

Открытое акционерное общество
«Первая генерирующая компания оптового рынка электроэнергии»
(ОАО «ОГК-1»)

**ПОЛИТИКА ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ОАО «ОГК-1»**

СОДЕРЖАНИЕ

| | |
|--|-----------|
| ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ | 3 |
| 1. ОБЩИЕ ПОЛОЖЕНИЯ | 5 |
| 2. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ | 6 |
| 3. ОБЛАСТЬ ДЕЙСТВИЯ | 6 |
| 4. РАЗГРАНИЧЕНИЕ ПОЛНОМОЧИЙ В РАМКАХ СУИБ ОАО «ОГК-1» | 7 |
| 5. РАЗВИТИЕ СУИБ | 8 |
| 6. УПРАВЛЕНИЕ РИСКАМИ ИБ | 9 |
| 7. УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА | 10 |
| 8. ОПОВЕЩЕНИЕ О НАРУШЕНИЯХ БЕЗОПАСНОСТИ | 10 |
| 9. ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ, ОБУЧЕНИЕ И ТРЕНИНГИ | 10 |
| 10. СОВЕРШЕНСТВОВАНИЕ СУИБ | 11 |
| 11. ОТВЕТСТВЕННОСТЬ | 12 |

0. Термины и определения

| Термин | Определение |
|--|---|
| Информационная безопасность (ИБ) | - Состояние защищенности ОАО «ОГК-1» (далее Общество), достигаемое за счет обеспечения конфиденциальности, целостности и доступности информационных активов и ресурсов Общества, а также аутентичности данных и неотказуемости. [ISO/IEC 17799:2005] |
| Обеспечение информационной безопасности | - Защита информации от внутренних и внешних угроз (в отношении конфиденциальности, целостности, доступности, аутентичности и неотказуемости) с целью обеспечения непрерывности бизнеса, минимизации бизнес рисков, максимизации прибыли на инвестированный капитал и получения дополнительных возможностей для бизнеса. |
| Доступность | - Свойство информации и связанных с ней активов, заключающееся в доступности и применимости для авторизованных субъектов, когда они им необходимы. [ISO/IEC 13335-1:2004] |
| Конфиденциальность | - Свойство информации и связанных с ней активов, заключающееся в их недоступности для неавторизованных лиц, субъектов или процессов. [ISO/IEC 13335-1:2004] |
| Целостность | - Свойство, заключающееся в обеспечении точности и полноты информации и методов ее обработки, а также отсутствии несанкционированных изменений информации. [ISO/IEC 13335-1:2004] |
| Аутентичность | - Подтверждение подлинности и достоверности электронных документов. |
| Неотказуемость | - Невозможность отрицания совершенных действий. |
| Актив | - Все что имеет ценность или находит полезное применение для организации, ее деловых операций и их непрерывности [BS 7799-3:2006] |
| Риск | - Комбинация вероятности события и его последствий [ISO Guide 73:2002] |
| Угроза | - Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации [ISO/IEC 13335-1:2004] |
| Уязвимость | - Слабость актива или группы активов, которая может использоваться при реализации одной или более угроз [ISO/IEC 13335-1:2004] |
| Целевая информация | - Информация, нарушения свойств (доступность, целостность, конфиденциальность, аутентичность, неотказуемость) которой, могут повлечь наступления негативных последствий для Общества. Включают в себя информацию, напечатанную или записанную на бумаге, |

пересылаемую по почте или демонстрируемую в видеозаписях, передаваемую устно, информацию, хранимую в электронном виде на серверах, web-сайтах, мобильных устройствах, магнитных и оптических носителях и т.п., а также информацию, обрабатываемую в корпоративных информационных системах и передаваемую по каналам связи.

