ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ИНТЕРТЕХЭЛЕКТРО-НОВАЯ ГЕНЕРАЦИЯ»
ОБЩЕСТВО С ОРГАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«НОЯБРЬСКАЯ ПАРОГАЗОВАЯ ЭЛЕКТРИЧЕСКАЯ СТАНЦИЯ»

УТВЕРЖДАЮ:
Генеральный директор
ООО «Интертехэлектро-Новая Генерация»
Управляющей организации
ООО «Ноябрьская ПГЭ»

_____ /С.С. Карапетян
«11» 12 2023 г.

ПОЛИТИКА
информационной безопасности в ООО «Ноябрьская ПГЭ»

г. Ноябрьск

Оглавление

1. Введение

Общество с ограниченной ответственностью «Ноябрьская парогазовая электрическая станция» (далее – Общество) является стабильно развивающимся предприятием в энергетическом секторе по производству энергетической и тепловой энергии, осознает характер и масштабы влияния своей деятельности, продукции и услуг на работников, определяет информационную безопасность одним из главных факторов эффективного управления производственной деятельностью и достижения стратегических целей.

Общество осознает, что информация, информационные технологии, программное обеспечение являются важнейшими активами, которые нуждаются в применении защитных мер для обеспечения информационной безопасности.

Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Общества и включает в себя любую деятельность, направленную на защиту информационных ресурсов и (или) поддерживающей инфраструктуры.

Защита информации представляет собой деятельность по соблюдению конфиденциальности, целостности и доступности информации путем предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи, уничтожения и иных неправомерных воздействий на защищаемую информацию.

2. Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

Бизнес-процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности организации.

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

Доступ к информации - возможность получения информации и ее использования.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность – состояние защищённости интересов организации.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационный ресурс (актив) – всё, что имеет ценность и находится в распоряжении организации.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Инцидент информационной безопасности – одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу информационной безопасности.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

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

Криптографическая защита информации - защита информации с помощью ее криптографического преобразования.

Критическая информация - информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.

Несанкционированный доступ – доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обработка информации - совокупность операций (сбор, ввод, запись, преобразование, считывание, хранение, уничтожение, регистрация), осуществляемых с помощью технических и программных средств, включая обмен по каналам передачи данных.

Политика – общие цели и указания, формально выраженные руководством организации.

Пользователь информационных ресурсов – физическое или юридическое лицо, которому предоставлен доступ к информационному ресурсу организации или обработке той или иной информации, владельцем которой является организация.

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Привилегии – права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Система управления информационной безопасности – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения,

эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

3. Общие положения

Политика информационной безопасности (далее – Политика) Общества определяет систему взглядов на проблему обеспечения информационной безопасности и стратегию ее развития.

Политика представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасности Общества.

Реализация Политики исходит из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы системы должны рассматриваться как часть единой системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий.

4. Цели информационной безопасности

Основными целями, на достижение которых направлены положения настоящей Политики, являются:

1. защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи;
2. обеспечение непрерывности и безопасности бизнес-процессов Общества;
3. сведение к минимуму величины возможного ущерба от событий, несущих угрозы безопасности информации.

5. Задачи информационной безопасности

Для достижения основных целей информационной безопасности должны быть реализованы следующие задачи:

1. обеспечение конфиденциальности информации, предотвращение ущерба за счет ее разглашения;
2. защита информации от несанкционированного доступа в бумажном и электронном документообороте;

3. предупреждение неправомерной передачи и распространения конфиденциальной информации через сеть международного информационного обмена «Интернет» и другие сети связи общего пользования;
4. обеспечение целостности, доступности и эффективного использования информационных ресурсов;
5. построение эффективной системы мониторинга и защиты всей информационной инфраструктуры Общества;
6. защита информации при передаче по каналам связи;
7. защита субъектов информационных отношений от возможного нанесения им материального, морального или иного ущерба посредством неправомерного использования касающейся их информации;
8. изучение партнёров, клиентов, конкурентов и кандидатов на работу;
9. своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности;
10. создание механизма оперативного реагирования на угрозы информационной безопасности;
11. предотвращение и (или) снижение ущерба от реализации угроз информационной безопасности;
12. обеспечение непрерывности критических бизнес-процессов Общества;
13. соответствие требованиям законодательства, методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части информационной безопасности;
14. недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями к информационным ресурсам Общества.
15. выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников Общества;
16. повышение деловой репутации и корпоративной культуры Общества.

