Филиал ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске
Направление подготовки 10.04.01 Информационная безопасность
Профиль направления «Безопасность автоматизированных систем»

Банк заданий по базовой части вступительного испытания в магистратуру

Задание 1 (5 баллов)

1.1. Понятие «угроза безопасности информации». Классификация угроз.

Ответ: Угроза (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (см. ГОСТ Р 50922-2006). Классификация угроз (см. ГОСТ Р ИСО/МЭК 27005-2012, Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК России, 2008 год).

1.2. Понятие уязвимости информации в информационных системах. Примеры уязвимостей.

Ответ: Уязвимость (информационной системы); *брешь*: Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

См. ГОСТ Р 50922-2006, ГОСТ Р ИСО/МЭК 27005-2012.

1.3. Понятие «риск информационной безопасности». Свойство риска.

Ответ: Риск информационной безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанести ущерб организации.

См. ГОСТ Р ИСО/МЭК 27005-2010. Дополнительно в ответ следует включить: В стандарте ГОСТ Р ИСО/МЭК реализован подход к созданию систем защиты информации основан на оценке показателей риска (R) информационной безопасности для каждой выявленной угрозы (T) по отношению к конкретному информационному активу (A) через имеющиеся уязвимости информационной системы (Y):

$$R = A \cap T \cap Y,$$

где $A \neq \varnothing$, $T \neq \varnothing$, $Y \neq \varnothing$;

$R = \varnothing$, *если* $(A = \varnothing) \cup (T = \varnothing) \cup (Y = \varnothing)$.

1.4. Основания и методика отнесения сведений к «коммерческой тайне».

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

1.5. Основания и методика отнесения сведений к «служебной информации ограниченного распространения».

Ответ: См. требования Указа Президента РФ № 188 1997 года «Об утверждении Перечня сведений конфиденциального характера»; 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).

Задание 2 (5 баллов)

2.1. Понятие «коммерческая тайна».

Ответ: Статья 3. Основные понятия, используемые в настоящем ФЗ "О коммерческой тайне".
1) Коммерческая тайна - режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
2) Информация, составляющая коммерческую тайну, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введён режим коммерческой тайны;
См. Федеральный Закон РФ №98-ФЗ 2004 года «О коммерческой тайне».

2.2. Понятие «персональные данные».

Ответ: персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
См. Федеральний Закон РФ №152-ФЗ 2006 года «О персональных данных».

2.3. Понятие «служебная тайна».

Ответ: Определение служебной тайны - перечень информации, считающейся конфиденциальной – т.е. непосредственно связанные с государственной, муниципальной или иной службой данные с ограниченным доступом.
К служебной информации с ограниченным доступом, в соответствии с законодательством РФ, относится любая информация, к которой доступ граждан ограничивается отдельными нормативными актами. При этом к таковым сведениям относятся не являющиеся секретными данные о деятельности организаций и служб, которые не могут быть разглашены по причине законодательного запрета на разглашение именно этих данных или тех, которые были получены в ходе осуществления профессиональной деятельности.
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. Правовой режим «государственной тайны».

Ответ: государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб Российской Федерации.
Государственную тайну составляют:

сведения в военной области (о проведении военных операций, стратегическому развертыванию ВС РФ, научно-исследовательских работ по созданию и модернизации образцов вооружения, о разработке ядерных боеприпасов, дислокации, наименованиях, организационной структуре войск);

сведения в области экономики (планы подготовки к возможным вооруженным действиям, об использовании инфраструктуры РФ в целях обеспечения обороноспособности государства, о силах и средствах гражданской обороны, об объемах государственного оборонного заказа, о достижениях науки и техники, имеющих важное оборонное или экономическое значение, о запасах платины, природных алмазов в Государственном фонде драгоценных металлов);

сведения в области внешней политики (о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести урон безопасности РФ, о финансовой политики в отношении иностранных государств);

сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму (о силах, средствах, источниках, планах и результатах такой деятельности, о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе, о системе президентской, правительственной, шифрованной связи, о защите Государственной границы).

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

2.5. Правовой режим «служебной информации ограниченного распространения».

Ответ: Правовой режим служебной тайны. Служебная тайна не может быть объектом гражданского оборота. Запрещение ее разглашать, как правило, основывается на законодательстве, регламентирующем отдельные виды деятельности, затрагивающей в т.ч. сферу частной жизни гражданина (см., например, ст. 33 Федерального закона от 27 ноября 1992 г. N 4015-1 «Об организации страхового дела в Российской Федерации», ст. 63 Федерального закона от 7 июля 2003 г. N 126-ФЗ «О связи» Российская газета. 2003. 10 июля.). Определенные категории работников, занимающихся такой деятельностью, обязаны сохранять в тайне сведения, к которым они имеют доступ в связи с выполняемой работой (банковские служащие, работники связи, налоговые инспекторы, страховые агенты, врачи и др.)»

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).

