Политика информационной безопасности персональных данных
АО «Чувашская энергосбытовая компания»

1. Область применения

Настоящая Политика определяет способы использования информационно-вычислительных ресурсов АО «Чувашская энергосбытовая компания» (далее – Общество) с соблюдением требований информационной безопасности.

Политика информационной безопасности (далее – Политика) разработана в соответствии с требованиями Концепции информационной безопасности персональных данных АО «Чувашская энергосбытовая компания».

Настоящая Политика является руководящим документом и обязательна для применения всеми сотрудниками Общества, предназначена для обязательного использования в Обществе и распространяется на всю деятельность Общества.

2. Термины, определения, обозначения и сокращения

В настоящей Политике Общества применены следующие термины с соответствующими определениями:

Администраторы ИСПДн – непосредственно разработчики ИСПДн, инженеры АСУ отделений.

Информационно-вычислительные ресурсы - серверы и основное коммутационное оборудование.

ИСПДн – информационная система персональных данных

Критичность информационного ресурса - важность информационного ресурса с точки зрения достижения задач деятельности Общества.

В настоящей политике организации применены следующие обозначения и сокращения:

НСД - несанкционированный доступ.

ФСБ - Федеральная служба безопасности.

ФСТЭК - Федеральная служба по техническому и экспортному контролю.

3. Общие положения

Политикой информационной безопасности охватываются все информационно-вычислительные ресурсы Общества. В состав информационно-вычислительных ресурсов Общества включаются данные, информация, программное обеспечение, аппаратные средства, средства обслуживания и телекоммуникации. Политика применима ко всем лицам, имеющим отношение к информационно-вычислительным ресурсам Общества, включая всех сотрудников, поставщиков и лиц, работающих по контракту, использующих эти ресурсы.

Лица, нарушившие требования Политики безопасности и иных руководящих документов по вопросам обеспечения безопасности информационно-вычислительных ресурсов Общества, несут ответственность в соответствии с действующим законодательством РФ, в том числе дисциплинарного характера.

4. Цели политики информационной безопасности

Основными целями Политики является обеспечение целостности, доступности и

конфиденциальности информационно-вычислительных ресурсов Общества.

Настоящая Политика определяет достижение следующих целей:

- обеспечение безопасности информационных ресурсов Общества в соответствии с критичностью, ценностью и значимостью.
- обеспечение защищенности информационно-вычислительных ресурсов с использованием решений, эффективных с точки зрения качества защиты и рентабельных с точки зрения экономической целесообразности.
- обеспечение качественной поддержки защиты информационно-вычислительных ресурсов во всех производственно-технических и управленческо-экономических областях функционирования Общества.
- обеспечение индивидуальной подотчетности всех участников информационно-вычислительного взаимодействия.
- обеспечение гарантированной возможности проверки информационно-вычислительной инфраструктуры Общества.
- обеспечение сотрудников Общества достаточно полными руководящими документами, которые осуществляют распределение обязанностей по соблюдению требований информационной безопасности во время работы с информационно-вычислительными ресурсами Общества.
- обеспечение каждого компонента информационно-вычислительной системы планом обеспечения непрерывности работы и сохранности информационно-вычислительных ресурсов.
- соблюдение законодательства Российской Федерации.

5. Реализация политики информационной безопасности

Реализация Политики информационной безопасности исходит из предпосылки, что невозможно обеспечить достаточный уровень защищенности информации не только с помощью одного отдельного мероприятия, но и с помощью их простой совокупности. Необходимо их системное и комплексное применение, а отдельно разрабатываемые элементы информационно-вычислительной системы Общества должны рассматриваться как часть единой информационно-вычислительной среды в защищенном исполнении.

Основными направлениями реализации общей Политики обеспечения безопасности информации являются:

- обеспечение защиты информационно-вычислительных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки.
- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи.

Настоящая Политика уточняет требования информационной безопасности по следующим направлениям:

- реализация системы инженерно-технических и организационных мер охраны информационно-вычислительных ресурсов Общества, с обязательной многорубежностью и равнопрочностью, с комплексным применением современных программно-технических средств обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий.
- ограничение доступа исполнителей и посторонних лиц в помещения, где производится накопление, хранение, обработка и передача данных между различными

структурными единицами информационно-вычислительной системы Общества.

