 2021. URL: <https://vec.etu.ru/moodle/pluginfile.php>.

См. URL: <https://www.kaspersky.ru/resource-center/definitions/firewall?ysclid=mkqp7qpxcu501259280>;

См. URL: <https://asher.ru/security/book/its/25?ysclid=mkqptol3cn318700379>;

См. URL: https://megavtogal.com/sovety/otlichie-ngfw-ot-obychnogo-mezhsetevogo-ekrana.php?utm_referrer=https%3A%2F%2Fya.ru%2F.

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

Ответ: См. URL: <https://www.infowatch.ru/>; <https://searchinform.ru/>.

7.3. Общая характеристика механизмов защиты информации, встроенных в современную отечественную операционную систему ASTRA LINUX: дискреционное и мандатное разграничение доступа; идентификация и аутентификация пользователей; контроль целостности, изоляция моделей; регистрация событий.

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;

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

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

См. 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;

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

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

См. 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 (15 баллов)

8.1. Порядок практического использования электронной подписи в соответствии с отечественным стандартом ГОСТ Р 34.10-2018. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

См. ГОСТ Р 34.10-2018. «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;

См. ГОСТ Р ИСО 19011 – 2021 года. Оценка соответствия. Руководящие указания по проведению аудита 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;

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

См. 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;

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

См. 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 ликвидации угроз безопасности.

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

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

См. ГОСТ Р 51558-2014. Национальный стандарт Российской Федерации. Средства и системы охраняемые телевизионные. Классификация. Общие технические требования. Методы испытаний.

Задание 9 (15 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 27002-2021. 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.

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

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

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

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

См. ГОСТ Р 51558-2014. 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.

См. 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 СОВИТ 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.

См. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

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.)