Задание 3 (10 баллов)

3.1. Причины возникновения угроз безопасности информации. Классификация угроз информационной безопасности ФСТЭК по инцидентам, объектам воздействия, способам (методам) реализации и источникам угроз

ГОСТ Р ИСО/МЭК 27005-2012, «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн» ФСТЭК России, Угрозы безопасности информации (см.http://fstec.ru)

3.2. Модель угроз (безопасности информации): Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

См. ГОСТ Р 50922-2006. Национальный стандарт РФ. Защита информации. Основные термины и определения; ГОСТ Р ИСО/МЭК 13335-1-2006; ГОСТ Р ИСО/МЭК 27005-2012; РС БР ИББС-2.2-2009; «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн» ФСТЭК России. Дополнительно при ответе на вопрос следует рассмотреть способ параметрического описание угроз. Основная цель моделирования угроз заключается в определении перечня и возможности реализации угроз информационным активам через различные уязвимости. В стандарте ГОСТ Р ИСО/МЭК 27005-2012 предусматривается последовательная разработка перечней угроз, уязвимостей и активов, и сценариев реализации угроз. Такой подход возможен только при условии независимости угроз, уязвимостей и активов. Однако это далеко не так и для умышленных угроз существует определенная статистическая связь между ценностью актива, уязвимостью и возможностью реализации угрозы, которая может быть выражена в виде следующих правил:

1. Чем выше ценность актива и больше его уязвимость, тем выше возможность угрозы.
2. Возможность реализации угрозы не может быть меньше максимального значения из значения ценности актива и его уязвимости.

Исходя из этих правил разрабатывается модель угроз и уязвимостей информационных активов, которая представляются в форме кортежа

{ nti, ti, nyi, yi, nai, ui },

где *nti* – угроза (наименование) или код; *ti* – возможность реализации угрозы по принятой шкале; *nai* – наименование актива (объекта) или его код, в отношении которого реализуется угроза; *nyi* – наименование уязвимости или её код; *yi* – уязвимость актива по этой угрозе, заданные по выбранной шкале; *ui* – оценка возможных результатов реализации угрозы.

Порядок реализации этой модели следующий:

- Проводится аудит уязвимостей информационных активов и осуществляется их классификация по их доступности.
- Определяются угрозы, которые могут быть реализованы через выявленные уязвимости по отношению к активам.
- Проводится классификация возможности реализации угроз по заданным шкалам и правилам.

Разработка модели угроз, уязвимостей и активов может проводиться путем экспертного опроса. Для проведения аудита используются информационные технологии (сканеры безопасности).

3.3. Причины возникновения уязвимости информации. Классификация и характеристика уязвимостей. Модель уязвимостей

Ответ: См. ГОСТ Р 56546-2015, ГОСТ Р ИСО/МЭК 27005-2012. Классификация уязвимостей информационных систем ***CVSS*** ФСТЭК (см.http://fstec.ru).

3.4. Система менеджмента информационной безопасности организации на основе цикла Деминга -Шухарта: цели управления, задачи, последовательность процессов и разрабатываемые документы управления.

Ответ: См. ГОСТ Р ИСО/МЭК 27001-2006.

3.5. Менеджмент рисков информационной безопасности.

Ответ: См. руководящие документы ГОСТ Р ИСО/МЭК 27005-2012. Дополнительно в ответе на этот вопрос необходимо привести следующую информацию.

В настоящее время не существует теоретических обоснований применения методик управления рисками информационной безопасности. Основная причина заключается в большой неопределенности исходных данных для оценки рисков информационной безопасности. Обычная статистика для угроз не может быть применена, так как повторные инциденты в сфере информационной безопасности не допустимы. По существу, мы имеем либо статистику одного инцидента, либо прогнозируем на основе угроз некоторые события информационной безопасности. Эти обстоятельства и является основной причиной отсутствия автоматизированных систем управления информационной безопасностью. Какие могут быть подходы к управлению рисками в этих условиях? Определимся сначала на целях и задачах управления рисками.

Можно выделить три группы возможных целей создания СМИБ по уровню возрастания сложности решаемых задач:

1. Провести высокоуровневую оценку рисков информационной безопасности и предложить адекватные рискам меры и средства управления и контроля системы менеджмента информационной безопасности (СМИБ). Такая оценка предполагает применение упрощенных методов управления рисками на основе комплексной модели угроз и применения ограниченных средств контроля и управления к агрегатам (группам) рисков.

2. Повысить эффективность СМИБ организации за счет обоснования адекватных рискам мер контроля и управления. Такая цель потребует применения эффективных стратегий управления и анализа рисков.

3. Повысить эффективность бизнеса за счёт совершенствования системы управления СМИБ и снижения ущерба от реализации возможных угроз информационной безопасности. Это наиболее полная группа задач по оценке рисков, которая потребует рассмотрение рисков с позиций всех возможных стратегий их управления, анализа, выявления агрегатов рисков и использования правил их обработки.