6. Принципы реализации политики

Основными принципами реализации Политики и достижения целей информационной безопасности Общества являются:

1. вовлеченность и ответственность руководства Общества в процессе обеспечения информационной безопасности;
2. законность обеспечения информационной безопасности;
3. согласованность действий по обеспечению информационной, физической и экономической безопасности;
4. экономическая целесообразность системы защиты информации;
5. знание своих работников (подбор персонала);
6. документированность требований информационной безопасности;
7. осведомленность персонала в вопросах обеспечения информационной безопасности;
8. своевременное реагирование на инциденты информационной безопасности;

9. персональная ответственность работников по соблюдению требований информационной безопасности;
10. учет действий с информационными ресурсами (активами);
11. предоставление минимально необходимых прав доступа к информационным ресурсам Общества;
12. ежегодное планирование организационных мероприятий по обеспечению и поддержанию необходимого уровня информационной безопасности и защиты информации;
13. учет требований информационной безопасности в проектной деятельности.

7. Основания для разработки политики

Настоящая Политика разработана на основе требований законодательства Российской Федерации, накопленного в Обществе опыта в области обеспечения информационной безопасности, интересов и целей Общества.

При определении отдельных положений настоящей Политики используются действующие стандарты Российской Федерации, содержащие методы и средства обеспечения информационной безопасности и защиты информации.

8. Область действия политики

Настоящая Политика распространяется на все бизнес-процессы Общества и обязательна для применения всеми работниками и руководством Общества, а также иными пользователями его информационных ресурсов.

Требования Политики охватывают все информационные, автоматизированные системы и телекоммуникационные сети, владельцем и пользователем которых является Общество.

Каждый руководитель и работник Общества должен знать свою роль и обязанности по обеспечению информационной безопасности, обладать полномочиями по использованию информации при строгом разграничении прав доступа к информационным ресурсам Общества.

Руководители и работники Общества обязаны соблюдать (либо обеспечить соблюдение) требования по обеспечению информационной безопасности и защиты информации, правила документооборота, эксплуатации информационных систем и обработки информации на средствах вычислительной техники, порядок обращения с конфиденциальной информацией и материальными носителями ее содержащих.

Правила и порядок реализации мер и методов защиты информации и обеспечения информационной безопасности документируются в соответствии с требованиями настоящей Политики и доводятся до сведений работников под подпись, в части их касающейся.

Лица, осуществляющие разработку внутренних документов Общества, регламентирующих вопросы защиты информации и обеспечения информационной безопасности, обязаны руководствоваться настоящей Политикой.

9. Руководящие указания в части информационной безопасности

На более низком уровне Политика поддерживается правилами и требованиями, относящимися к конкретным направлениям в обеспечении информационной безопасности, которые далее предусматривают внедрение мер обеспечения необходимого

уровня информационной безопасности и структурируются для удовлетворения потребностей определенных категорий информации или для охвата определенных областей.

В целях реализации требований настоящей Политики и обеспечения безопасности объектов защиты от неправомерного доступа, уничтожения, модификации и иных действий, в соответствии с требованиями законодательства Российской Федерации, в Обществе реализуются меры и методы, определенные уполномоченными федеральными государственными органами Российской Федерации для установленной категории значимости или уровня защищенности информации (информационных систем) и иных объектов защиты.

10. Содержание политики информационной безопасности

10.1 Соблюдение требований законодательства

Все значимые требования, установленные действующим законодательством Российской Федерации, подзаконными актами и договорными отношениями, а также подход Общества к соответствию этим требованиям, должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Защищаемая информация, а также важная документация Общества, должны быть защищены от утери, уничтожения и фальсификации в соответствии с требованиями законодательства Российской Федерации.

Процесс обработки информации должен обеспечивать чёткую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Этот процесс должен иметь возможность уничтожения информации по истечении периода хранения, если эта информация больше не требуются Обществу.

Средства защиты информации должны использоваться в Обществе в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, доступности и конфиденциальности информационных ресурсов, содержащих конфиденциальную информацию.

В Обществе должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного программного обеспечения.

