ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ

РЕКОМЕНДАЦИИ ПО РАЗМЕЩЕНИЮ ЦЕНТРАЛИЗОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЩЕГОРОДСКОМ ЦЕНТРЕ ОБРАБОТКИ ДАННЫХ.

ОБЩИЕ ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦЕНТРАЛИЗОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Москва, 2012

СОДЕРЖАНИЕ

1. Область применения

1.1. Данные рекомендации и требования распространяются на централизованные информационные системы и виртуализированную среду общегородского центра (центров) обработки данных, предназначенную для размещения серверных компонентов централизованных информационных систем.

1.2. Документ устанавливает общие положения по обеспечению информационной безопасности централизованных информационных систем и виртуализированной среды.

1.3. Документ рекомендован для применения путем включения ссылок на него и (или) прямого использования установленных в нем положений во внутренних нормативных документах государственных организаций и ведомств г. Москвы.

2. Нормативные ссылки

2.1. В настоящем документе использованы следующие нормативные ссылки:

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
3. «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено Государственной технической комиссии при Президенте Российской Федерации 25.11.1994;
4. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения»;
5. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 4.06.1999 №114 «Руководящий документ. Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»;
6. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
7. ГОСТ Р 51624-2000 «Автоматизированные системы в защищенном исполнении»;
8. ГОСТ 34.003 – 90 «Автоматизированные системы. Термины и определения».
9. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)», утверждено Приказом ФСБ России №66 от 9.02.2005 г.
10. «Типовые требования по организации и обеспечению функционирования

шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены руководством 8 центра ФСБ России 21 февраля 2008 года № 149/6/6-622.

11. «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утверждена Приказом ФАПСИ от 13 июня 2001 года N 152
12. Приказ Федеральной службы по техническому и экспортному контролю от 05.02.2010 №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»
13. Приказ Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 №282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»
14. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 25.07.1997 «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации»
15. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»
16. «Требования к системам обнаружения вторжений», утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638

3. Термины и определения

Back-end сервер – специально выделенный сервер системы, предназначенный для обработки и хранения информации и не имеющий непосредственного взаимодействия с рабочими местами пользователей системы.

Front-end сервер – специально выделенный сервер системы, обеспечивающий непосредственный интерфейс взаимодействия с рабочими местами пользователей или иными информационными системами и предназначенный для обработки запросов пользователей на получение информации и передачи им результатов запроса от Back-end сервера.

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [8].

Авторизация - предоставление прав доступа.

Аттестация информационной системы - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что информационная система соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России) [3].

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности) [4].

Виртуализированная среда – технологическая информационная система, созданная с использованием программных средств виртуализации и обеспечивающая размещение и функционирование других информационных систем.

Доступность информации – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [4].

Информационная безопасность - состояние защищенности информации и информационных систем, в условиях угроз, связанных с информационной сферой.

Информационная система персональных данных - совокупность, содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [2].

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения [7].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [1].

Мониторинг - постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации [6].

Недекларированные возможности - функциональные возможности ПО (ТС), не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение характеристик безопасности защищаемой информации [5].

Недоверенный сетевой узел – любой узел, находящийся за пределами контролируемой зоны защищаемого объекта и который не может контролироваться и управляться организацией.

Несанкционированный доступ (несанкционированные действия) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами [4].

Общегородской центр обработки данных - центр обработки данных города Москвы, предназначенный для размещения централизованных информационных систем.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных [1].

Регистрация - фиксация данных о совершенных действиях (событиях).

Роль - заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

Сетевая атака – сетевые пакеты, содержащие программный код, который, используя возможности предоставляемые ошибкой, отказом или уязвимостью, ведёт к повышению привилегий, несанкционированному доступу к данным или нарушению функционирования сетевого узла.

Сервер виртуализации – сервер с установленной специализированной операционной системой (гипервизором), предназначенной для запуска и управления виртуальными машинами.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения) [4].

Централизованная информационная система - информационная система, для которой возможна консолидация всех вычислительных ресурсов и обеспечение для всех пользователей системы единой точки доступа к информации.

Цифровой сертификат - выпущенный удостоверяющим центром электронный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов.

Характеристика безопасности информации – одно или несколько свойств информации, требующих обеспечения информационной безопасности – конфиденциальность, целостность, доступность, неотказуемость, достоверность, аутентичность и другие.

4. Обозначения и сокращения

DDoS	Distributed Denial of Service - распределённая атака типа «отказ в обслуживании»
IDS	Intrusion Detection System - система обнаружения вторжений
vLAN	Virtual Local Area Network — виртуальная локальная компьютерная сеть
VM	Виртуальная машина
VPN	«Virtual Private Network» - виртуальная частная сеть
АПМДЗ	Аппаратный модуль доверенной загрузки (электронный замок)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ДМЗ	Демилитаризованная зона
ИС	Информационная система
МЭ	Межсетевой экран
НДВ	Недокументированные возможности
НСД	Несанкционированный доступ
ОС	Операционная система
ОЦОД	Общегородской центр обработки данных
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
СХД	Система хранения данных
ТС	Техническое средство
ЦИС	Централизованная информационная система

5. Определение и классификация ЦИС

5.1. Отнесение информационных систем к централизованным информационным системам

5.1.1. Централизованной информационной системой (ЦИС) является информационная система, для которой возможна консолидация всех вычислительных ресурсов и обеспечение для всех пользователей системы единой точки доступа к информации (ресурсам системы).