При моделировании рисков информационной безопасности возможно решение следующих двух групп задач:

a) Обоснование системы информационной безопасности на основе упорядочивании и классификации рисков по степени их опасности:

1. $R = \{r_i\}$, где $r_i \geq r_{i+1} \geq r_{i+2} \geq \ldots \geq r_1$.
2. $\forall r, (r_i \in R) \rightarrow (r_i \in K_1) \cup (r_i \in K_2) \cup (r_i \in K_3) \ldots$,
где K_1, K_2, K_3 – классы опасности риска.
3. $\forall r_i, (r_i \in R) \rightarrow (r_i \in v1) \cup (_i i \in v2) \cup (r_i \in v3) \cup (r_i \in v4)$,
где *v1, v2, v3, v4*– способы обработки рисков (снижение, сохранение, предотвращение или перенос риска).
4. Выделение агрегатов рисков (А), связанных между собой по параметрам *T, Y, A* и оценкам их мощности. Это позволяет применить меры контроля и управления к группе рисков.

$$A = < |T| : |Y| : |A| > .$$

b) Обоснование системы информационной безопасности на основе экономических оценок рисков.

5. Создание неизбыточных СМИБ:
$R = <T, Y, U>$ при условии, что $\forall$ *ri, (zi< ui)*.
6. Создание СМИБ в условиях ограничений на затраты:
$R = <T, Y, U>$ при условии, что $\forall ri, (zi < ui), (\Sigma zi < zo)$,
где *zo* – планируемые затраты на создание системы информационной безопасности.
7. Создание условно-оптимальных решений по информационной безопасности:

$R = <T, Y, U>$ при условии $\Sigma ui \rightarrow \max$
и ограничениях $(\Sigma zi < zo) \cap (zi < ui)$.

Следует отметить что в настоящее время стандарт ГОСТ Р ИСО/МЭК 27005 предусматривает решение только первых трех задач, хотя и не исключает решение и более сложных задач (5-7).

Решение осуществляется следующим образом. Выбираются произвольным образом метрики для оценки угроз, уязвимостей и ценности активов, которые задаются в виде числовой шкалы и определяют значение оцениваемого показателя. Например, угроза может быть “высокой”, “средней” и “незначительной”, что будет соответствовать числовым значениям “1”, “2” и “3”. Метрика риска (*M*) находится комбинацией числовых значений показателей *T, Y, A* обычно в форме их суммы. Подобные метрики не имеют физического смысла и позволяют находить решения только для первых трех задач по классификации рисков.

Определение приоритетов рисков осуществляется путем их ранжирования по величине, как правило по убыванию значений показателей. Отношения порядка для метрики *M* будет иметь следующий вид: $m1 > m2 > \ldots > mn$. Аналогичные отношения порядка будут и для других показателей.

Ранжирование рисков по этим параметрам позволяет выделить наиболее опасные из них с различных точек зрения и оценить их возможные последствия.

Выявление связей между отдельными рисками по активам, угрозам и уязвимостям позволяет создавать агрегаты рисков. Наиболее эффективными для обобщения и анализа могут быть следующие агрегаты рисков:

1. |***T***|:|***Y***|:|***A***| как |***M***|:|**1**|:|***M***|. Это отношение рассматривается как отношение «многие угрозы» к «одной уязвимости» и ко «многим активам». При этих условиях проектируется защитная мера для одной уязвимости, что исключает все угрозы относящиеся к этой уязвимости и множеству активов. Обычно в этом случае обработка риска предусматривает его снижение путем устранения уязвимости.
2. |***T***|:|***Y***|:|***A***| как |***M***|:|**1**|:|**1**| (отношение «много угроз» к «одной уязвимости» и «одному активу»). Вариант обработки риска аналогичен предыдущему.
3. |***T***|:|***Y***|:|***A***| как |**1**|:|**1**|:|***M***| (отношение «одна угроза» к «одной уязвимости» и «многим активам»). При этих условиях проектируется защитная мера для уязвимости или от предполагаемой угрозы. В этом случае обработка риска осуществляется либо снижением риска путем устранения уязвимости, либо его перенос.
4. |***T***|:|***Y***|:|***A***| как |**1**|:|***M***|:|***M***| (отношение «одна угроза» к «многим уязвимостям» и «многим активам»). Рациональные защитные меры принимаются в отношении угрозы.
5. |***T***|:|***Y***|:|***A***| как |**1**|:|***M***|:|**1**| (отношение «одна угроза» к «многим уязвимостям» и «одному активу»). Защитные меры принимаются в отношении угрозы, либо по отношению к активу (предотвращение риска, либо его перенос).
6. |***T***|:|***Y***|:|***A***| как |***M***|:|***M***|:|**1**| (отношение «много угроз» к «многим уязвимостям» и «одному активу»). Защитные меры принимаются обычно в отношении актива (предотвращение риска, либо его перенос).
7. |***T***|:|***Y***|:|***A***| как |**1**|:|**1**|:|**1**| (отношение «одна угроза» к «одной уязвимостям» и «одному активу»). Защитные меры принимаются по отношению к уязвимости, угрозе или активу. Конкретный вариант выбирается исходя из величины затрат на обработку риска.

Вторая группа задач относится к экономическим оценкам риска и позволяет решать задачи управления рисками на основе ограничений на затраты и поиск условно-оптимального решения при максимальном возможном предотвращенном ущербе при реализации рисков. При этом термин условно-оптимальное решение введен потому, что отдельные показатели риска имеют вероятностный характер. Поиск решений для 5 и 6 задач осуществляется путем выбора стратегий упорядочивания рисков по различным показателям рисков (2) и другим параметрам.