Криптографические средства (в случае их применения) должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

10.2 Система управления информационной безопасности

10.2.1 Общие положения

Система управления информационной безопасности Общества документирована в настоящей Политике, положениях, инструкциях, регламентах и иной внутренней документации Общества, устанавливающей правила и процедуры защиты информации и обеспечения информационной безопасности Общества.

Система управления информационной безопасности действует в Обществе для достижения целей, задач и контроля исполнения требований, определенных настоящей Политикой. Кроме того, система управления информационной безопасности направлена на:

1. исключение или существенное снижение негативных последствий (ущерба) в отношении Общества вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;
2. обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;
3. повышение защищенности Общества от возможного нанесения материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем Общества или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;
4. на обеспечение надежности, эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры Общества;
5. на обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры Общества.

10.2.2 Структура документов

В целях создания взаимосвязанной структуры внутренних документов Общества в области обеспечения информационной безопасности, разрабатываемые и обновляемые документы соответствуют следующим уровням:

Первый уровень: настоящая Политика информационной безопасности;

Второй уровень: положения и иные политики, устанавливающие общие правила к обеспечению защиты той или иной категории защищаемой информации, объектов критической информационной инфраструктуры, информационных и автоматизированных систем, технических средств, программного обеспечения и иных объектов защиты;

Третий уровень: планы мероприятий, инструкции, регламенты, порядки, перечни и иные документы, определяющие практические шаги к реализации требований внутренних документов первого и второго уровней, в соответствии с настоящей Политикой;

Четвертый уровень: документы, подтверждающие исполнение требований документов верхних уровней (отчеты, акты, журналы и др.).

Документы первого и второго уровней являются документами, регулирующие организационную и внутреннюю деятельность Общества в части защиты информации и обеспечения информационной безопасности, утверждаются и вводятся в действие Генеральным директором Общества.

Требования к выполнению тех или иных действий по защите информации и обеспечению информационной безопасности, определенные в документах третьего уровня, утверждаются и вводятся в действие исполнительным директором Общества.

Документированные требования по обеспечению информационной безопасности должны доводиться до сведений работников Общества под подпись, в части их касающейся.

10.2.3 Область действия

Система управления информационной безопасности действует в отношении всех информационных ресурсов, защищаемой информации и информационных систем для ее обработки (в т.ч. информационных систем персональных данных), автоматизированных систем и иных объектов защиты Общества (в т.ч. объектов критической информационной инфраструктуры), определенных в соответствии с настоящей Политикой и в соответствии с требованиями законодательства Российской Федерации.

Реализация требований информационной безопасности базового, уточненного и адаптированного наборов мер и методов, осуществляется на основании определенных категорий значимости объектов защиты, уровней защищенности и иных категорий защищаемой информации и объектов защиты, установленных в соответствии с требованиями законодательства Российской Федерации.

Процесс разработки и внедрения мер и методов для нейтрализации актуальных угроз информации и необходимых в соответствии с требованиями законодательства Российской Федерации, должен предусматривать документированную регламентацию правил и процедур реализации соответствующих мер.

10.2.4 Организационная инфраструктура информационной безопасности

Управление информационной безопасности в Обществе осуществляется с участием высшего руководства Общества с целью согласования и утверждения правил в соответствии с настоящей Политикой, назначения ответственных лиц в области обеспечения информационной безопасности, а также осуществления координации внедрения мероприятий по управлению информационной безопасности и контроля.

Исполнительный директор Общества является лицом, принимающим решение в отношении обеспечения информационной безопасности и защиты информации в Обществе.

Непосредственная организация эффективного функционирования системы управления информационной безопасности возложена на подразделение (лицо), ответственное за обеспечение информационной безопасности в Обществе (далее – отдел информационной безопасности), функциями которого в том числе являются:

- пересмотр Политики информационной безопасности и соответствующих обязанностей по ее выполнению;
- отслеживание существенных изменений в воздействиях основных угроз информационным активам;
- анализ и мониторинг инцидентов нарушения информационной безопасности;
- разработка основных проектов в области информационной безопасности.

Основные задачи, функции, права и обязанности отдела информационной безопасности определяются внутренними документами Общества по защите информации и обеспечению информационной безопасности, разрабатываемые в соответствии с требованиями законодательства Российской Федерации.