5.1.2. Информационная система относится к централизованной, если все критерии, указанные в таблице 5.1 имеют значения, соответствующие ЦИС.

Табл.5.1 Критерии отнесения информационной системы к централизованной

	Критерий	Значение критерия, соответствующего ЦИС
1	Число взаимодействующих с ИС субъектов или объектов	Число пользователей ≥10 или число взаимодействующих с данной системой других ИС ≥3
2	Архитектура системы	Клиент-серверная ИС, в которой компоненты распределены по нескольким компьютерам с выделением отдельных клиентских мест и функциональных серверов
3	Режим обработки информации	Режим тонкого клиента, при котором вся вычислительная обработка информации выполняется на серверных компонентах системы, клиентское ПО обеспечивает только пользовательский интерфейс (выполняет отображение результатов обработки и передачу команд пользователя)
4	Технология доступа пользователей к информации	Единый доступ, при котором все группы пользователей (за исключением администраторов системы) используют единый механизм (способ) доступа и имеют единственную точку подключения (компонент системы, который обеспечивает доступ пользователей к функциям и информации)

5.2. Условия переноса ЦИС в ОЦОД

5.2.1. Условия возможности переноса ЦИС в виртуализированную среду ОЦОД указанны в таблице 5.2.

Табл.5.2 Условия для переноса ЦИС в ОЦОД

	Критерий	Значение критерия
	Основные	
1	Вид, обрабатываемой информации	Сведения, не составляющие государственную тайну
2	Объем трафика информационного взаимодействия[1]	Средний объем трафика составляет менее 40% пропускной способности внешнего канала связи

[1] Информационное взаимодействие между клиентами и серверными компонентами системы, а также между серверными компонентами системы и иными информационными системами, размещенными вне среды ОЦОД

		ОЦОД
3	Технология (способы) обработки информации	Ввод / вывод информации на стороне клиента без использования устройств, требующих непосредственного подключения к серверному оборудованию.
	Дополнительные	
4	Распределенность ЦИС	ЦИС, компоненты которой размещаются на множестве удаленных друг от друга объектов
5	Взаимодействие с удаленными информационными системами	ЦИС взаимодействует более чем с одной информационной системой, размещенной на удаленных объектах
6	Критичность ЦИС к отказам	Нарушение функционирования ЦИС вследствие сбоя работы технических средств, отключения электроэнергии, нарушения климатических условий и т.п. может привести к значительным негативным последствиям
7	Срок окончания эксплуатации	Система выводится из эксплуатации не раньше чем через 1 год

5.2.2. Решение о переносе ЦИС в ОЦОД может быть принято при ее соответствии всем основным критериям и хотя бы одному из дополнительных.

5.3. Классификация ЦИС

5.3.1. Классификация ЦИС проводится в целях группирования их по схожим требованиям обеспечения безопасности и размещения в соответствующей зоне безопасности виртуализированной среды ОЦОД.

5.3.2. Классификация ЦИС проводится на основании характера обрабатываемых данных, критичности системы и используемой технологии информационного взаимодействия с пользователями системы.

5.3.3. По характеру обрабатываемых данных ЦИС подразделяются на группы:

1. Группа «Специальные ЦИС» - ЦИС, которые относятся к системам персональных данных, классифицированных по классу К1;
2. Группа «Обычные» - ЦИС, которые относятся к системам персональных данных, классифицированных по классу К2, К3 и К4 (обрабатывающие обезличенные персональные данные, но не являющиеся общедоступными), а также ЦИС, обрабатывающие иные сведения, ограниченного доступа (за исключением сведений, составляющих государственную тайну);
3. Группа «Общедоступные» - ЦИС, обрабатывающие только общедоступные данные.

5.3.4. По степени воздействия нарушения функционирования ЦИС на деятельность ведомств и организаций Правительства Москвы подразделяются на группы:

1. Группа «Критичные» - ЦИС, для которых нарушение характеристик безопасности обрабатываемой информации может вызвать значительные негативные последствия[2];
2. Группа «Не критичные» - ЦИС, для которых нарушение характеристик безопасности обрабатываемой информации может вызвать незначительные негативные последствия.

Для оценки степени негативных последствий рекомендуется использовать методики, определенные в ГОСТ 13335-3: 2007 (раздел 9.3.3 и Приложение В) и ГОСТ 13569: 2007 (Приложение С).

5.3.5. По реализованной структуре ЦИС подразделяются на группы:

1. Группа «Системы с front-end серверами» - ЦИС, в структуре которых выделяются front-end серверы для взаимодействия с пользователями и back-end серверы для обработки информации;
2. Группа «Системы без front-end серверов» - ЦИС, структура которых не имеет разделения на front-end серверы и back-end серверы[3].

5.3.6. На основании отнесения ЦИС к различным группам определяется ее категория в соответствии с таблицей 5.3

Табл.5.3 Система классификации ЦИС

Группы ЦИС	Критичная	Не критичная		
		Специальная	Обычная	Обще-доступная
Системы без front-end серверов	**ЦИС 1**	**ЦИС 1**	**ЦИС 2**	**ЦИС 3**
Системы с front-end серверами	**ЦИС 1F**	**ЦИС 1F**	**ЦИС 2F**	

6. Организация виртуализированной среды ОЦОД

6.1. Зоны безопасности

6.1.1. В структуре виртуализированной среды ОЦОД организуются следующие зоны безопасности:

1. Зона «1» - предназначена для размещения ЦИС категорий 1 и 1F (back-end серверов);
2. Зона «2» - предназначена для размещения ЦИС категорий 2 и 2F (back-end серверов);

[2] Экспертная оценка уровня негативных последствия выполняется ведомством – оператором ЦИС самостоятельно.
[3] Отсутствие в структуре ЦИС front-end сервера не исключает доступ к системе пользователей из внешних сетей.