В последние годы интерес к совершенствованию методов управления рисками стал возрастать. Причины этого явления во многом связаны не только с недостатками информационных систем по управлению рисками, но и совершенствованием и распространением нормативных документов, в которых используются процессные подходы к созданию СМИБ на основе управления рисками информационной безопасности и значительным интересом к методам управления рисками на основе нечётких множеств.

Задание 4 (10 баллов)

4.1. Общая характеристика современных методов криптографического преобразования информации.

В ответе рассмотреть работу блочных симметричных алгоритмов на примере сети Фейстеля, принцип работы ассиметричных алгоритмов шифрования и расшифрования, достоинства и недостатки этих алгоритмов.

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. Характеристика технических каналов утечки информации.
Ответ: См. Хорев А.А. Техническая защита информации. Том 1. М.: Изд. НПЦ «Аналитика» 2008.

4.3. 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.

4.4. Характеристика механизмов защиты, основанных на разделении конфиденциальной информации на виды тайн.
Ответ: См. Федеральный Закон РФ №5485-1 1993 года «О государственной тайне»; Федеральный Закон РФ № 149-ФЗ 2006 года «Об информации, информационных технологиях и защите информации»; Федеральный Закон РФ №63-ФЗ 2011 года «Об электронной подписи»; Федеральный Закон РФ № 98-ФЗ 2004 года «О коммерческой тайне»; Федеральный Закон РФ № 152-ФЗ 2006 года «О персональных данных»; Указ Президента РФ № 1203 1995 года «Об утверждении Перечня сведений, отнесенных к государственной тайне». Указ Президента РФ № 188 1997 года «Об утверждении Перечня сведений конфиденциального характера».

4.5. Общая характеристика системы защиты информации, встроенной в системное программное обеспечение.
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 5 (20 баллов)

5.1. Способы и средства выявления технических каналов утечки информации.
Ответ: См. Невский А.Ю., Баронов О.Р. Технические средства охраны. М.: ВНИИгеосистем, 2015; Хорев А.А. Техническая защита информации. Том 1. М.: Изд. НПЦ «Аналитика» 2008; Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное *пособие.* М.: Горячая линия-Телеком, 2005; Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. М.: Горячая линия-Телеком, 2014.

5.2. Способы и средства защиты технических каналов утечки информации.
Ответ: См. Хорев А.А. Техническая защита информации. Том 1. М.: Изд. НПЦ «Аналитика» 2008; Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное *пособие.* М.: Горячая линия-Телеком, 2005; Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. М.: Горячая линия-Телеком, 2014.

5.3. Средства защиты информационных систем организаций от компьютерных вирусов. Классификация антивирусного программного обеспечения и современные технологии антивирусной защиты.
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.

5.4. Харектеристика программных и программно-аппаратных межсетевых экранов, основные отличия, примеры программной (программно-аппаратной) реализации, преимущества и недостатки.
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.

5.5. Характеристика технических средства ораны по обнаружению угроз: средств видеонаблюдения (CCTV) и контроля, охранно-пожарной сигнализации.
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.

Банк заданий по специальной части вступительного испытания в магистратуру

Задание 6 (5 баллов)

6.1. Порядок обеспечения безопасности персональных данных граждан РФ на основе требований федерального законодательства.
Ответ: См. Федеральный Закон РФ № 152-ФЗ 2006 года «О персональных данных»; «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн» ФСТЭК России; Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персоноальных данных при их обработке в информационных системах персональных данных».

6.2. Порядок установления в организации правового режима обращения со служебной информацией ограниченного распространения.
Ответ. См. Указ Президента РФ №188 от 06.03.1997.
6.3. Порядок установления правового режима коммерческой тайны в организации на основе требований федерального законодательства.
Ответ: См. Федеральный Закон РФ №98-ФЗ 2004 года «О коммерческой тайне».

6.4. Порядок установления правового режима государственной тайны в организации на основе требований федерального законодательства.
Ответ: См. Федеральный Закон РФ №5485-1 1993 года «О государственной тайне».

6.5. Порядок обращения с документами, содержащими служебную информацию ограниченного доступа.
Ответ. См. Указ Президента РФ №188 от 06.03.1997.

Задание 7 (5 баллов)

7.1. Понятие системы резервного копирования и требования, предъявляемые к ней. Основы политики 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 операционную систему.
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.

7.4. Характеристика процессов идентификации и аутентификации.
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».
Ответ: См. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

8.2. Последовательность и режимы алгоритма симметричного шифрования в соответствии с отечественным стандартом ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
Ответ: См. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

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. Платонов В.В. Программно-аппаратные средства защиты информации. Издательство: "Academia", 2014. 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. Практическое задание 1. Расчет, оценка степени защищенности конфиденциальной акустической информации на объекте информатизации от утечки информации по виброакустическому каналу и разработка предложений по обеспечению требуемого уроня её защищенности.

Руководством компании принято решение по оборудованию конференц-зала. Начальнику службы защиты информации предложено разработать рекомендации руководству компании по обеспечению защиты информации от утечки по виброакустическому каналу.