Для реализации требований информационной безопасности в Обществе назначаются уполномоченные лица, которые являются частью системы управление информационной безопасности, в том числе по вопросам обнаружения, реагирования и информирования об инцидентах информационной безопасности. Уполномоченные лица в специальном отношении руководствуются требованиями и методическими рекомендациями федеральных служб Российской Федерации в области обеспечения информационной безопасности.

Должностные лица, входящие в систему управления информационной безопасности Общества, контролируют в пределах своей компетенции состояние защиты

информации с целью своевременного выявления и предотвращения возникновения инцидентов информационной безопасности, в том числе с использование программных и технических средств системы защиты информации.

Должностные лица, входящие в систему управления информационной безопасности Общества, в пределах своих компетенций имеют право в установленном порядке без уведомления производить проверки выполнения действующих инструкций по вопросам обеспечения информационной безопасности.

С целью повышения эффективности выполнения поставленных задач и достижения целей, система управления информационной безопасности взаимодействует с системой управления физической и экономической безопасности Общества, а также с внешними организациями и специалистами по безопасности с целью актуализации отраслевых тенденций, способов и методов ее оценки, а также с целью адекватного реагирования на инциденты информационной безопасности.

10.3 Объекты защиты

10.3.1 Ответственность за ресурсы

В целях определения объектов защиты, в Обществе должны выявляться, классифицироваться и оцениваться, с точки зрения их важности, информационные и технические ресурсы, которые отображаются в форме соответствующих перечней или реестров, на основании и в соответствии которых реализуется система защиты информации, степень которой соразмерна ценности и важности определенных объектов защиты.

В Обществе присутствуют следующие типы информационных ресурсов, подлежащих защите:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа и распространения;
- открыто распространяемая информация, необходимая для работы Общества, независимо от формы и вида её представления;
- критическая информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, каналы информационного обмена и телекоммуникации, автоматизированные системы управления, телекоммуникационные сети, иные информационные системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Для каждого информационного ресурса должны быть назначены лица, ответственные за соответствующую их классификацию, а также за периодическую проверку соблюдения требований системы защиты информации и обеспечения информационной безопасности.

10.3.2 Классификация информации

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена исполнительным директором Общества.

Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически

классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса.

Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку.

10.4 Безопасность персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с настоящей Политикой, должны быть доведены до работника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке Политики, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

10.4.1 Условия найма

Все принимаемые на работу работники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за обеспечение информационной безопасности в Обществе. В договор должно быть включено согласие на проведение контрольных мероприятий со стороны Общества по проверке выполнения требований информационной безопасности, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения требований информационной безопасности.

Обязанности по обеспечению информационной безопасности должны быть включены в должностные инструкции каждого работника Общества.

Все принимаемые работники должны быть ознакомлены под подпись с перечнем информации, ограниченного доступа, с установленными правилами работы с ней и с мерами ответственности за нарушение этих правил.

При предоставлении работнику доступа к информационным ресурсам Общества, он должен ознакомиться под подпись с соответствующей локальной документацией, устанавливающей правила работы с данным информационным ресурсом.

10.4.2 Ответственность руководства

Руководство Общества должно требовать от всех работников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Обществе политиками и процедурами.

Уполномоченные руководством Общества работники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- выполнения действующих инструкций по вопросам обеспечения информационной безопасности;
- данных, находящихся на носителях информации;
- порядка использования информационных ресурсов;
- содержания служебной переписки.

10.4.3 Обучение информационной безопасности

Все сотрудники должны проходить периодическую подготовку в области политики и процедур информационной безопасности, принятых в Обществе.

Формирование и поддержание необходимого уровня знаний работников Общества в сфере защиты информации и обеспечения высокого уровня безопасности защищаемой информации, технических и программных средств, входящих в состав объектов

информатизации, систем обработки информации, объектов критической информационной инфраструктуры и иных информационных ресурсов Общества, реализуются в рамках системы повышения уровня осведомленности работников Общества в области информационной безопасности.

Система повышения уровня осведомленности работников Общества в области информационной безопасности включает в себя проведение инструктажей, доведение до сведений работников требований информационной безопасности, информирование о новых угрозах и уязвимостях, обучение и отработку действий при возникновении нештатной ситуации, контроль осведомленности.