3. Зона «3 (Частная ДМЗ)» - предназначена для размещения front-end серверов ЦИС категорий 1F, 2F;
4. Зона «4 (Общая ДМЗ)» - предназначена для размещения ЦИС категории 3.

6.1.2. Для каждой зоны безопасности в структуре виртуализированной среды выделяются свои сервера виртуализации, свое адресное пространство и раздел на СХД, предназначенный для хранения файлов виртуальных машин (VM).

6.1.3. Сервера виртуализации каждой зоны безопасности должны размещаться в отдельных серверных стойках.

6.1.4. Изоляция зон безопасности между собой может обеспечиваться следующими методами:

- использования в общей среде механизмов разграничения доступа ПО виртуализации и/или средств защиты информации от несанкционированного доступа, предназначенных для использования в виртуальной среде;
- использование отдельной среды виртуализации для каждой зоны безопасности.

6.1.5. Для каждой ЦИС категорий 1 и 1F, размещаемых в зоне безопасности «1» ОЦОД, должны выделяться отдельные сервера виртуализации для монопольного использования ресурсов данных серверов виртуальными машинами, на которых разворачиваются компоненты данной ЦИС. Для зоны безопасности «1» не допускается запускать на одном сервере виртуализации виртуальные машины, принадлежащие различным ЦИС.

6.2. Администрирование безопасности виртуализированной среды

6.2.1. Для администрирования безопасности виртуализированной среды должна быть выделена и документально определена роль администратор безопасности виртуализированной среды.

6.2.2. В состав роли «Администратор безопасности виртуализированной среды» должны включаться полномочия:

- управление средствами защиты информации виртуализированной среды;
- контроль структуры виртуализированной среды и политик безопасности, включая правила разграничения доступа к элементам виртуализированной среды и предоставления необходимых полномочий системным администраторам виртуализированной среды;
- аудит событий безопасности в виртуализированной среде.

6.2.3. В отношении администратора безопасности виртуализированной среды в трудовом договоре должна устанавливаться персональная ответственность за выполнение своих обязанностей, определяемых должностной инструкцией.

6.2.4. В организации, обеспечивающей управление виртуализированной средой, должны быть документально определены процедуры приема на работу лиц, назначаемых на роли администраторов, включающие:

- проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;
- проверку в части профессиональных навыков и оценку профессиональной пригодности.

6.2.5. Все администраторы должны давать письменное обязательство о соблюдении конфиденциальности.

6.2.6. Предоставлять полномочия по администрированию виртуализированной среды администраторам ЦИС не допускается.

7. Требования по обеспечению безопасности

7.1. Персонал безопасности

7.1.1. Для администрирования безопасности ЦИС рекомендуется выделять и документально оформлять роль администратор безопасности ЦИС.

7.1.2. В целях обеспечения доверия администратору безопасности ЦИС в организации – оператора ЦИС рекомендуется проводить следующие процедуры в отношении данного лица:

- проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;
- проверку в части профессиональных навыков и оценку профессиональной пригодности;
- получение письменного обязательства о соблюдении конфиденциальности.

7.2. Физическая безопасность

7.2.1. Размещение всех технических средств виртуализированной среды (серверное оборудование, системы хранения данных, СЗИ, устройства и средства коммутации, устройства резервного копирования и носители резервных копий) должно производиться внутри отдельных серверных стоек (шкафов).

7.2.2. Размещение в стойках с оборудованием виртуализированной среды оборудования, не имеющего отношения к виртуализированной среде ОЦОД не допускается.

7.2.3. Серверные стойки (шкафы) должны оборудоваться запирающими устройствами и опечатываться методами, гарантирующими невозможность вскрытия стойки без нарушения целостности печати.

7.2.4. Коммуникации между стойками (шкафами) должны выполняться отдельным оптическим кабелем, прокладываемым в пределах серверных помещений, в которых расположены стойки. Расшивка кабеля должна проводиться на патч - панелях, размещенных внутри стоек.

7.2.5. Серверные помещения ОЦОД, в которых размещаются стойки (шкафы) с оборудованием виртуализированной среды, должны оборудоваться средствами видеонаблюдения, обеспечивающими возможность проведения визуального

контроля доступа персонала к каждой из стоек. Архивные записи системы видеонаблюдения должны быть доступны для просмотра за период не менее чем 30 дней.

7.2.6. Рабочие места, предназначенные для администрирования виртуализированной среды и размещаемые в помещениях ОЦОД, должны быть выделенными и предназначены только для администраторов виртуализированной среды. Системные блоки рабочих мест администраторов должны опечатываться методами, гарантирующими невозможность вскрытия блока без нарушения целостности печати.

7.2.7. Серверное оборудование ЦИС, не перемещаемых в ОЦОД, должно размещаться в зонах, обеспечивающих невозможность непосредственного доступа к оборудованию посторонних лиц.