- разграничение доступа сотрудников к информационно-вычислительным ресурсам, программно- аппаратным средствам обработки (передачи) и защита информации в подсистемах различного уровня и назначения.
- учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль над несанкционированным доступом и действиями сотрудников и посторонних лиц.
- надежное хранение машинных носителей информации, и паролей (и иной подобной информации) и их обращение, исключающее хищение, подмену и уничтожение.

Практическая реализация целей защиты информации, в каждом структурном подразделении Общества, предполагает создание и функционирование систем и комплексов защиты информации в составе этих подразделений.

Последовательность реализации конкретных мероприятий по обеспечению безопасности информации предполагает решение следующих задач:

- определение критичной информации и её носителей.
- выявление наиболее вероятных угроз для конкретных информационно-вычислительных ресурсов Общества.
- выявление уязвимых мест процессов накопления, хранения, обработки, передачи и использования информации.
- оценку возможных последствий, вызванных нарушением безопасности информации.
- разработку эффективных требований информационной безопасности.
- разработку системы управления информационной безопасности Общества.
- контроль за реализацией комплекса мер защиты в соответствии с требованиями информационной безопасности.

Необходимо регулярно проводить уточнение и конкретизацию целей, задач и путей обеспечения безопасности информационно-вычислительной инфраструктуры Общества применительно к функциональному назначению конкретных структурных подразделений Общества.

6. Организационная структура системы безопасности информационно-вычислительной инфраструктуры

Организационную структуру системы безопасности информационно-вычислительной инфраструктуры образуют:

- ответственный за обеспечение безопасности персональных данных - руководитель дирекции экономической безопасности.
- руководитель дирекции поддержки централизованных информационных систем.
- руководитель отдела информационных технологий.
- инженеры АСУ МРО, Администраторы ИСПДн, Разработчики ИСПДн, Администраторы.
- исполнители, допущенные к информационно-вычислительным ресурсам, связанным с обработкой критичной информации.

Зоны ответственности и функции участников процесса обеспечения информационно- вычислительной инфраструктуры определяются в соответствии с положениями о подразделениях, приказами по Обществу.

7. Организационные и организационно-технические мероприятия по созданию и поддержанию системы управления информационной безопасности

Достижение необходимого уровня защиты информационно-вычислительной инфраструктуры Общества обеспечивается подготовкой и принятием соответствующих административно-правовых и организационно-технических мер поддержки функционирования системы управления информационной безопасности.

Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования системы управления информационной безопасности включают:

- разовые мероприятия.
- периодически проводимые мероприятия.
- постоянно проводимые мероприятия (мониторинг).
- мероприятия, проводимые при осуществлении или возникновении изменений в составе информационно-вычислительной системы.

7.1. Разовые мероприятия

К разовым мероприятиям относят:

- разработку и утверждение должностных обязанностей сотрудников, ответственных за обеспечение и контроль безопасности информационно-вычислительной инфраструктуры Общества.
- мероприятия по созданию нормативных и организационно-распорядительных документов по обеспечению защиты информационно-вычислительных ресурсов Общества.
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы по вопросам обеспечения безопасности информационно-вычислительной системы.
- оформление юридических документов по вопросам регламентации отношений Общества с сотрудниками.
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании объектов информатизации.
- мероприятия по созданию системы управления информационной безопасности.
- мероприятия по разработке правил разграничения доступа к информационно-вычислительным ресурсам Общества.
- определение порядка проектирования, разработки, модификации, приобретения, приема в эксплуатацию, контроля целостности программных продуктов, а также порядок обновления версий используемого программного обеспечения.

7.2. Периодически проводимые мероприятия

К периодически проводимым мероприятиям относят:

- распределение реквизитов разграничения доступа (ключей, паролей, идентификаторов и т.п.).
- анализ системных журналов, для обнаружения нарушений и принятия мер по выявлению причин нарушений.
- анализ прав доступа сотрудников к информационно-вычислительным

ресурсам.

- мероприятия по корректировке системы управления информационной безопасностью.