Общество принимает профилактические меры по предотвращению мошеннических действий с использованием информационно-телекоммуникационных технологий. До сведений каждого работника Общества доводится информация об актуальных схемах действий мошенников для повышения их бдительности в этой области.

10.4.4 Завершение или изменения трудовых отношений

При увольнении все предоставленные работнику права доступа к информационным ресурсам должны быть заблокирован и удалены в последний рабочий день.

При изменении трудовых отношений блокируются и удаляются только те права, необходимость в которых отсутствует в новых отношениях.

10.5 Физическая безопасность

10.5.1 Защищённые области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Общества, должны быть размещены в защищённых областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, автоматические телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации.

Защищённые области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала.

Запрещается несанкционированное нахождение посторонних лиц в помещениях, в которых осуществляется обработка информации ограниченного доступа.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами, оборудованными надежными запирающими устройствами.

Помещения, в которых производится обработка информации ограниченного доступа, должны быть обеспечены средствами уничтожения документов.

10.5.2 Области общего доступа

Места доступа, через которые неавторизованные лица могут попасть в помещения Общества должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.

10.5.3 Вспомогательные службы

Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов информационных и автоматизированных систем Общества.

10.5.4 Утилизация или повторное использование оборудования

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное программное обеспечение.

Отсутствие защищаемой информации на носителях должно быть проверено уполномоченными на это лицами, о чём должна быть сделана отметка в акте списания.

10.5.5 Перемещение имущества

Оборудование, информация или программное обеспечение должны перемещаться за пределы Общества только при наличии письменного разрешения руководства.

Работники, имеющие право перемещать оборудование и носители информации за пределы Общества должны быть чётко определены.

Время перемещения оборудования за пределы Общества и время его возврата должны регистрироваться.

10.6 Контроль доступа

Требование по управлению доступом заключается в ограничении доступа к информации и средствам ее обработки. Правила управления доступом разрабатываются, документируются и периодически пересматриваются с учетом деятельности Общества и требований информационной безопасности.

Основными пользователями информационных ресурсов в Обществе являются работники структурных подразделений и отделов. Уровень полномочий каждого работника определяется индивидуально. Каждый работник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Допуск пользователей к работе с информационными ресурсами строго регламентируется. Любые изменения состава и полномочий пользователей подсистем производятся в установленном порядке, согласно регламенту предоставления доступа пользователей.

Каждому пользователю, допущенному к работе с конкретным информационным ресурсом Общества, должно быть сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать.

В случае производственной необходимости работникам могут быть сопоставлены несколько уникальных имён (учётных записей).

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизации бизнес-процесса или организации труда (например, посменное дежурство), использование общей учётной записи должно сопровождаться отметкой в журнале учёта машинного времени, которая должна однозначно идентифицировать текущего владельца учётной записи в каждый момент времени. Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением правил, установленных локальными документами по обеспечению информационной безопасности в Обществе.

10.6.1 Управление привилегиями

Доступ работника к информационным ресурсам Общества должен быть санкционирован руководителем структурного подразделения, в котором числится, согласно штатному расписанию, данный работник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий.

10.6.2 Управление и использование паролей

Пароли – средство проверки личности пользователя для доступа к сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Правила использование паролей, права и обязанности пользователей, устанавливаются локальными документами Общества.

Не допускается использование различными пользователями одних и тех же учётных данных.

Первоначальное значение пароля учетной записи пользователя устанавливает уполномоченное лицо, назначенное в соответствии с внутренним регламентом информационной безопасности. После первого входа в систему и в дальнейшем пароли выбираются пользователями самостоятельно с учетом установленных требований их сложности.

Общество оставляет за собой право осуществлять периодическую проверку стойкости паролей пользователей, используемых для доступа к информационным ресурсам.

10.6.3 Контроль прав доступа

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Общества осуществляется по мере необходимости и в процессе аудита информационной безопасности.

10.6.4 Пользовательское оборудование, оставляемое без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях информационной безопасности и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

10.6.5 Политика «чистого стола» и «чистого экрана»

Работники Общества, исполняющие свои трудовые функции с применением средств вычислительной техники, обязаны:

1. сохранять известные им пароли в тайне;
2. закрывать активные сеансы по завершении работы.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён исполнительным директором.

Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы (блокировки экрана), когда они находятся без присмотра. Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место, пользователь обязан заблокировать компьютер.