Постановка задачи:

Исходя из требований руководящих документов по оценке защищенности конфиденциальной информации от утечки по техническим каналам и результатов измерений звукоизоляции инженерных конструкций, разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Исходные данные и ограничения:

А) Ограничения:

- защита информации от утечки из защищаемого помещения по другим каналам не рассматривается;
- показатели звукоизоляции стены с окнами определяются показателями звукоизоляции окон;
- показатели звукоизоляции стены с дверью определяются показателями звукоизоляции двери;
- показатели звукоизоляции стены определяются показателями звукоизоляции стены;
- конференц-зал оборудован средствами звукоусиления.

Б) Исходные данные:

- защищаемое помещение расположено в правой угловой части здания и имеет три окна и две входные двери;
- правая боковая стена защищаемого помещения выходит в тупик, левая - смежная с кабинетом бухгалтерии;
- окна защищаемого помещения выходят на улицу, а двери – в общий коридор;
- площадь защищаемого помещения составляет 126 кв. метров;
- средние значения измерений, проведенные в контрольных точках с использованием генератора сигналов низкой частоты (при уровене тестового интегрированного акустического сигнала равен 85 дБ) и шумомера составляют:
- стена с входными дверями – 55 дБ;
- правая боковая стена – 66 дБ;
- левая боковая стена – 32 дБ;
- внешняя стена здания с окнами – 38 дБ.

Выполнить:
1. Оценить степень соответствия защищаемого помещения требованиям руководящих документов по оценке защищенности конфиденциальной информации от ее утечки по виброакустическому каналу.
2. Разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

9.2. Практическое задание 2. Расчет, оценка степени защищенности конфиденциальной акустической информации на объекте информатизации от утечки информации по виброакустическому каналу и разработка предложений по обеспечению требуемого уроня её защищенности.

Руководством компании принято решение по оборудованию переговорной комнаты. Начальнику службы защиты информации предложено разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Постановка задачи:

Исходя из требований руководящих документов по оценке защищенности конфиденциальной информации от утечки по техническим каналам и результатов измерений звукоизоляции инженерных конструкций, разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Исходные данные и ограничения:

А) Ограничения:

- защита информации от утечки из защищаемого помещения по другим каналам не рассматривается;
- показатели звукоизоляции стены с окнами определяются показателями звукоизоляции окон;
- показатели звукоизоляции стены с дверью определяются показателями звукоизоляции двери;
- показатели звукоизоляции стены определяются показателями звукоизоляции стены.

Б) Исходные данные:

- защищаемое помещение расположено в левой угловой части здания и имеет два окна и входную дверь;
- левая боковая стена защищаемого помещения выходит на улицу без транспорта, правая - смежная с кабинетом генерального директора;
- окна защищаемого помещения выходят на улицу с интенсивным движением транспорта, а дверь – в общий коридор;
- площадь защищаемого помещения составляет 31 кв. метр;
- средние значения измерений, проведенные в контрольных точках с использованием генератора сигналов низкой частоты (при уровене тестового интегрированного акустического сигнала равен 80 дБ) и шумомера составляют:
- стена с входной дверью – 48 дБ;
- правая боковая стена – 40 дБ;
- левая боковая стена – 24 дБ;
- внешняя стена здания с окнами – 42 дБ.

Выполнить:

1. Оценить степень соответствия защищаемого помещения требованиям руководящих документов по оценке защищенности конфиденциальной информации от ее утечки по виброакустическому каналу.
2. Разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

9.3. Практическое задание 3. Расчет, оценка степени защищенности конфиденциальной акустической информации на объекте информатизации от утечки информации по виброакустическому каналу и разработка предложений по обеспечению требуемого уроня её защищенности.

Руководством компании принято решение по оборудованию кабинета руководителя. Начальнику службы защиты информации предложено разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Постановка задачи:

Исходя из требований руководящих документов по оценке защищенности конфиденциальной информации от утечки по техническим каналам и результатов измерений звукоизоляции инженерных конструкций, разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Исходные данные и ограничения:

А) Ограничения:

- защита информации от утечки из защищаемого помещения по другим каналам не рассматривается;
- показатели звукоизоляции стены с окнами определяются показателями звукоизоляции окон;
- показатели звукоизоляции стены с дверью определяются показателями звукоизоляции двери;
- показатели звукоизоляции стены определяются показателями звукоизоляции стены.

Б) Исходные данные:

- защищаемое помещение имеет два окна и входную дверь;
- боковые стены защищаемого помещения смежны: справа с кабинетом генерального директора; слева с бухгалтерией;
- окна защищаемого помещения выходят во внутренний двор, а дверь – в общий коридор;
- площадь защищаемого помещения составляет 22 кв. метра;
- средние значения измерений, проведенные в контрольных точках с использованием генератора сигналов низкой частоты (при уровене тестового интегрированного акустического сигнала равен 75 дБ) и шумомера составляют:
- стена с входной дверью – 50 дБ;
- смежные боковые стены – 38 дБ;
- внешняя стена здания с окнами – 44 дБ.