7.3. Постоянно проводимые мероприятия

Постоянно проводимые мероприятия включают:

- мероприятия по обеспечению надлежащего уровня физической защиты объектов информатизации Общества, в том числе и противопожарная охрана, охрана помещений, пропускной режим.
- мероприятия по непрерывной поддержке функционирования системы управления информационной безопасности.
- контроль за реализацией системы управления информационной безопасности.
- проведение анализа состояния и оценка эффективности системы управления информационной безопасностью.

7.4. Мероприятия, проводимые при осуществлении или возникновении изменений в составе информационно- вычислительной системы

К мероприятиям, проводимым при осуществлении или возникновении изменений в составе информационно-вычислительной системы, относят:

- мероприятия, осуществляемые при кадровых изменениях.
- мероприятия, осуществляемые при модификациях оборудования и программного обеспечения.
- мероприятия по обучению основам информационной безопасности вновь принятых на работу сотрудников.

7.5. Плановые мероприятия по обеспечению безопасности информационно-вычислительной инфраструктуры

Важной и специфической проблемой является поддержание функционирования и эффективности системы управления информационной безопасностью. Для решения этой задачи дирекция экономической безопасности организует и регулярно проводит ряд плановых мероприятий:

- в целях обеспечения выполнения требований информационной безопасности проводит плановые и внеплановые выборочные проверки выполнения этих требований, обоснованность использования работниками доступа к информационно-вычислительным ресурсам Общества, с помощью специализированного программного обеспечения.
- следит, чтобы все правила и требования по обеспечению информационной безопасности исключали двоякое толкование и четко указывали на необходимость принимать те или иные меры, когда эти правила нарушаются.
- проводит внутренние проверки технического состояния и режима эксплуатации системы управления информационной безопасности.
- проводит внеплановые проверки функционирования системы управления информационной безопасности.
- совместно с отделом ИТ и ДПЦИС курирует разработку планов работ по восстановлению информационно вычислительных ресурсов в нештатных ситуациях.

7.6. Обучение сотрудников методам защиты информации

Обучение сотрудников Общества основам безопасного использования информационно- вычислительных ресурсов строится по следующему плану:

- доведения до сотрудников принципов защиты информации в Обществе.
- организация регистрации фактов, причин и обстоятельств инцидентов, связанных с нарушением требований информационной безопасности.
- введение персональной ответственности за защиту информационно-вычислительных ресурсов.

Ответственность за разработку планов защиты автоматизированных систем возлагается на руководителя ОИТ.

8. Организация работ по защите информационно- вычислительной системы

Организацию работ по обеспечению безопасности информационно-вычислительной системы и контроль эффективности принимаемых мер защиты в Обществе и его отделениях осуществляет ответственный за обработку персональных данных.

Ответственным за обеспечение защиты персональных данных осуществляется:

- проведение исследования состояния информационно-вычислительной системы для определения эффективности защиты и соблюдения всех требований информационной безопасности.
- разработка модели нарушителя.
- определение возможных угроз информационно-вычислительной системы, путей и последствий их реализации.
- определение необходимого уровня защищённости информационно-вычислительной системы в виде перечня требований по защите.
- определение необходимых функций системы управления информационной безопасностью в соответствии с установленными требованиями.
- разработка комплекса мероприятий, обеспечивающих необходимый уровень защищённости информационно-вычислительной системы.

8.1. Администрирование информационно-вычислительных ресурсов

Администрирование информационно-вычислительных ресурсов должно обеспечивать надежное и бесперебойное функционирование информационной инфраструктуры Общества, соответствие требованиям информационной безопасности и возлагается на системных Администраторов. Обязанности Администраторов в части обеспечения информационной безопасности излагаются в должностных инструкциях.

Разрабатываемыми нормативными документами, регламентирующими процесс обеспечения информационной безопасности, обязательно должны быть отражены следующие положения:

- процедура запуска и остановки информационно-вычислительных ресурсов.
- инструкции по выполняемым мероприятиям в случае возникновения каких-либо внештатных ситуаций.
- инструкции по изготовлению резервной копии хранимой и обрабатываемой

информации на информационно-вычислительных ресурсах Общества.