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги, а документы в электронной форме - специализированным программным обеспечением.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте, необходимо запирать все шкафы и сейфы, в которых хранятся конфиденциальные сведения.

10.6.6 Мобильное компьютерное оборудование

При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Обществу. Необходимо принять официальную политику, учитывающую риск, связанный с использованием мобильных компьютеров, и, в частности, с работой в незащищённой среде.

10.7 Допустимое использование информационных ресурсов

10.7.1 Общие обязанности пользователя

Обязанности и права пользователя определяются локальными документами Общества по информационной безопасности.

Пользователю запрещено производить несанкционированное распространение информации, которая становится доступна при подключении к корпоративной локальной вычислительной сети Общества.

10.7.2 Использование программного обеспечения

На автоматизированных рабочих местах и иных средствах вычислительной техники Общества допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

Запрещено незаконное хранение на жестких дисках Общества информации, являющейся объектом авторского права.

Решение о приобретении и установке новых технических средств, оборудования и программного обеспечения, необходимого для реализации задач принимает исполнительный директор Общества по представлению руководителя соответствующего отдела или подразделения.

Документы, подтверждающие покупку новых технических средств, оборудования и программного обеспечения, хранятся в бухгалтерии Общества в течении всего времени использования лицензии. Копии указанных документов вместе с лицензионными соглашениями, и дистрибутивами хранятся в соответствующих отделах или подразделениях.

Сведения о вновь приобретаемых средствах должны актуализироваться в соответствующих перечнях, реестрах и иных документах.

Пользователи информационных ресурсов не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на рабочих местах Общества. Указанные работы, а также работы по установке, регистрации и активации приобретённого лицензионного программного обеспечения могут быть выполнены только уполномоченными на это лицами.

10.7.3 Использование ресурсов информационных и автоматизированных систем

К работе с информационными ресурсами Общества допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

Каждому работнику Общества, которому необходим доступ к информационным ресурсам в рамках его должностных обязанностей, выдаются под роспись необходимые средства автоматизации.

Правила использования автоматизированных рабочих мест и информационных систем, а также иных объектов защиты, в том числе объектов критической информационной инфраструктуры, при выполнении своих служебных обязанностей, устанавливаются локальными документами Общества по информационной безопасности, в том числе определяющие правила обработки конфиденциальной информации, правила работы в локальной вычислительной сети, правила работы с электронной почтой и в сети «Интернет», правила работы с техническими и программными средствами.

10.7.4 Использование мобильных устройств

Под использованием мобильных устройств и носителей информации в Обществе понимается их подключение к инфраструктуре информационных систем с целью обработки, приёма или передачи информации.

На предоставленных Обществом мобильных устройствах допускается использование программного обеспечения, входящего в перечень разрешённого к использованию программного обеспечения.

К предоставленным Обществом мобильным устройствам и носителям информации предъявляются те же требования информационной безопасности, что и для стационарных автоматизированных рабочих мест.

Требования к использованию личных мобильных технических средств устанавливаются в локальных документах Общества по информационной безопасности.

10.7.5 Защита от вредоносного программного обеспечения

В целях предотвращения воздействия на информационные ресурсы вредоносным программным обеспечением, в Обществе должны применяться лицензированное антивирусное программное обеспечение и средства.

10.8 Приобретение, разработка и обслуживание систем

Приобретение новых систем, технических средств и программного обеспечения, должны в обязательном порядке согласовываться с управлением информационной безопасности Общества с целью обеспечения их соответствия установленным требованиям.

При описании требований к созданию новых систем или к модернизации существующих, учитывается потребность в средствах обеспечения безопасности.

Требования к обеспечению информационной безопасности и процессам, обеспечивающим защиту информации, включаются на ранних стадиях проектирования новый и модернизации действующих систем.

Все поступающие в Общество системы и средства, учитываются в соответствующем порядке.

Соглашения с внешними поставщиками средств и услуг должны охватывать вопросы ответственности и надёжности.

Программные и технические средства системы защиты информации и управления информационной безопасности внедряются в Обществе по результатам проведения внутреннего (или внешнего) аудита, определения угроз безопасности информации и анализа моделей нарушителей информационной безопасности.

Внедряемые средства защиты информации в системы должны иметь возможность модернизации и должны быть обеспечены гарантийной и технической поддержкой российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических или юридических лиц.