7.2.8. В ОЦОД, а также на других объектах размещения серверных компонентов ЦИС должны быть реализованы и поддерживаться организационно – режимные меры, обеспечивающие возможность пребывания и/или непосредственного доступа к техническим средствам только уполномоченных лиц или в сопровождении уполномоченных лиц.

7.2.9. Рекомендуется включать во внутренние инструкции ведомств (учреждений), регламентирующих работу пользователей и администраторов ЦИС, положения запрещающие несанкционированное изменение конфигурации аппаратных средств АРМ.

7.3. Безопасность межсетевого взаимодействия

7.3.1. Во внутренней сети виртуализированной среды должны выделяться изолированные сегменты, предназначенные для размещения различных компонентов:

- сегменты виртуальных машин, относящиеся к различным зонам безопасности ОЦОД;
- сегмент серверов виртуализации и серверов управления виртуальной средой;
- сегмент управления СЗИ;
- сегмент сети хранения данных.

7.3.2. Виртуальные машины (VM), принадлежащие одной ЦИС, необходимо размещать в отдельном vLAN сетевого сегмента, предназначенного для размещения VM.

7.3.3. Рабочие станции пользователей ЦИС, размещенные во внутренних локальных сетях ведомств (учреждений), а также серверные компоненты ЦИС не перемещаемых в ОЦОД, рекомендуется выделять в отдельные сетевые сегменты с использованием технологии vLAN и маршрутизацией в них трафика обмена между АРМ пользователей и серверными компонентами ЦИС.

7.3.4. Коммуникационное оборудование виртуализированной среды и внутренних локальных сетей ведомств (учреждений) – операторов ЦИС должно использовать последние версии системного ПО и обновления безопасности. Оборудование

должно быть корректно настроено для предотвращения получения несанкционированного доступа к трафику, циркулирующему в vLAN.

7.3.5. Весь входящий и исходящий трафик между сетевыми сегментами виртуализированной среды и между всеми vLAN ЦИС должен контролироваться при помощи межсетевых экранов, а также трафик внутри защищенных VPN соединений удаленного доступа к ресурсам ЦИС. Доступ в сегменты серверов виртуализации и серверов управления виртуальной средой, управления СЗИ должен быть разрешен только со стороны рабочих мест администраторов виртуализированной среды.

7.3.6. Серверные компоненты ЦИС, не перемещаемых в ОЦОД, и имеющие подключения к локальной сети ведомства – оператора ЦИС или подключения к сетям общего пользования должны защищаться с использованием межсетевых экранов, контролирующих весь входящий и исходящий трафик серверов ЦИС.

7.3.7. Межсетевые экраны должны обеспечивать прохождение только необходимого для нормального функционирования ЦИС трафика. Весь явно не разрешенный администраторами трафик блокируется.

7.3.8. Фильтрация трафика на межсетевом экране должна проводиться:

- на сетевом уровне для каждого сетевого пакета независимо, на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов;
- на транспортном уровне с учетом транспортных адресов отправителя и получателя (портов);
- на прикладном уровне запросов с учетом используемых протоколов.

7.3.9. Должна проводиться фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.

7.3.10. На всех интерфейсах межсетевого экрана должна проводиться проверка сетевых пакетов с учетом входного и выходного сетевых интерфейсов как средство контроля подлинности сетевых адресов (правила антиспуфинга).

7.3.11. Весь входящий во внутреннюю сеть виртуализированной среды ОЦОД или серверный сегмент ЦИС внутренней локальной сети ведомств (учреждений) – операторов ЦИС трафик, поступающий от недоверенных сетевых узлов (удаленные АРМ пользователей, сеть Интернет, информационные системы, размещенные вне виртуализированной среды), должен дополнительно контролироваться при помощи средств обнаружения / предотвращения вторжений (IDS/IPS).

7.3.12. Контроль трафика на предмет наличия в нем программного кода, реализующего сетевую атаку, должен проводиться в отношении протоколов сетевого, транспортного и прикладного уровней.

7.3.13. Детектирование сетевых атак должно проводиться методами сигнатурного анализа, выявления аномалий, с использованием поведенческих сигнатур.

7.3.14. Для защиты web приложений ЦИС, размещаемых в ОЦОД, от атак отказа в обслуживании (DDoS атак) в составе ОЦОД должны применяться специализированные средства защиты.

7.3.15. На серверных компонентах ЦИС и серверах виртуализации должна разрешаться работа только тех сетевых служб и сервисов, которые необходимы для нормального функционирования систем.

7.4. Защита данных и управление доступом

7.4.1. Все СЗИ, применяемые для защиты ЦИС, должны использовать встроенные механизмы защиты от НСД. Доступ к функциям управления СЗИ должен предоставляться только после прохождения администратором (пользователем) процедуры аутентификации.

7.4.2. Перед началом использования СЗИ все установленные по умолчанию пароли доступа должны быть изменены.

7.4.3. В составе виртуализированной среды, так же как и в ЦИС должны применяться встроенные защитные меры, при наличии сертификации системного или прикладного ПО, реализующие механизмы управления доступом, а в случае их отсутствия, сертифицированные средства защиты информации от НСД.

7.4.4. Работа всех администраторов виртуализированной среды и администраторов ЦИС должна осуществляться под уникальными учетными записями.

7.4.5. Доступ к функциям управления и объектам виртуализированной среды, а также самих ЦИС должен предоставляться только после прохождения процедуры идентификации и аутентификации.