- Информационные активы** - Информационные активы – активы, имеющие влияние на целевую информацию и ее защищенность. Все активы должны быть определены и могут включать:
- человеческие ресурсы,
 - инфраструктуру,
 - инструменты,
 - оборудование
 - средства коммуникации,
 - службы,
- любые другие активы, включая услуги по поставке и покупаемый материал.
- Общество** - ОАО «ОГК-1», а также партнеры, являющиеся пользователями или администраторами информационных систем ОАО «ОГК-1», подписавшие соответствующие соглашения и принимающие данную Политику информационной безопасности и требования СУИБ.
- СУИБ** - Система управления информационной безопасностью – это та часть общей системы управления Общества, основанной на оценке бизнес рисков, и построенная в соответствии со спецификацией, приведенной в ISO/IEC 27001:2005, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности в ОАО «ОГК-1». СУИБ включает в себя организационную структуру, политики, планы, должностные обязанности, практики, процедуры, процессы, ресурсы, механизмы контроля, а также все организационно-распорядительные документы Общества в области информационной безопасности.
- Инцидент информационной безопасности** - Одно или ряд нежелательных или непредвиденных событий, относящихся к информационной безопасности, которые имеют существенную вероятность компрометации бизнес-операций и представления собой угрозы информационной безопасности [ISO/IEC TR 18044:2004]
- Средство криптографической защиты информации** - Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности

1. Общие положения

1.1 Миссией ОАО «ОГК-1» является – создание компании, обеспечивающей максимальную доходность и сохранность вложений акционеров в долгосрочной перспективе за счет:

- прибыльной продажи электроэнергии и услуг;
- удовлетворения требований клиентов путем предоставления качественных услуг;
- надежности и экологической безопасности производства;
- эффективного управления активами и затратами;
- использование передовых технологий в производстве и управлении.

Вышеуказанное определяет усиление зависимости бизнес-процессов от надежности и защищенности информационных активов. Обеспечение безопасности информационных активов является одним из основных факторов, определяющих устойчивость ведения и развития бизнеса.

1.2 Целью настоящей Политики является определение основных положений по организации защиты информационных активов Общества от всех видов угроз (внешних и внутренних, умышленных и непреднамеренных), обеспечение непрерывности бизнеса и минимизация ущерба, наносимого бизнесу в результате инцидентов информационной безопасности, максимизация прибыли на инвестированный капитал и получение дополнительных возможностей для бизнеса.

1.3 Руководство ОАО «ОГК-1» привержено обеспечению информационной безопасности Общества для достижения основных целей Компании.

1.4 Система управления информационной безопасностью является одним из элементов системы безопасности, которая охватывает более широкий круг вопросов, начиная от охраны материальных ценностей Общества и защиты ее персонала до использования средств криптографической защиты информации и предотвращения возможной утечки информации за счет побочных электромагнитных излучений. Элементы системы безопасности Общества должны быть взаимосвязаны и согласованы.

1.5 Защита персональных данных сотрудников ОАО «ОГК-1» осуществляется в соответствии с данной политикой и «Положением о защите персональных данных работников ОАО «ОГК-1», утвержденным приказом Генерального директора от 24.08.2007 № 272.

1.6 Работа с документами, содержащими сведения, составляющие коммерческую тайну Общества, осуществляется в соответствии с данной Политикой и приказом от 03.10.2005 № 43 «О мероприятиях по защите информации, составляющей коммерческую тайну ОАО «ОГК-1».

1.7 Все сотрудники Общества должны предотвращать преднамеренные или случайные случаи несанкционированного доступа к информационным активам и системам Общества, включая сведения, составляющие коммерческую тайну

Общества, персональные данные ее сотрудников, партнеров и клиентов, а также любые другие виды информации ограниченного распространения.

1.8 Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей тогда, когда они им необходимы. Должно осуществляться своевременное обнаружение и реагирование на угрозы, которые могут повлечь недоступность информационных активов и систем.

1.9 Все сотрудники ОАО «ОГК-1» должны осуществлять предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1.10 СУИБ является механизмом, дающим возможность для совместного использования информации, осуществления электронных операций и электронной коммерции, а также уменьшения рисков информационной безопасности до приемлемого уровня.

2. Соответствие требованиям

2.1 ОАО «ОГК-1» ставит своей целью получение и поддержание сертификации по требованиям международного стандарта ISO/IEC 27001:2005.

2.2 Требования информационной безопасности должны постоянно находиться в соответствии с бизнес целями Общества.

2.3 ОАО «ОГК-1» обеспечивает выполнение контрактных обязательств в отношении информационной безопасности, включая защиту персональных данных сотрудников и клиентов Общества, коммерческой тайны внешних сторон, а также других видов информации ограниченного распространения, передаваемой на основании соглашений о конфиденциальности, заключаемых между Обществом и другими организациями или гражданами.