Выполнить:

1. Оценить степень соответствия защищаемого помещения требованиям руководящих документов по оценке защищенности конфиденциальной информации от ее утечки по виброакустическому каналу.
2. Разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

9.4. Практическое задание 4. Расчет, оценка степени защищенности конфиденциальной акустической информации на объекте информатизации от утечки информации по виброакустическому каналу и разработка предложений по обеспечению требуемого уроня её защищенности.

Руководством компании принято решение по оборудованию защищаемого помещения. Начальнику службы защиты информации предложено разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Постановка задачи:

Исходя из требований руководящих документов по оценке защищенности конфиденциальной информации от утечки по техническим каналам и результатов измерений

звукоизоляции инженерных конструкций, разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Исходные данные и ограничения:

А) Ограничения:

- защита информации от утечки из защищаемого помещения по другим каналам не рассматривается;
- показатели звукоизоляции стены с окнами определяются показателями звукоизоляции окон;
- показатели звукоизоляции стены с дверью определяются показателями звукоизоляции двери;
- показатели звукоизоляции стены определяются показателями звукоизоляции стены.
- защищаемое помещение оборудовано средствами звукоусиления.

Б) Исходные данные:

- защищаемое помещение расположено в средней части здания и имеет три окна и одну входную дверь;
- правая боковая стена защищаемого помещения смежная с помещением кинопроекторной, левая - смежная с кабинетом бухгалтерии;
- окна защищаемого помещения выходят на улицу, а двери – в общий коридор;
- площадь защищаемого помещения составляет 126 кв. метров;
- средние значения измерений, проведенные в контрольных точках с использованием генератора сигналов низкой частоты (уровень интегрированного акустического сигнала равен 80 дБ) и шумомера составляют:
- стена с входной деревянной дверью – 59 дБ;
- правая боковая гипсокартонная стена – 56 дБ;
- левая боковая кирпичная стена – 32 дБ;
- внешняя кирпичная стена здания с окнами – 34 дБ;

Выполнить:

1. Оценить степень соответствия защищаемого помещения требованиям руководящих документов по оценке защищенности конфиденциальной информации от ее утечки по виброакустическому каналу.
2. Разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

9.5. Практическое задание 5. Расчет, оценка степени защищенности конфиденциальной акустической информации на объекте информатизации от утечки информации по виброакустическому каналу и разработка предложений по обеспечению требуемого уровня её защищенности

Руководством компании принято решение по оборудованию защищаемого помещения. Начальнику службы защиты информации предложено разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Постановка задачи:

Исходя из требований руководящих документов по оценке защищенности конфиденциальной информации от утечки по техническим каналам и результатов измерений звукоизоляции инженерных конструкций, разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Исходные данные и ограничения:

А) Ограничения:

- защита информации от утечки из защищаемого помещения по другим каналам не рассматривается;

- показатели звукоизоляции стены с окнами определяются показателями звукоизоляции окон;

- показатели звукоизоляции стены с дверью определяются показателями звукоизоляции двери;

- показатели звукоизоляции стены определяются показателями звукоизоляции стены.

Б) Исходные данные:

- защищаемое помещение расположено в левой угловой части здания и имеет два окна и входную дверь;

- левая боковая бетонная стена защищаемого помещения выходит на улицу, правая кирпичная стена - смежная с кабинетом генерального директора;

- окна защищаемого помещения выходят на улицу без транспорта, а дверь – в общий коридор;

- площадь защищаемого помещения составляет 31 кв. метр;

- средние значения измерений, проведенные в контрольных точках с использованием генератора сигналов низкой частоты (уровень интегрированного акустического сигнала равен 70 дБ) и шумомера составляют:

- кирпичная стена с входной дверью – 40 дБ;

- правая боковая кирпичная стена – 36 дБ;

- левая бетонная боковая стена – 26 дБ;

- внешняя кирпичная стена здания с окнами – 42 дБ;

Выполнить:

1. Оценить степень соответствия защищаемого помещения требованиям руководящих документов по оценке защищенности конфиденциальной информации от ее утечки по виброакустическому каналу.

2. Разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Материалы для решения задач

Требования к звукоизоляции ограждающих конструкций защищаемого помещения

Таблица 1

Акустическая защищенность помещения

Место возможного перехвата речевой конфиденциальной информации		Нормативное значение параметра акустической защищенности помещения, дБ	
		Помещения, не оборудованные системами звукоусиления	Помещения, оборудованные системами звукоусиления
Смежные помещения		46	60
Уличное пространство	Улица без транспорта	36	50
	Улица с транспортом	26	40

Таблица 2

Звукоизоляции различных конструкций окон

№ пп	Конструкция	Примечание	Значение (дБ) на частотах, Гц				
			250	500	1000	2000	4000
1	Одинарное остекление	3 мм	17	22	28	31	32
		4 мм	23	26	31	32	32
		6 мм	22	26	30	27	25
2	Двойное остекление с воздушным промежутком	57 мм (толщина 3 мм)	20	32	41	49	36
		90 мм (толщина 3 мм)	29	38	44	50	48
		170 мм (толщина 3 мм) с прокладками	33	36	38	38	38
		57 мм (толщина 4 мм)	31	38	46	49	35
		90 мм (толщина 4 мм)	33	41	47	48	36
		100 мм (толщина 4 мм) (с герметизацией)	35	39	47	46	52
		200 мм (толщина 4 мм) (с прокладками)	36	41	47	49	55
		300 мм (толщина 4 мм) (с прокладками)	39	43	47	51	55
3	Стеклопакет	Толщина 98 мм (с прокладками)	40	42	45	48	50