7.4.6. Аутентификация должна проводиться, по меньшей мере, одним из следующих методов:

- использование пароля (парольной фразы);
- двух факторная аутентификация.

7.4.7. При использовании паролей, они должны отвечать следующим минимальным требованиям:

- длина пароля должна составлять не менее 8 символов;
- пароль должен состоять, по крайне мере, из цифровых и буквенных символов;
- срок действия пароля не должен превышать 90 дней.

7.4.8. Необходимо настраивать блокировку учетных записей пользователей при нескольких неудачных попытках регистрации в течение установленного периода времени. Допускается не использовать блокировку учетных записей при использовании механизмов регистрации и выявления инцидентов, связанных с атаками типа «подбор пароля».

7.4.9. Первоначальный доступ в операционную систему VM предоставляется администратору ЦИС администратором виртуализированной среды.

Администратор ЦИС должен изменить пароли доступа в ОС после первичной авторизации.

7.4.10. При увольнении или изменении должностных обязанностей сотрудников, выполняющих функции одного из администраторов виртуализированной среды или ЦИС, необходимо выполнить процедуры соответствующего пересмотра прав доступа и смены паролей.

7.4.11. Предоставление доступа пользователей ЦИС к информации, предоставляемой данной ЦИС, обеспечивается администратором ЦИС и осуществляется в соответствии с внутренней регламентирующей документацией ведомства (учреждения).

7.4.12. Для защиты от НСД компонентов виртуализированной среды должны использоваться следующие механизмы и мероприятия:

- ограничение возможности использования системных устройств сервера виртуализации виртуальными машинами;
- ограничение на использование системных ресурсов серверов виртуализации и систем хранения данных со стороны виртуальных машин только необходимыми максимальными значениями;
- контроль и обеспечение запуска виртуальных машин ЦИС на серверах виртуализации, размещаемых в той зоне безопасности, которая отвечает соответствующей категории ЦИС;
- выделение для нескольких ЦИС, требующих для своей работы общего файлового ресурса, отдельного раздела на системе хранения данных, не содержащего файлов самих виртуальных машин ЦИС;
- обеспечение контроля целостности файлов конфигурации ПО виртуализации и файлов виртуальных машин.

7.4.13. Следует проводить настройку блокировки сеанса доступа к операционной системе на всех рабочих станциях пользователей и администраторов ЦИС, а также и администраторов виртуализированной среды при бездействии пользователя в течение определенного периода времени. Рекомендуемыми значениями блокировки являются следующие значения периода бездействия:

- пользователь – 5 минут;
- администратор – 3 минуты.

7.4.14. Носители информации (в составе ТС или съемные), предназначенные для утилизации или передаваемые на ремонт в сторонние организации в обязательном порядке должны проходить процедуры очистки данных, методами обеспечивающими невозможность их восстановления:

- многократная перезапись;
- размагничивание.

7.4.15. При невозможности проведения очистки данных, носители должны уничтожаться физическим способом, процедура уничтожения должна регистрироваться, проводиться или контролироваться доверенным персоналом.

7.4.16. Рабочие места администраторов виртуализированной среды оборудуются аппаратными модулями доверенной загрузки (АПМДЗ), настраиваемыми на контроль загрузки АРМ только с доверенного носителя и на контроль целостности системных файлов ОС и средств управления виртуализированной средой.

7.4.17. Необходимость оборудования рабочих мест пользователей (администраторов) ЦИС АПМДЗ определяется моделью нарушителя и угроз ЦИС.

7.4.18. Порядок работы и защита съемных носителей информации, при их использовании в составе ЦИС, определяется в соответствии с внутренней регламентирующей документацией ведомства (учреждения).

7.5. Антивирусная защита

7.5.1. На всех АРМ администраторов виртуализированной среды должны применяться средства антивирусной защиты.

7.5.2. Для ЦИС категорий 1 и 1F использование средств антивирусной защиты на серверах и АРМ пользователей является обязательным. Для ЦИС категорий 2, 2F и 3 необходимость использования средств антивирусной защиты может определяться частной моделью угроз.

7.5.3. Антивирусное программное обеспечение должно выявлять, удалять и защищать объекты файловой системы ОС и съемных носителей от угроз вредоносного ПО следующих типов:

- классических вирусов;
- сетевых червей;
- троянских программ;
- программ-реклам;
- потенциально опасных приложений.

7.5.4. В состав проверки в обязательном порядке должны включаться следующие объекты:

- файлы при их записи и чтении;
- альтернативные потоки файловых систем NTFS;
- главные загрузочные записи и загрузочные сектора жестких дисков и съемных носителей.

7.5.5. Антивирусная проверка на АРМ пользователей должна проводиться в режиме реального времени. Для серверов допускается проводить антивирусную проверку по расписанию в период наименьшей нагрузки.

7.5.6. Для предотвращения загрузки пользователями на web сервера ЦИС файлов, содержащих вредоносное ПО, в составе ОЦОД должен быть организован

антивирусный шлюз, обеспечивающий антивирусную проверку загружаемого контента с использованием протоколов HTTP, FTP.

7.5.7. Необходимо регулярно выполнять обновление антивирусного ПО и его баз данных. Установку обновлений рекомендуется организовать в автоматическом режиме.

7.6. Регистрация событий информационной безопасности

7.6.1. В виртуализированной среде и непосредственно ЦИС должны проводиться процедуры мониторинга и анализа данных регистрации событий безопасности. Для осуществления мониторинга рекомендуется применение специализированных программных и/или технических средств.