- порядок работы с носителями информации и их уничтожения.
- процедура восстановления работоспособности информационно-вычислительной системы.

8.2. Администрирование ИСПДн

Администратор ИСПДн должен обеспечивать надежное и бесперебойное функционирование ИСПДн ресурсов Общества и соответствие требованиям информационной безопасности. Обязанности администратора ИСПДн в части обеспечения информационной безопасности излагаются в должностных инструкциях.

Разрабатываемые администратором ИСПДн нормативные документы, регламентирующие процесс обеспечения информационной безопасности, обязательно должны содержать следующие положения:

- процедура запуска и остановки ИСПДн.
- допустимые процедуры оперирования с массивами информации.
- инструкции по выполняемым мероприятиям в случае возникновения каких-либо внештатных ситуаций с ИСПДн.
- инструкции по изготовлению резервной копии системной информации на информационно-вычислительных ресурсах Общества.
- процедура восстановления работоспособности ИСПДн.

8.3. Управление правами доступа сотрудников

В информационно-вычислительной системе Общества организуется контроль за предоставлением и использованием правам доступа сотрудников.

Устанавливаются следующие общие правила:

- обязательное использование имени пользователя и пароля (или иных способов идентификации, авторизации и аутентификации), что позволяет определить права доступа того или иного сотрудника к информационно-вычислительным ресурсам и подтвердить его полномочия на том или ином ресурсе Общества.
- идентификация терминалов, рабочих станций и других устройств по сетевым реквизитам (по имени, по IP-адресу, по MAC-адресу).
- выдаваемые сотруднику права не должны быть избыточными, то есть должны иметь только минимально необходимые права для доступа к тем или иным информационно-вычислительным ресурсам.
- блокирование пользователей на периоды длительного отсутствия (более 21 рабочего дня) в связи с отпуском, командировкой. Доступ к информационным ресурсам, закреплённым за руководителем подразделения, предоставляется на период его отсутствия, сотруднику, исполняющему обязанности руководителя подразделения, на основании приказа о возложении обязанностей.
- обязательная постоянная блокировка учетных записей пользователей при их увольнении с минимальной задержкой между увольнением и блокировкой. Блокирование учётных записей осуществляется администратором на основании информации, предоставляемой отделом по работе с персоналом, в течение одного рабочего дня, с момента увольнения сотрудника.

8.4. Пересмотр прав сотрудников

В целях обеспечения эффективного контроля за соблюдением требований информационной безопасности Общества производится регулярный пересмотр прав доступа сотрудников к информационно-вычислительным ресурсам. В связи с этим устанавливается период пересмотра полномочий доступа сотрудников не реже 1 раз в год.

Если у сотрудника меняются должностные обязанности (в связи с переводом на другую должность, в связи с изменением функциональных обязанностей и т.п.) пересмотр прав доступа производится сразу же после изменения статуса сотрудника. Изменение прав доступа сотрудника производится Администратором ИСПДн на основании заявки, направляемой руководителем подразделения, в подчинении которого состоит сотрудник.

Организация процесса пересмотра прав доступа сотрудников к информационно-вычислительным ресурсам возлагается на сотрудников отдела ИТ.

8.5. Требования обоснованности доступа

Требование обоснованности предоставления прав доступа для работы с информационно-вычислительными ресурсами Общества позволяют значительно снизить количество попыток необоснованного получения избыточных прав.

Устанавливается следующий порядок предоставления прав доступа к информационно-вычислительным ресурсам Общества:

- при необходимости получения доступа к информационно-вычислительным ресурсам пользователь направляет заявку в ДПЦИС или ОИТ, где указывает необходимые уровни доступа в соответствии с функциональными обязанностями.
- данная заявка визируется руководителем сотрудника, который несет ответственность за необоснованность или чрезмерные права, предоставленные его подчиненному.
- Сотрудник отдела ИТ на основании полученной заявки с визами руководителя дирекции поддержки централизованных информационных систем и непосредственного руководителя сотрудника подключает указанного в заявке сотрудника к ресурсам.
- В случае необходимости получения доступа к ИСПДн, на основании полученной заявки с визами, администратор дирекции поддержки централизованных информационных систем подключает указанного в заявке сотрудника к ресурсам ИСПДн.
- периодически, но не реже 1 раз в квартал сотрудники отдела ИТ проводят проверку списка пользователей для выявления уволенных сотрудников или необоснованного завышения прав.
- получение доступа к ресурсам, не входящим в функциональные обязанности пользователя предоставляются на основании служебной записки, согласованной с исполнительным директором.