2.4 В Обществе должны соблюдаться действующее в Российской Федерации законодательство и нормативная база, требования международных и отраслевых стандартов в области информационной безопасности.

3. Область действия

3.1 Требования настоящей Политики распространяются на всех сотрудников ОАО «ОГК-1» (штатных, временных или работающих по контракту), информационные системы ОАО «ОГК-1», физические активы, средства телекоммуникаций и иное оборудование, используемое в ОАО «ОГК-1», информацию, обрабатываемую в информационных системах ОАО «ОГК-1».

4. Разграничение полномочий в рамках СУИБ ОАО «ОГК-1»

4.1 Система управления информационной безопасности Общества строится на основе разграничения полномочий управленческих и функциональных подразделений ОАО «ОГК-1» в данной сфере. Основными элементами организационной системы обеспечения информационной безопасности Общества являются: Совет директоров, Правление ОАО «ОГК-1», Генеральный директор, Директор по безопасности, отдел экономической и информационной безопасности, Департамент информационных технологий и руководители структурных подразделений Общества.

4.2 Совет директоров ОАО «ОГК-1» утверждает Политику информационной безопасности.

4.3 Правление ОАО «ОГК-1» определяет приоритетные направления деятельности в области обеспечения информационной безопасности, принятия стратегически важных для Общества решений по данному направлению, пересматривает Политику информационной безопасности, а также осуществляет надзор за эффективным функционированием Системы управления информационной безопасностью.

4.4 Генеральный директор Общества определяет меры по реализации Политики информационной безопасности, утверждает политики, регламенты, а также перечни сведений, подлежащих защите, формулирует допустимые уровни рисков информационной безопасности.

4.5 Директор по безопасности, с учетом определенных Правлением ОАО «ОГК-1» приоритетных направлений в области обеспечения информационной безопасности, осуществляет руководство мероприятиями по защите информации и координирует деятельность сотрудников с учетом требований информационной безопасности и мерами определенными Генеральным директором Общества.

4.6 Отдел экономической и информационной безопасности во взаимодействии с другими структурными подразделениями Общества обеспечивает выполнение административно-правовых, организационных, режимных и технических мер по соблюдению информационной безопасности, включая:

- координацию деятельности подразделений филиалов и дочерних компаниях Общества в области информационной безопасности;
- работу по выявлению и оценке потенциальных угроз, разработку предложений по их предотвращению;
- работу по минимизации ущерба от состоявшегося инцидента ИБ;
- выявление, оценку рисков информационной безопасности, реализацию утвержденных мер реагирования и предоставление информации в Департамент управления рисками не реже 1 раза в квартал.

4.7 Департамент информационных технологий во взаимодействии с отделом экономической и информационной безопасности участвует в выполнении технических мер по соблюдению информационной безопасности, координирует деятельность подразделений информационных технологий

в Филиалах и дочерних компаниях Общества в области технических мер защиты целевой информации и информационных активов.

4.8 Департамент управления рисками участвует в работе по управлению рисками информационной безопасности согласно прописанному в «Политике управления рисками ОАО «ОГК-1» функционалу.

4.9 Руководители структурных подразделений Общества обеспечивают выполнение всеми подчиненными сотрудниками установленных требований в области обеспечения информационной безопасности. Обеспечение информационной безопасности Общества непосредственно на рабочих местах возлагается на сотрудников подразделений Общества.

5. Развитие СУИБ

5.1 С целью поддержания СУИБ в постоянной пригодности, адекватности и эффективности на всех уровнях управления и согласованного принятия стратегически важных для Общества решений в области информационной безопасности не реже одного раза в год проводится специальное заседание Правления ОАО «ОГК-1» по вопросам информационной безопасности, с обязательным участием на нем руководителей всех структурных подразделений, департаментов, центров и служб исполнительного аппарата ОАО «ОГК-1», а также директоров ГРЭС и руководителей подразделений информационной безопасности и информационных технологий филиалов Общества.