Таблица 3

Звукоизоляция ограждащих конструкций, дБ

Материал конструкции	Толщина, мм	Поверхностная плотность	Среднегеометрическая частота октавной полосы							
			63	125	250	500	1000	2000	4000	8000
Кирпичная кладка, штукатуренная с двух сторон	½ кирпича 1 кирпич 1,5 кирпича 2 кирпича 2,5 кирпича	220 420 620 820 1000	32 36 41 45 45	39 41 44 45 47	40 44 48 52 55	42 51 55 59 60	48 58 61 65 67	54 64 65 70 70	60 65 65 70 70	60 65 65 70 70

Железобетонны е плиты	40 50 100 160 200 300 400 800	100 125 250 400 500 750 1000 2000	- 28 34 - 40 44 45 47,5	32 34 40 43 42 44,5 47,5 55	36 35 40 47 44 50 55 61	35 35 44 51 51 58 61 67,5	38 41 50 60 59 65 67,5 70	47 48 55 63 65 69 70 70	53 55 60 - 65 69 70 70	- 55 60 - 65 69 70 70
Гипсобетонные плиты	95	135	-	32	37	37	42	48	53	-
Шлакоблоки, штукатуренные с двух сторон	220	360	-	42	42	48	54	60	63	-
Древесностружечная плита	20	12	23	26	26	26	26	26	26	33
Две железобетонные плиты на общем фундаменте	40-40-40	180	-	36	43	42	46	55	57	-
Две гипсобетонные плиты на общем основании	95-100-95	270	-	41	43	42	48	56	62	-

Таблица 4

Звукоизоляции дверей различных конструкций

№ п. п.	Конструкция	Примечание	Значение Q_f (дБ) для частоты f (Гц)				
			250	500	1000	2000	4000
1	Стандартное дверное полотно толщиной 40мм (обыкновенная дверь)	Без уплотняющих прокладок	14	16	22	22	20
2		С уплотняющими прокладками из пористой резины	25	25	26	26	23
3	Стандартное дверное полотно толщиной 40мм с обивкой дермантином по минеральному войлоку	Уплотняющий валик на дверной коробке	26	29	32	35	36
4	Глухая щитовая дверь толщиной 40мм,	Без уплотняющих прокладок	23	24	24	24	23

5	облицованная с двух сторон фанерой толщиной 4 мм	С уплотняющими прокладками	27	32	35	34	35
6	Щитовая дверь из древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой	Без уплотняющих прокладок	26	30	31	28	29
7		С уплотняющими прокладками	30	33	36	32	30
8	Дверное полотно толщиной 84 мм из двух наружных листов фанеры и одного асбоцементного листа по 6 мм каждый с двумя промежуточными слоями стекловолокна толщиной 16 и 50 мм	Два ряда прокладок из пористой резины	25	31	37	39	35
9	Двойная дверь предыдущей конструкции с тамбуром шириной 300 мм	Два ряда прокладок из пористой резины	29	36	46	49	42
10	Дверь звукоизолирующая облегченная	Прокладки из пористой резины	30	39	42	45	42
11	Двойная дверь звукоизолирующая облегченная с тамбуром шириной 200 мм	Прокладки из пористой резины	42	55	58	60	60
12	Дверь звукоизолирующая тяжелая двойная с тамбуром шириной 300 мм	Прокладки из пористой резины	46	60	65	65	65
13	Дверь звукоизолирующая тяжелая. Прокладки из пористой резины	Одинарная	36	45	51	50	49
14		Двойная с тамбуром шириной 300 мм	46	60	65	65	65
15		Двойная с облицованным тамбуром шириной 300 мм	58	65	70	70	70

Ответ: См. Пример решения практического задания

Руководством компании принято решение по оборудованию защищаемого помещения. Начальнику службы защиты информации предложено разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по акустическому каналу.

Постановка задачи:

Исходя из требований руководящих документов по оценке защищенности конфиденциальной информации от утечки по техническим каналам и результатов измерений звукоизоляции инженерных конструкций, разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Исходные данные и ограничения:

А) Ограничения:

- защита информации от утечки из защищаемого помещения по другим каналам не рассматривается;
- показатели звукоизоляции стены с окнами определяются показателями звукоизоляции окон; двери;

- показатели звукоизоляции стены с дверью определяются показателями звукоизоляции
- показатели звукоизоляции стены определяются показателями звукоизоляции стены.