8.6. Управление паролями сотрудников

На объектах информационно-вычислительной системы должен осуществляться контроль над процессом назначения и использования паролей.

Управление паролями организуется в соответствии с Регламентом по

обеспечению парольной защиты.

Рекомендуется разделить требования к паролям на две группы: обыкновенные требования и повышенные требования. Обыкновенные требования распространяются на всех сотрудников Общества, а повышенные требования предъявляются к паролям сотрудников, наделенных особыми правами в информационно-вычислительной системе, и к паролям руководителей среднего и высшего звена.

Повышенные требования предъявляются к паролям: системных администраторов, администраторов ИСПДн, сотрудников, ответственных за информационную безопасность, и, как ранее оговаривалось, к паролям среднего и высшего руководства. Особо в этой группе следует выделить пароли доступа к коммутационному оборудованию и серверам, использование этих паролей для доступа к каким-либо иным ресурсам запрещается, необоснованное постоянное использование этих паролей так же недопустимо.

8.6.1. Основные требования к паролям с повышенными требованиями таковы:

- смена пароля должна производиться не реже одного раза в шесть месяцев.
- в самом пароле обязательное использование букв в разном регистре, цифр, специальных символов.
- запрещено хранение и передача аутентификационных данных для доступа в ИС в электронном виде (файлы, электронная почта, флэш-накопители и так далее) и на бумажных носителях. В случае необходимости допускается организовать безопасное хранение парольной или ключевой информации с использованием дополнительных средств защиты (сейфы, запирающиеся шкафы и ящики).
- количество символов в пароле должно быть не менее 9.

8.6.2. Основные требования к паролям с обыкновенными требованиями:

- смена пароля должна производиться не реже одного раза в год.
- запрещено хранение и передача аутентификационных данных для доступа в ИС в электронном виде (файлы, электронная почта, флэш-накопители и так далее) и на бумажных носителях. В случае необходимости допускается организовать безопасное хранение парольной или ключевой информации с использованием дополнительных средств защиты (сейфы, запирающиеся шкафы и ящики).
- количество символов в пароле должно быть не менее 6.

Администраторы ИСПДн должны иметь по две учетные записи. Одна учетная запись должна иметь практически обыкновенные права в информационно-вычислительной системе, и пароль к этой учетной записи должен удовлетворять обыкновенным требованиям. Вторая учетная запись должна использоваться только для выполнения специальных работ, связанных с высоким уровнем доступа, в которых требуется наличие повышенных прав, а пароль к этой учетной записи должен удовлетворять повышенным требованиям. Запрещается использование одинакового пароля для разных требований. Также запрещается необоснованная работа с учетной записью, предназначенной для выполнения специальных работ, связанных с высоким уровнем доступа.

8.7. Регистрация пользователей

На всей территории деятельности Общества вводятся в действие единые

процедуры управления процессом предоставления прав доступа к информационно-вычислительной системе. Процедуры регистрации включают в себя все стадии жизненного цикла управления доступом сотрудников - от начальной регистрации новых пользователей до удаления учетных записей сотрудников.

Процедура регистрации пользователей в информационно-вычислительной системе должна включать как минимум следующие основные проверки:

- предоставлено ли пользователю разрешение на использование информационно-вычислительных ресурсов его непосредственным руководителем и ответственным за обеспечение защиты персональных данных.
- наличие регистрации в системе у сотрудников, использующих информационно-вычислительные ресурсы Общества.
- достаточность уровня доступа сотрудников к информационно-вычислительной системе и соответствие этого уровня принятой Политике информационной безопасности.
- своевременности лишения всех прав доступа сотруднику, покинувшему Общество.
- отсутствия в системе устаревших учетных записей.

8.8. Работа с представителями сторонних организаций

Привлечение представителей сторонних организаций к работе по модернизации информационно-вычислительной инфраструктуры Общества может привести к появлению дополнительных рисков.