Стоимость внедряемых средств защиты информации и управления информационной безопасностью не должна превышать возможный ущерб, возникающий при реализации угроз.

10.9 Криптографические средства

Все, поступающие в Общество средства криптографической защиты информации (далее – СКЗИ) должны быть учтены в соответствии с требованиями законодательства Российской Федерации.

В Обществе должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям. Шифрование любой другой информации в Обществе должно осуществляться только после получения письменного разрешения на это.

10.9.1 Требования по обеспечению информационной безопасности при использовании СКЗИ

Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Общества и должен включать:

- порядок ввода в действие СКЗИ;
- порядок эксплуатации;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;

– порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

При использовании СКЗИ в Обществе должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

10.9.2 Электронные подписи

Электронная подпись обеспечивает защиту аутентификации и целостности электронных документов.

Электронная подпись может применяться для любой формы документа, обрабатываемого электронным способом, в том числе для доступа в информационные системы. Электронная подпись должна быть реализована при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете. Защита целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

При использовании электронной подписи, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

10.9.3 Управление ключами

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации.

Следует применять систему защиты для обеспечения использования в Обществе криптографических методов в отношении открытых ключей. Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия.

Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Секретные ключи пользователей должны храниться так же, как и пароли. О любом подозрении на компрометацию секретного ключа пользователь должен немедленно доложить об этом в отдел информационной безопасности Общества.

10.10 Управление инцидентами информационной безопасности

В Обществе должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области информационной безопасности, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

Все работники Общества должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

В дополнение к уведомлению о происшествиях информационной безопасности и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов информационной безопасности.

Цели управления инцидентами информационной безопасности должны быть согласованы с руководством для учёта приоритетов Общества при обращении с инцидентами.

Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

10.11 Управление непрерывностью и восстановлением

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности бизнес-процессов Общества. Данный процесс должен объединять в себе основные элементы поддержки непрерывности бизнес-процессов.

В Обществе должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес- процессов.

В каждом плане поддержки непрерывности бизнеса должны быть чётко указаны условия начала его исполнения и работники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы восстановления и возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

10.12 Аудит информационной безопасности

Общество должно проводить внутренние проверки системы управления информационной безопасности через запланированные интервалы времени.

Основные цели проведения таких проверок:

- оценка текущего уровня защищённости информационных ресурсов;
- выявление и локализация уязвимостей в системе защиты информационных ресурсов;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении информационных ресурсов;
- оценка соответствия системы защиты требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию системы управления информационной безопасности за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

В число задач, решаемых при проведении проверок и аудитов информационной безопасности, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре информационных систем, необходимых для оценки состояния информационной безопасности;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);

- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности информационных ресурсов;
- разбор инцидентов информационной безопасности и минимизация возможного ущерба от их проявления.

Руководство и работники Общества при проведении аудита информационной безопасности, обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

10.13 Конфиденциальность информации

Конфиденциальной информацией являются сведения о деятельности Общества, его отделов и подразделений и другая информация, обрабатываемая в Обществе, которая не имеет действительной или потенциальной коммерческой ценности, но в отношении которой Обществом предпринимаются меры по охране ее недоступности для третьих лиц.

Обществом не осуществляется обработка сведений, составляющих государственную тайну.

Обработка (в т.ч. сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача, распространение, предоставление, доступ, блокирование, удаление, уничтожение) и защита конфиденциальной информации в Обществе осуществляется с использованием средств автоматизации или без использования таких средств на материальных (бумажных, магнитных, цифровых и иных) носителях информации, с учетом требований законодательства Российской Федерации, устанавливающих правила обработки и защиты такой информации.

Хранение конфиденциальной информации должно осуществляться в местах, исключающих несанкционированный доступ третьих лиц к такой информации. Сроки хранения документов, содержащие конфиденциальную информацию, устанавливаются в соответствии с требованиями законодательства Российской Федерации.

По достижению целей обработки и сроков хранения конфиденциальной информации, такая информация, и при необходимости, ее материальные носители, должны быть уничтожена специализированными средствами, гарантирующими невозможность ее восстановления. Порядок уничтожения информации и носителей информации определяется в отдельных локальных документах Общества, разработанными в с соблюдением требованиями настоящей Политики.