5.2 Данные для анализа СУИБ на специальном заседании Правления по вопросам ИБ должны включать в себя следующую информацию:

- результаты аудитов и анализа СУИБ;
- отзывы заинтересованных сторон;
- новые методики, продукты и процедуры, которые могли бы использоваться в Обществе для повышения производительности и эффективности СУИБ;
- статус превентивных и корректирующих мер;
- уязвимости и угрозы, которые не были в достаточной степени учтены во время предыдущей оценки рисков;
- результаты измерений эффективности;
- меры, предпринятые по результатам предыдущих анализов СУИБ руководством;
- любые изменения, которые могли бы повлиять на СУИБ;
- рекомендации по совершенствованию.

5.3 Данные по результатам специального заседания Правления ОАО «ОГК-1» по вопросам ИБ должны включать в себя следующие решения и меры:

- повышение эффективности СУИБ;
- корректировка плана оценки и плана обработки рисков;
- внесение необходимых изменений в процедуры и механизмы контроля, влияющие на информационную безопасность, в ответ на внутренние или внешние события, которые могут повлиять на СУИБ, включая изменения в:
 - требованиях бизнеса,

- требованиях безопасности,
 - бизнес процессах, влияющих на существующие требования бизнеса,
 - требованиях нормативной или законодательной базы,
 - контрактных обязательствах,
 - уровнях риска и/или критериях принятия рисков
- потребности в ресурсах;
- совершенствование методов измерения эффективности механизмов контроля.

6. Управление рисками ИБ

6.1 Существующая в Обществе система управления рисками предусматривает идентификацию, оценку, разработку мер реагирования, контроль реализации мер реагирования и актуализацию информационных рисков Общества согласно общей методологии управления рисками, отраженной в «Политике по управлению рисками ОАО «ОГК-1» путем создания и сопровождения СУИБ.

6.2 Основные риски информационной безопасности связаны с нарушениями конфиденциальности, целостности и доступности информационных активов Общества, а также авторских и смежных прав.

6.3 Результаты оценки рисков, Декларация о применимости, разработка мер реагирования на риски и политика управления рисками определяют, каким образом в Обществе осуществляется управление рисками информационной безопасности.

6.4 ОАО «ОГК-1» при управлении рисками информационной безопасности использует обязательные элементы, которые включают в себя:

- выявление и классификацию рисков;
- определение критериев, в соответствии с которыми принимается решение об управлении информационными рисками – их минимизации, передаче, избегании, принятии;
- определение допустимого уровня риска;
- оценку риска, в том числе, вероятности реализации риска и ущерба от его реализации на чистый денежный поток Общества в рассматриваемом отчетном периоде (по операционным информационным рискам) и на приведенный чистый денежный поток Общества в долгосрочной перспективе (по стратегическим информационным рискам);
- ранжирование рисков по степени влияния;
- разработку мер реагирования на риски и оценку ресурсов, необходимых для реализации мер реагирования;
- определение остаточного риска – уровня риска, остающегося после реализации мер реагирования на риски, направленных на снижение вероятности или ущерба при наступлении риска.

7. Управление непрерывностью бизнеса

7.1 В Обществе должен быть разработан и поддерживаться управляемый и документированный процесс обеспечения непрерывности бизнеса, учитывающий требования информационной безопасности, и служащий для того, чтобы препятствовать прерываниям хозяйственной деятельности ОАО «ОГК-1» и защищать критические важные бизнес-процессы от влияния крупных сбоев или аварий и обеспечивать их своевременное восстановление.

7.2 Планы обеспечения непрерывности бизнеса определяют общую систему мер, ответственность, необходимые требования и условия для предотвращения прерываний критически важных бизнес-процессов, обеспечения требуемого уровня доступности информационных активов, сервисов и инфраструктуры, а также восстановления после аварии.

7.3 Последовательность действий и способы взаимодействия персонала в критической ситуации определяются разрабатываемыми в Обществе аварийными процедурами.

8. Оповещение о нарушениях безопасности

8.1 Сотрудники Общества обязаны информировать о ставших им известными фактах нарушения положений настоящей Политики и инцидентах информационной безопасности своего непосредственного руководителя, сотрудников отдела экономической и информационной безопасности или руководство Общества в соответствии с установленной в ОАО «ОГК-1» процедурой.

8.2 Отделом экономической и информационной безопасности в обязательном порядке иницируются и проводятся служебные расследования по факту нарушений и инцидентов информационной безопасности в соответствии с установленной в Обществе процедурой, и результаты расследований докладываются руководству Общества.