7.6.2. Регистрация событий должна обеспечивать выявление неправомерных или подозрительных действий (операций). Как минимум должна проводиться регистрация следующих событий:

- события входа (выхода) пользователя (администратора) в систему (из системы) либо загрузки и инициализации операционной системы и ее программного останова;
- события запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых данных или защиты информации;
- события доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам или полям записей;
- события доступа программных средств к таким объектам доступа как терминалы, узлы сети, линии (каналы) связи, внешние устройства;
- события изменения конфигурации параметров безопасности и учетных записей администраторов.

7.6.3. В параметрах регистрации событий должны фиксироваться:

- дата и время события;
- идентификаторы субъектов и объектов доступа;
- тип события;
- результат события.

7.6.4. Сбор событий в виртуализированной среде и ЦИС должен осуществляться на всех компонентах, включая средства защиты информации.

7.6.5. Система регистрации событий виртуализированной среды дополнительно должна иметь возможность сбора и анализа событий регистрируемых в локальных журналах безопасности операционных и прикладных систем серверов VM.

7.6.6. Системное время на всех компонентах виртуализированной среды должно быть синхронизировано с использованием единого источника времени.

7.6.7. Журналы регистрации событий должны быть защищены от изменений и доступны только администраторам информационной безопасности виртуализированной среды.

7.6.8. События в журналах регистрации виртуализированной среды и серверных компонентах ЦИС должны сохраняться в течение не менее 3 месяцев.

7.7. Контроль защищенности

7.7.1. Контроль защищенности компонентов ЦИС и виртуализированной среды (включая возможность контроля ПО, установленное на VM) должен проводиться с использованием специализированных программных средств реализующих функции:

- выявления и идентификацию всех функционирующих сетевых узлов;
- выполнение поиска наличия уязвимостей системного и прикладного программного обеспечения сканируемых узлов, включая как уязвимости самого программного обеспечения, так и уязвимости связанные с ошибками его конфигурирования;
- проведение оценки опасности (критичности) выявленных уязвимостей с выдачей рекомендаций по их устранению.

7.7.2. Контроль защищенности должен проводиться на регулярной основе не реже чем один раз в три месяца, а также после значимых изменений конфигурации виртуализированной среды: установка новых компонентов, запуска новых VM, изменение топологии сети, изменение правил МЭ, установка новых версий ПО и других изменений, определяемых администратором как значимые.

7.7.3. Сканирование компонентов ЦИС и виртуализированной среды должно выполняться как со стороны внутренней сети ЦИС или виртуализированной среды, так и со стороны внешних по отношению к ЦИС или виртуализированной среде сетей.

7.7.4. Установка обновлений безопасности на компоненты ЦИС и виртуализированной среды должна проводиться не позже чем через 1 месяц после их выпуска при условии, что они не нарушают требования сертификации.

7.8. Криптографическая защита

7.8.1. Средства криптографической защиты должны использоваться при осуществлении удаленного административного доступа к компонентам виртуализированной среды и операционным системам VM, а также при осуществлении сетевого взаимодействия серверных компонентов ЦИС с пользователями или иными информационными системами с использованием каналов связи общего пользования.

7.8.2. Защита удаленного доступа и сетевого информационного взаимодействия осуществляется с использованием технологий VPN.

7.8.3. Защиту с использованием протокола SSL/TLS допускается осуществлять только в отношении ЦИС категории 3.

7.8.4. SSL соединения должны проводиться в режиме аутентификации сервера. Цифровой сертификат сервера должен доверенным способом записываться на

АРМ пользователя или иметь возможность проверки с использованием внешнего доверенного центра сертификации.

7.8.5. Рекомендуется использовать для организации защищенных VPN туннелей цифровые сертификаты.

7.8.6. Срок действия сертификатов или общих ключей, используемых для создания VPN соединений, не должен превышать 1 года.

7.8.7. Для хранения криптографических ключей рекомендуется использовать специальные съемные носители в защищенном исполнении (токены, смарт – карты и т.п.).

7.8.8. Криптографическая защита информации должна осуществляться с использованием криптоалгоритма ГОСТ 28147-89.

7.8.9. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ должны осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам, а также требованиями нормативных документов ФСБ России [9 - 11].

7.9. Обеспечение устойчивости функционирования

7.9.1. Создание виртуализированной среды должно осуществляться с применением высоконадежных устройств обработки и хранения данных, имеющих собственные функции отказоустойчивости или функции горячего резервирования (кластеризации).

7.9.2. Для зоны безопасности «1» ОЦОД должен создаваться избыток серверов виртуализации для обеспечения возможности перезапуска на них VM, ранее запущенных на серверах которые вышли из строя.

7.9.3. Электропитание серверного оборудования, используемого в зоне безопасности «1» ОЦОД должно осуществляться с использованием сетевых фильтров предназначенных для подавления промышленных высокочастотных помех.

7.9.4. Резервное копирование в виртуализированной среде осуществляется для файлов VM. Процедуры резервного копирования и восстановления осуществляются только администратором виртуализированной среды, на основании регламента резервного копирования или заявок предоставляемых администраторами ЦИС.

7.9.5. Запись и хранение резервных копий файлов VM может осуществляться на следующих устройствах:

- выделенный раздел системы хранения данных;
- роботизированная ленточная библиотека.