В Обществе принимаются следующие меры по снижению указанных рисков:

- запрет удаленного администрирования информационно-вычислительных ресурсов. Удаленное администрирование разрешено только в исключительных случаях с разрешения исполнительного директора Общества, при этом должны быть заключены соответствующие соглашения с обязательным обозначением границ ответственности и правил администрирования этих ресурсов.
- запрет использования информационно-вычислительных ресурсов Общества сторонними организациями. Предоставлять информационно-вычислительные ресурсы Общества для использования сторонним организациям можно только в исключительных случаях с разрешения исполнительного директора Общества, при этом должны быть заключены соответствующие соглашения с обязательным обозначением границ ответственности и правил использования этих ресурсов.
- правила работы с представителями сторонних организаций и порядок проверки соблюдения требований информационной безопасности должны быть описаны в инструкциях Администраторов Общества. Разработка инструкций входит в функции отдела ИТ.
- отдельно необходимо оговорить ответственность за нарушение требований информационной безопасности и санкции в случае незаконного разглашения информации, нарушения целостности или нарушения работоспособности ресурса.

9. Обеспечение безопасности при эксплуатации информационно-вычислительных ресурсов

Основой обеспечения информационной безопасности при эксплуатации информационно- вычислительных ресурсов Общества является:

- разделение на независимые информационно-вычислительные сети

пользовательские и производственно-технологические.

- запрещение пробных запусков вновь изготовленного программного обеспечения на реально работающих объектах, для подобных испытаний необходимо подготовить специальный сегмент виртуализации с обязательным изолированием от остальной сети Общества.
- изолирование коммутационного оборудования и информационно-вычислительных ресурсов для обработки, хранения и накопления информации, систем резервного копирования, в отдельных помещениях (шкафах) с ограниченным и строго контролируемым доступом сотрудников Общества.
- размещение вычислительных мощностей и резервных хранилищ данных в разнесенных помещениях.
- внедрение в информационно-вычислительную инфраструктуру Общества системы управления информационными ресурсами, позволяющей контролировать разграничение доступа к информационным ресурсам и осуществлять мониторинг событий.
- внедрение в информационно-вычислительную инфраструктуру Общества системы управления информационной безопасностью.
- исключение подключения в информационно-вычислительную сеть Общества удаленных подразделений и территориальных отделений без использования защищенного обмена информацией между ними с использованием криптографических средств защиты информации либо защищенных туннелей, не позволяющих считывать информацию с каналов связи третьими лицами.
- организация резервных каналов связи для обеспечения бесперебойных информационных потоков между структурными подразделениями.
- организация системы обеспечения информационной безопасности таким образом, чтобы отключение МРО или участков от сети Общества не оставила их незащищенными (отделения или участки должны иметь свои средства обеспечения информационной безопасности).
- все сервера Общества и сервера МРО должны быть выделены в отдельные сетевые сегменты (подсети), снабженными системами мониторинга вторжений.
- любое соприкосновение информационно-вычислительной среды с внешним миром должно происходить только через системы обеспечения информационной безопасности.
- информационно-вычислительная система Общества должна иметь в своем составе демилитаризованную зону для создания каких - либо информационно-вычислительных ресурсов общего пользования.

9.1. Контроль доступа в помещения и к коммуникационному оборудованию

Узловое коммуникационное оборудование, важные или уязвимые элементы информационно - вычислительной системы размещаются в отдельных помещениях с контролем доступа. Рядовые коммутаторы размещаются в изолированных шкафах (ящиках), запирающихся на ключ.

На объектах информационно-вычислительной инфраструктуры устанавливается обязательный для всех сотрудников режим деятельности, его описывают в документах по пропускному и внутриобъектовому режиму, и включает меры, направленные на исключение нарушения требований информационной безопасности:

- двери в рабочие кабинеты в нерабочее время или при отсутствии в кабинетах

сотрудников запираются на ключ.

- выдача ключей производится только лицам, работающим в помещении или ответственным за него.
- несанкционированный вынос информационно-вычислительной техники запрещается.
- перемещение информационно-вычислительной техники и ресурсов, и иных составных частей информационно-вычислительной структуры Общества без соответствующих сопроводительных документов запрещается.