9. Повышение осведомленности, обучение и тренинги

9.1 При приеме на работу сотрудники Общества в обязательном порядке должны проходить инструктаж в отделе экономической и информационной безопасности в отношении существующих требований в этой области, а также подписать «Соглашение о конфиденциальности».

9.2 Все сотрудники Общества должны пройти соответствующее обучение с целью повышения осведомленности в вопросах информационной безопасности.

9.3 Отдельные сотрудники, специалисты по безопасности и технический персонал Общества должны проходить специализированное обучение и практические тренинги по информационной безопасности.

9.4 Руководство Общества, все постоянные и временные работники, подрядчики, консультанты и другие лица, охватываемые областью действия настоящей Политики, должны быть осведомлены о своей ответственности (которая определена в их должностных инструкциях или в контрактах) за обеспечение информационной безопасности, сообщении о нарушениях безопасности (в соответствии с установленной в Общества процедурой оповещения) и необходимости соблюдения требований СУИБ.

10. Совершенствование СУИБ

10.1 В ОАО «ОГК-1» должна систематически пересматриваться, совершенствоваться и повышаться эффективность СУИБ путем использования данной политики, целей безопасности, результатов аудитов внутренних и внешних, анализа отслеживаемых событий, корректирующих и превентивных мер и анализа со стороны руководства.

10.2 Внутренние аудиты информационной безопасности должны проводиться на регулярной основе не реже одного раза в два года и охватывать все филиалы ОАО «ОГК-1». Обязанности за проведение внутренних аудитов ИБ возлагается на Департамент внутреннего аудита. Если в течение указанного периода проводились внешние аудиты информационной безопасности ОАО «ОГК-1», то руководство Департамента внутреннего аудита может принять решение о переносе сроков планового аудита информационной безопасности. Порядок проведения внутренних аудитов ИБ Общества определяется на основании «Методики проведения внутренних аудитов ОАО «ОГК-1».

10.3 Внешние аудиты информационной безопасности проводятся в соответствии с требованиями заинтересованных подразделений внутри Общества, а также при необходимости таковых со стороны стратегических партнеров ОАО «ОГК-1».

10.4 Отдел экономической и информационной безопасности во взаимодействии с Департаментом информационных технологий должен предпринимать меры по устранению причин несоответствий требованиям СУИБ в целях предотвращения их повторений. Процедура по реализации корректирующих мер включает в себя:

- идентификацию несоответствий;
- определение причин несоответствий;
- оценку необходимости принятия мер по предупреждению повторения несоответствий;
- определение и реализацию необходимых корректирующих мер;
- протоколирование результатов принятых мер;
- анализ предпринятых мер.

10.5 Отдел экономической и информационной безопасности во взаимодействии с Департаментом информационных технологий должен определить меры по устранению причин потенциальных несоответствий требованиям СУИБ с целью предотвращения их возникновения. Процедура по реализации превентивных мер включает в себя:

- идентификацию потенциальных несоответствий и их причин;
- оценки необходимости принятия мер для предотвращения возникновения несоответствий;
- определение и реализация необходимых превентивных мер;
- протоколирование результатов предпринимаемых мер;
- анализ принятых превентивных мер.

Должны быть идентифицированы изменившиеся риски и требования к превентивным мерам. Приоритетность превентивных мер должна определяться на основе результатов оценки рисков.

10.6 Настоящая Политика должна пересматриваться на ежегодной основе, а также в случае любых изменений результатов оценки рисков или мер реагирования на риски.

11. Ответственность

11.1 Соблюдение правил, устанавливаемых настоящей Политикой, входит в должностные обязанности всех сотрудников Общества.

11.2 Руководители всех уровней несут ответственность за выполнение положений настоящей Политики в подконтрольных им подразделениях.

11.3 Ответственность за осуществление общего контроля выполнения правил настоящей Политики, предоставление рекомендаций по их выполнению, а также за поддержание данного документа в актуальном состоянии несет отдел экономической и информационной безопасности.

11.4 На основании ст. 192 Трудового кодекса РФ сотрудники Общества, нарушающие требования настоящей Политики, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение по соответствующим основаниям.