7.9.6. Установка любых обновлений на всех программных компонентах виртуализированной среды должна выполняться только после успешного тестирования обновлений на отдельных элементах.

7.9.7. Обеспечение необходимых условий эксплуатации технических средств виртуализированной среды, противопожарной защиты, гарантированного

электропитания, доступа к внешним сетям передачи данных, а также других необходимых условий должны обеспечиваться путем заключения сервисных соглашений с организацией, эксплуатирующей ОЦОД. Сервисное соглашение должно предусматривать необходимые параметры каждого сервиса и допустимые периоды простоя.

7.9.8. Обеспечение требуемого режима доступности серверных компонентов ЦИС должно регламентироваться сервисными соглашениями между ведомствами (учреждениями) операторами ЦИС и организациями, обеспечивающими эксплуатацию виртуализированной среды.

7.9.9. Ведомствам (учреждениям) операторам ЦИС, относящихся к категориям 1 и 1F, рекомендуется использовать услуги нескольких провайдеров связи для доступа АРМ пользователей к ресурсам ЦИС посредством внешних сетей передачи данных.

7.10. Защита от утечек по техническим каналам

7.10.1. Процедуры аутентификации администраторов ЦИС и виртуализированной среды с использованием паролей должны исключать непосредственное присутствие посторонних лиц при вводе пароля.

7.10.2. Размещение устройств вывода информации, входящих в состав АРМ, должно выполняться таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей защищаемые данные.

7.10.3. При необходимости, оконные проемы помещений, в которых размещаются АРМ, должны оборудоваться шторами, жалюзями или иными методами, препятствующими удаленному просмотру информации.

7.10.4. Необходимость организации защиты компонентов ЦИС, размещаемых в ОЦОД, от утечек за счет ПЭМИН устанавливается с учетом реализованных на объекте ОЦОД организационно-технических мер - пропускного режима, контроля за действиями персонала в помещениях ОЦОД, условий размещения ОЦОД на объекте, наличия контролируемой территории, использование СЗИ от утечки по техническим каналам. При наличии оснований полагать их недостаточными могут приниматься дополнительные меры, реализуемые на уровне отдельной ЦИС.

7.10.5. Ведомствам (учреждениям) операторам ЦИС, относящихся к категориям 1 и 1F, рекомендуется размещать серверы ЦИС, не переносимых в ОЦОД, и АРМ пользователей в местах, наиболее удаленных от границ контролируемой зоны объекта, на котором размещаются компоненты ЦИС.

7.11. Регламентация мероприятий по защите информации

7.11.1. Содержание мероприятий по поддержанию необходимого уровня ИБ в ОЦОД и ЦИС, выполняемых персоналом в ходе эксплуатации систем, а также ответственность за выполнение данных мероприятий должны устанавливаться во внутренних документах, определяющих политику ИБ в отношении эксплуатируемых систем.

7.11.2. Рекомендуется включать в инструкции персонала следующие положения:

- Порядок организации работ по защите информации;
- Периодичность выполнения мероприятий;
- Действия при выявлении инцидентов безопасности.

8. Требования по сертификации используемых средств защиты

8.1. Для защиты компонентов ЦИС категорий 1 и 1F допускается использовать только сертифицированные программные или аппаратно - программные компоненты, выполняющие функции защиты информации, а также специальные средства защиты информации:

- межсетевые экраны не ниже чем по 3 классу защищенности (в соответствии с [14]);
- средства обнаружения вторжений не ниже чем по 4 классу защиты (в соответствии с [16])[4];
- СЗИ (программные части) не ниже чем по 4 уровню отсутствия НДВ (в соответствии с [5]);
- СЗИ предназначенные для использования в АС класса не ниже 1Г (в соответствии с [15]).

8.2. Для защиты компонентов ЦИС категорий 2 и 2F допускается использовать только сертифицированные программные или аппаратно - программные компоненты, выполняющие функции защиты информации, а также специальные средства защиты информации:

- МЭ, не ниже чем по 4 классу защищенности (в соответствии с [14]);
- средства обнаружения вторжений по 6 - 4 классу защиты в зависимости от требуемой защищенности ЦИС (в соответствии с [16])[5];
- СЗИ, предназначенные для использования в АС класса не ниже 1Г (в соответствии с [15]).

8.3. Для защиты компонентов ЦИС категорий 3 допускается использовать иные, разрешенные к применению руководителем организации оператора ЦИС средства защиты информации.

8.4. Средства криптографической защиты информации, применяемые для защиты ЦИС всех категорий и виртуализированной среды, должны быть сертифицированными и иметь класс защиты, определяемой соответствующей моделью нарушителя.

8.5. Для гарантированного удаления (уничтожения) данных с магнитных носителей должны применяться сертифицированные программные или технические средства.

[4] Только для средств, версии которых выпущены после 15 марта 2012 г.
[5] Только для средств, версии которых выпущены после 15 марта 2012 г.

9. Требования к переносу ЦИС в виртуализированную среду ОЦОД

9.1. В виртуализированную среду ОЦОД могут быть перенесены ЦИС соответствующие критериям целесообразности переноса, определенных в разделе 5.2настоящего документа.

9.2. ЦИС может быть перенесена в виртуализированную среду ОЦОД после выполнения следующих мероприятий:

- классификация ЦИС и отнесение ее к одной из категорий в соответствии с разделом 5.3 настоящего документа;
- определения требуемых сервисов обеспечения информационной безопасности, предоставляемых ОЦОД, которые ЦИС будет использовать;
- реализации в ЦИС всех необходимых собственных механизмов обеспечения информационной безопасности в соответствии с требованиями нормативных документов по защите информации и частной моделью угроз и нарушителя.