Б) Исходные данные:

- защищаемое помещение расположено в левой угловой части здания и имеет два окна и входную дверь;
- левая боковая бетонная стена защищаемого помещения выходит на улицу с транспортом, правая кирпичная стена - смежная с кабинетом генерального директора;
- окна защищаемого помещения выходят на улицу без транспорта, а дверь – в общий коридор;
- площадь защищаемого помещения составляет 31 кв. метр;средние значения измерений, проведенные в контрольных точках с использованием генератора сигналов низкой частоты (уровень интегрированного акустического сигнала равен 70 дБ) и шумомера составляют:
- кирпичная стена с входной дверью – 31 дБ;
- правая боковая кирпичная стена – 38 дБ;
- левая бетонная боковая стена – 26 дБ;
- внешняя кирпичная стена здания с окнами – 36 дБ; Выполнить:

1. Оценить степень соответствия защищаемого помещения требованиям руководящих документов по оценке защищенности конфиденциальной информации от ее утечки по виброакустическому каналу.
2. Разработать рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу.

Решение

1. Внимательно ознакомиться с постановкой задачи и материалами для ее решения.
2. Определить величины звукоизоляции ограждающих конструкций, для чего из показателя уровня интегрированного акустического сигнала необходимо вычесть значение показателя уровня тестового сигнала, измеренного в соответствующих точках за ограждающими конструкциями:

70 – 31 = 39 (дБ) - величина звукоизоляции кирпичной стены с входной дверью; 70 – 38 = 32 (дБ) - величина звукоизоляции правой боковой кирпичной стены; 70 – 26 = 44 (дБ) - величина звукоизоляции левой бетонной боковой стены;
70 – 36 = 34 (дБ) - величина звукоизоляции внешней кирпичной стены здания с окнами.

3. Определить соответствие величины звукоизоляции каждой ограждающей конструкции относительно показателей требований по акустической защищенности представленных в таблице 1 материалов для решения задачи. Для этого необходимо из виличин звукомзоляции каждой ограждающей конструкции вычесть соответствующее значение требования из таблицы 1 материалов для решения задачи с учетом условий смежного помещения, улицы с транспортом и без транспорта, а также размещения в защищаемом помещении средств звукоусиления:

39 – 46 = - 5 (дБ), где 46 дБ – показатель величины звукоизоляции соответствующий

требованию – смежное помещение и без средств звукоусиления;

32 – 46 = - 14 (дБ), где 46 дБ – показатель величины звукоизоляции соответствующий требованию – смежное помещение и без средств звукоусиления;

44 – 26 = 18 (дБ), где 26 дБ – показатель величины звукоизоляции соответствующий требованию – улица с транспортом и без средств звукоусиления;

34 – 36 = -2 (дБ), где 36 дБ – показатель величины звукоизоляции соответствующий требованию – улица без транспорта и без средств звукоусиления.

4. Оценить степень соответствия ограждающих конструкций защищаемого помещения требованиям руководящих документов по оценке защищенности конфиденциальной информации от ее утечки по виброакустическому каналу:

- кирпичная стена с входной дверью – необходимо увеличить звукоизоляцию двери на 5
- правая боковая кирпичная стена – необходимо увеличить звукоизоляцию правойбоковой кирпичной стены на 14 дБ; левая бетонная боковая стена – нет необходимости увеличивать звукоизоляцию стены, т.к. она соответствует требуемой звукоизоляции;
- внешняя кирпичная стена здания с окнами – необходимо увеличить звукоизоляцию окон на 2 дБ.

5. Рекомендации руководству компании по оборудованию защищаемого помещения для обеспечения защиты информации от утечки по виброакустическому каналу разрабатываются в виде предложений по усилению защитных свойств ограждающих конструкции за счет замены или установки дополнительных окон и дверей, а также «плиты на относе» для ограждающих конструкций без окон и дверей с использованием показателей звукоизоляции из таблиц 2,3 и 4 в материалах для решения задачи. Выбор средств защиты выполняется относительно выбора минимального значения, которое обеспечит требуемый уровень виброакустической защищенности по величине звукоизоляции ограждающей конструкции.

Предлагается увеличить звукоизоляцию:

- входной двери на 5 дБ за счет установки второй дополнительной двери - стандартное дверное полотно толщиной 40мм (обыкновенная дверь), без уплотняющих прокладок, которая увеличит звукоизоляцию на 14 дБ или заменить дверь звукоизолирующей тяжелой двойной двкрью с тамбуром шириной 300 мм с прокладками из пористой резины, которая позволит обеспечить требуемую звукоизоляцию ограждающей конструкции в 46 дБ.

- правой боковой кирпичной стены на 14 дБ за счет установки конструкции типа «плита на относе» выполненной из материала древесностружечная плита, применение которой позволит увеличить величину звукоизоляции ограждающей конструкции на 23 дБ;
- окон на внешней кирпичной стене здания на 2 дБ за счет их замены окнами с конструкцией типа двойное остекление с воздушным промежутком 200 мм (толщина стекла 4 мм) (с прокладками), что позволит обеспечит звукоизоляцию внешней кирпичной стены с окнами в требуемые 36 дБ.

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. Цель, задачи и общая характеристика мероприятий специальных исследований по оценке защищенности технических каналов утечки конфиденциальной информации. Ответ: См. Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное *пособие.* М.: Горячая линия-Телеком, 2005.

10.4. Цель, задачи и общая характеристика мероприятий по применению средств пассивной защиты технических каналов утечки информации.

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

10.5 Цель, задачи и общая характеристика мероприятий по применению средств активной защиты технических каналов утечки информации.

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