9.2. Требования к помещениям, в которых расположены информационно-вычислительные ресурсы

Помещения, в которых расположены информационно-вычислительные ресурсы Общества (серверы и основное коммутационное оборудование), должны удовлетворять следующим требованиям:

- помещение должно иметь площадь, позволяющую проводить беспрепятственное обслуживание информационно-вычислительных ресурсов.
- наличие источников бесперебойного питания для защиты информационно-вычислительных ресурсов обязательно.
- помещения должны быть снабжены пожарной и охранной сигнализациями.
- помещения должны комплектоваться средствами пожаротушения.
- помещения должны снабжаться системами кондиционирования воздуха с дублированием.
- по возможности необходимо использовать помещения, не имеющие окон, в случае наличия окон их необходимо сделать непрозрачными и укрепить с помощью металлических конструкций для исключения проникновения посторонних лиц в помещение.
- помещение желательно должно иметь окна только во внутренний двор.
- в помещениях не должно быть рабочих мест, за исключением рабочего места администратора, которое используется для обслуживания и управления информационно - вычислительной системой.

9.3. Удаленный доступ к информационно-вычислительным ресурсам

Информационно-вычислительные ресурсы Общества должны быть доступны удаленным подразделениям и отделениям (участкам) Общества. Для обеспечения информационной безопасности необходимо соблюдать следующие требования:

- всегда использовать только защищенное соединение с использованием криптографических средств к информационно-вычислительным ресурсам Общества удаленных подразделений и отделений/участков.
- все удаленные соединения должны быть под особым контролем (мониторингом) дирекции экономической безопасности.
- подключение удаленного отделения или участка производится только с согласования ДЭБ.
- удаленное подключение сотрудников к информационно-вычислительным ресурсам Общества возможно только после процедуры согласования с дирекцией экономической безопасности, с обязательным соблюдением требований использования криптографической защиты.

- все сотрудники, осуществляющие удаленное соединение, должны быть учтены отделом ОИТ, и их удаленная работа должна регулярно проверяться на предмет соблюдения всех требований информационной безопасности.
- удаленный доступ могут получить только действующие сотрудники Общества.

9.4. Использование криптографической защиты

Использование криптографической защиты позволит обезопасить информационные ресурсы Общества от незаконных посягательств различных внешних и внутренних недоброжелателей.

Криптографические средства защиты должны использоваться для защиты информационных ресурсов в процессе передачи информации за пределами Общества и при хранении ее на переносных компьютерах и носителях.

Мобильные пользователи обязаны использовать криптографические системы защиты информации, которые должны защищать хранящуюся информацию на жестком диске и информацию при перемещении ее между сетью Общества и мобильным пользователем.

Использование криптографических систем, не удовлетворяющих требованиям нормативных документов ФСБ, ФСТЭК и других государственных органов Российской Федерации, запрещается.

На линиях связи необходимо использовать программно-аппаратные системы шифрования, у которых имеются разрешительные документы в соответствии с требованием законодательства РФ.

Эксплуатацию и обслуживание средств криптографической защиты должны осуществлять специально подготовленные сотрудники Общества.

9.5. Обеспечение безопасности серверов

Сервера, используемые в информационно-вычислительной инфраструктуре Общества, должны быть защищены, а именно:

- в информационно-вычислительной системе необходимо сделать специализированный сегмент, в котором будут находиться сервера (в отделениях сервера также должны выделяться в отдельный сегмент).
- все программное обеспечение, которое устанавливается на сервера Общества, должно быть законно приобретенным с соблюдением всех требований авторского права.
- сегменты серверного оборудования должны быть защищены с использованием программно-аппаратных систем защиты от НСД при наличии технической возможности.
- все системы защиты должны управляться централизованно с использованием соответствующих систем управления, сотрудниками отдела ИТ.
- в тех случаях, когда не представляется возможным установка специализированных программно-аппаратных систем защиты, возможно использование программных реализаций подобных систем защиты.
- администрирование серверов должны производить сотрудники Общества - отдела ИТ и дирекции поддержки централизованных информационных систем.
- программное обеспечение должно регулярно обновляться из официальных

источников производителей программного обеспечения.