9.3. Перенос ЦИС в виртуализированную среду ОЦОД должен выполняться в следующем порядке:

1. оформление заявки в адрес организации оператора виртуализированной среды на выделение необходимого количества виртуальных машин, с указанием их параметров и требований к установке операционных систем, а также на использование сервисов информационной безопасности, предоставляемых ОЦОД с указанием необходимых параметров для каждого сервиса;
2. оператор виртуализированной среды выполняет проектирование размещения ЦИС;
3. оператор виртуализированной среды производит выделение необходимых ресурсов, установку необходимого системного ПО, подключение и настройку всех необходимых сервисов обеспечения информационной безопасности в отношении ЦИС;
4. осуществляется организация и настройка защищенного канала взаимодействия между площадкой (ми) ведомства (учреждения) и ОЦОД, необходимого для безопасного взаимодействия администраторов и пользователей ЦИС с серверными компонентами системы и предоставление администратору ЦИС данных о выделенном адресном пространстве и параметров удаленного доступа;
5. установка и настройка администратором ЦИС на выделенных виртуальных машинах прикладного программного обеспечения;
6. поверка функционирования серверных компонентов ЦИС в виртуализированной среде;
7. перенос данных на серверные компоненты ЦИС и предоставление пользователям удаленного доступа к ЦИС;

8. заключение сервисных соглашений между ведомством и организацией оператором виртуализированной среды сервисных соглашений по использованию сервисов обеспечения информационной безопасности и обеспечения доступности серверных компонентов ЦИС для пользователей.

10. Процедура пересмотра требований

10.1. Пересмотр требований настоящего документа выполняется на периодической основе не реже чем раз в два года, а также в следующих случаях:

- изменений в законодательстве Российской Федерации, касающихся вопросов защиты информации;
- изменений в нормативных документах Правительства г. Москвы, касающихся вопросов защиты информации и имеющих более высокий статус чем данный документ;
- изменения бизнес – требований к функционированию централизованных информационных систем и использованию новых способов и технологий обработки информации.
- появления новых угроз и способов нарушения безопасности информации, обрабатываемой в виртуализированной среде ОЦОД.

10.2. Инициация процедуры пересмотра осуществляется владельцем документа – лицом или подразделением в чью обязанность входит поддержка в актуальном состоянии актов Технической политики города Москвы в сфере информационно-коммуникационных технологий.

10.3. Непосредственно пересмотр требований выполняется рабочей группой экспертов по информационным технологиям и информационной безопасности, привлекаемых владельцем документа. Рабочая группа готовит предложения по изменению положений настоящего документа.

10.4. Согласование изменений положений настоящего документа осуществляется руководством Департамента информационных технологий г. Москвы и утверждается руководителем органа, утвердившим предыдущую версию.

10.5. Обновленная версия документа рассылается владельцем всем заинтересованным организациям, подразделениям и лицам и публикуется в сборнике актов Технической политики города Москвы в сфере информационно-коммуникационных технологий.

10.6. Владельцем настоящего документа является Департамент информационных технологий города Москвы.

11.Приложение. Сервисы обеспечения ИБ ОЦОД

Сервисы обеспечения информационной безопасности, предоставляемые виртуализированной средой ОЦОД для ЦИС, а также параметры необходимые для оформления заявок на использование данных сервисов перечислены в таблице.

Таблица сервисов обеспечения ИБ ОЦОД

Сервис обеспечения ИБ	Параметры заявки на использование сервиса
Контроль трафика информационного обмена серверных компонентов ЦИС с пользователями и другими ИС с помощью средств МЭ, IDS/IPS (на сетевом и прикладном уровнях)	Таблица требуемых соединений с указанием IP адресов, протоколов и портов, правил трансляции адресов, необходимость в дополнительном контроле протоколов прикладного уровня (HTTP, SQL и др.)
Контроль защищенности системного и прикладного ПО компонентов ЦИС	Таблица с указанием IP адресов контролируемых узлов, версий операционных систем и прикладного ПО
Защита ЦИС от атак отказа обслуживания «DDoS»	IP адреса и DNS имена web серверов (сайтов)
Централизованная регистрация событий ИБ на серверных компонентах ЦИС и выявления инцидентов безопасности	Таблица с указанием IP адресов узлов, версий операционных систем и прикладного ПО, имена файлов журналов регистрации событий, возможность использования протокола SMTP для сбора событий
Организация защищенного удаленного доступа пользователей и администраторов ЦИС к серверным компонентам систем с использованием VPN шлюза	Перечень лиц, которым необходим доступ для администрирования ЦИС, IP адреса АРМ или подсетей с которых будет проводиться подключение, IP адреса ресурсов к которым будет проводиться подключение.
Организация защищенного удаленного доступа пользователей к web серверам с использованием SSL шлюза (алгоритм ГОСТ 28147-89)	Перечень IP адресов и hostname web серверов, сертификаты и закрытые ключи сервера, необходимые для установления SSL соединений
Резервное копирование и восстановление файлов VM	Регламент резервного копирования определяющий состав объектов и периодичность резервного копирования.
Антивирусный контроль входящего трафика на серверные компоненты ЦИС	IP адреса web серверов для которых необходимо выполнять проверку трафика.