Допуск лиц к сведениям и документам, содержащим конфиденциальную информацию, осуществляется с соблюдением принципа необходимой достаточности для выполнения служебных обязанностей и поставленных задач.

10.14 Взаимодействие со сторонними организациями

Обеспечение конфиденциальности информации при взаимодействии с другими организациями (контрагентами) регулируется договорными обязательствами, предусматривающими ответственность сторон за разглашение конфиденциальной информации.

Обязательства по сохранению конфиденциальной информации включаются во все заключаемые Обществом договоры и соглашения.

Предоставление доступа к информационным ресурсам для иных организаций осуществляется на основе заключаемых соглашений и договоров, в которые в обязательном порядке включаются требования по информационной безопасности.

Предоставление доступа к информационным ресурсам для государственных, силовых и иных структур осуществляется в соответствии с предъявляемыми запросами и предписаниями.

В Обществе должны быть разработаны и утверждены правила приобретения, приёмки новых информационных и автоматизированных систем, в том числе технических и программных средств, а также их модернизации и обновления, в том числе согласование с отделом информационной безопасности Общества.

11. Ответственность

Исполнительный директор Общества несет персональную ответственность за обеспечение информационной безопасности в Обществе.

Пользователи информационных ресурсов Общества несут персональную ответственность за соблюдение требований информационной безопасности, предусмотренную действующим законодательством Российской Федерации.

Нарушение требований локальных документов по обеспечению информационной безопасности является инцидентом информационной безопасности и служит поводом и основанием для проведения служебного расследования в отношении нарушителей.

Права, обязанности и ответственность работников Общества при работе с информационными ресурсами и обработке информации той или иной категории, регулируются должностными инструкциями и иной локальной документацией Общества, устанавливающей требования по информационной безопасности.

В должностные обязанности работника включаются пункты по соблюдению требований информационной безопасности в Обществе и ответственность, в соответствии с видом выполняемой работы и доступом к определенным категориям объектов защиты.

Роли и обязанности по обеспечению безопасности информационных ресурсов доводятся до работников при трудоустройстве, а работникам сторонних организаций, непосредственно перед предоставлением информации или доступа к определенным информационным ресурсам.

Должностные лица, входящие в систему управления информационной безопасности Общества, имеют право в установленном порядке без уведомления производить проверки выполнения действующих инструкций по вопросам обеспечения информационной безопасности.

В случае несоблюдения правил использования информационных ресурсов, пользователь незамедлительно отстраняется от доступа к предоставленной информации и информационным ресурсам до выяснения обстоятельств.

Все работники Общества обязаны:

- одобрить и подписать свои трудовые договоры;
- ознакомиться под подпись с должностными инструкциями;
- подписать обязательства или соглашения, определяющие дополнительные требования по соблюдению конфиденциальности информации;
- ознакомиться под подпись с внутренними документами, регламентирующими требования информационной безопасности, в части их касающейся;

12. Контроль и пересмотр

Общий контроль состояния информационной безопасности Общества осуществляется исполнительным директором Общества.

Текущий контроль соблюдения требований настоящей Политики осуществляет отдел информационной безопасности Общества. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Общества, по результатам внутреннего аудита и оценки общего состояния информационной безопасности, а также в рамках иных контрольных мероприятий.

Отдел информационной безопасности Общества при необходимости пересматривает положения настоящей Политики и иных локальных документов по информационной безопасности. Изменения и дополнения локальных документов утверждаются и вводятся в действие в соответствии с требованиями настоящей Политики.

13. Заключительные положения

Положения настоящей Политики распространяются только на деятельность Общества и не затрагивают вопросов защиты государственной тайны Российской Федерации.

Политика информационной безопасности утверждается и вводится в действие Генеральным директором Общества, вступает в силу с момента его утверждения, и действует до момента ее отмены либо замены иными локальными документами.

Политика информационной безопасности периодически пересматривается с учетом изменений законодательства Российской Федерации, международных и национальных стандартов, а также развития инфраструктуры Общества.

Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

Ознакомление с настоящей Политикой осуществляется вновь принимаемым работником при трудоустройстве в отделе кадров Общества.

Все что не урегулировано настоящей Политикой и иными локальными актами Общества в вопросах обеспечения информационной безопасности и защиты информации, регулируется в соответствии требований законодательства Российской Федерации.