- сервера должны находиться в специально подготовленных помещениях.
- сервера должны быть подключены к системе централизованного мониторинга и управления информационно-вычислительной системы Общества, позволяющей централизованно управлять и осуществлять наблюдение за ними.

9.6. Контроль за работой пользователей

Пользователи информационно-вычислительных ресурсов Общества должны знать свои обязанности по соблюдению требований информационной безопасности. Контроль за работой пользователей включает следующие аспекты:

- мониторинг объема, входящего/исходящего трафика каждой рабочей станции.
- постоянный мониторинг авторизации при подключении к информационно-вычислительным ресурсам Общества.
- прямой мониторинг действий пользователя с применением системы DLP.
- аудит адресатов отправителей и получателей электронной почты, участвующих в переписке с сотрудниками Общества.
- аудит посещаемых Интернет адресов с рабочего места сотрудников.

9.7. Контроль за оборудованием

При работе с информационно-вычислительными ресурсами необходимо постоянно контролировать их общее состояние и режим работы.

Для обеспечения подконтрольности информационно-вычислительных ресурсов необходимо обеспечить доступ к этим ресурсам только авторизованных сотрудников, а сотрудники, в свою очередь должны, выполнять ряд правил и требований. Оставляя рабочее место, сотрудники должны обеспечить надлежащую защиту закрепленного за ними информационно-вычислительного оборудования и информации. Таким образом, сотрудник обязан:

- в конце рабочего дня завершить все сеансы связи.
- отлучаясь с рабочего места, сотрудник обязан заблокировать консоль своего компьютера, если программное обеспечение не позволяет блокировать консоль, компьютер должен выключаться.
- в конце рабочего дня перед уходом с рабочего места сотрудник обязан выключить свой компьютер, разрешается оставлять включенным компьютер только в исключительных случаях, предварительно согласовав это с непосредственным руководителем. Сотрудники, ответственные за соблюдение требований информационной безопасности, вправе проверить обоснованность принятого решения о включенном компьютере во внерабочее время. Данная норма не распространяется на сервера и иные информационно-вычислительные ресурсы общего использования.
- в случае обнаружения вредоносного программного обеспечения на каком-либо носителе или на рабочем компьютере, сотрудник обязан сообщить об этом своему непосредственному начальнику, сотрудникам отдела ИТ, которые в свою очередь сообщают об инциденте сотрудникам ответственным за антивирусную безопасность.
- запрещается передавать свои пароли кому-либо когда-либо.
- запрещается допускать к работе сторонних посетителей, не являющихся сотрудниками Общества.
- сотрудник Общества обязан применять все возможные и доступные средства в

рамках законодательства РФ и нормативно-правовых документов Общества для обеспечения соблюдения требований информационной безопасности.

9.8. Обеспечение безопасности кабельных систем

Защита кабельной системы направлена на снижение вероятности угроз информационной безопасности путем непосредственного подключения к информационным линиям, а также на обеспечение защиты кабельного оборудования от электромагнитных помех.

Политикой информационной безопасности предусматриваются следующие меры по защите кабельной системы:

- все информационные линии должны прокладываться вне общедоступных мест, что позволит значительно повысить защищенность от различных угроз и повреждений.
- силовые и информационные кабели должны быть разнесены в пространстве.
- кроссовые помещения и шкафы должны надежно запираться.
- резервирование линии связи.
- постепенный переход на применение оптического кабеля в качестве магистрального и для организации вертикальных сетей.
- регулярные проверки на наличие несанкционированных подключений к информационным линиям и коммутационному оборудованию.
- при проектировании структурированной кабельной системы необходимо закладывать некоторую избыточность для дальнейшего развития информационно-вычислительной системы Общества.
- кабельная система должна позволять расширять информационно-вычислительную систему Общества без глобальных переделок.
- кабельная система должна иметь актуальную исполнительную документацию и, в случае, каких - либо изменений и дополнений, эта документация должна корректироваться незамедлительно.
- кабельная инфраструктура Общества строится на основе структурированных кабельных систем из расчета на эксплуатацию в течение всего жизненного цикла зданий.