Публичное акционерное общество «Уралкалий»

П 13-2019

УТВЕРЖДЕНО
приказом
от 19.12.2019 № 2444
«Об утверждении и вводе в действие
Политики информационной
безопасности ПАО «Уралкалий»

ПОЛИТИКА

информационной безопасности ПАО «Уралкалий»

Издание 3

г. Березники, Пермский край

Предисловие

1. РАЗРАБОТАНО отделом методологии и управления процессами информационной безопасности дирекции по информационным технологиям ПАО «Уралкалий».

2. ВВЕДЕНО В ДЕЙСТВИЕ приказом от 19.12.2019 № 2442

Дата введения 19.12.2019

3. ВЗАМЕН Политики информационной безопасности ПАО «Уралкалий», утвержденной приказом от 17.03.2016 № 444.

Содержание

1. Область применения

1.1 Политика информационной безопасности ПАО «Уралкалий» (далее – Политика) является основополагающим документом, отражающим видение руководства Компании касательно обеспечения информационной безопасности (далее – ИБ). Политика разработана для установления целей, принципов и подходов к обеспечению информационной безопасности в группе «Уралкалий».

1.2 Политика распространяет свое действие на все организации группы «Уралкалий», и является документом, обязательным к ознакомлению и исполнению каждым работником группы «Уралкалий» и внешними сторонними организациями.

1.3 По решению каждого руководителя организации группы «Уралкалий», данная Политика информационной безопасности вводится в действие приказом по организации, либо разрабатывается и утверждается собственная Политика информационной безопасности, учитывающая специфику деятельности организации, и не вступающая в противоречие с настоящей Политикой.

1.4 Внутренние документы, детализирующие Политику, не должны вступать в противоречие с ней. В случае противоречия они приводятся в соответствие с Политикой в ходе очередной актуализации.

2. Нормативные ссылки

При разработке Политики были использованы следующие документы:

- законодательные и нормативно-правовые акты Российской Федерации в сфере информационной безопасности;
- руководящие и методические документы ФСТЭК России и ФСБ России
- серия международных стандартов ИСО/МЭК 27000;
- Кодекс корпоративной культуры ПАО «Уралкалий».

3. Термины и определения

В Политике используются следующие термины и определения:

Группа «Уралкалий» – ПАО «Уралкалий» и его дочерние общества. Состав Группы «Уралкалий» может изменяться по мере появления новых дочерних обществ ПАО «Уралкалий».

Информационная безопасность – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Информация – сведения (сообщения, данные) независимо от формы их представления.

4. Сокращения

Группа – Группа «Уралкалий»;
Компания – Публичное акционерное общество «Уралкалий»;
СУИБ – Система управления информационной безопасностью.

5. Общие положения

5.1 Информация является важным активом Компании, а мероприятия по информационной безопасности являются ключевым фактором достижения миссии и видения

Компании, составляющих основу корпоративной культуры, и сохранения ценностей Компании, утвержденных Кодексом о корпоративной культуре.

5.2 Информационная безопасность является инструментов для достижения стратегических целей Компании и минимизации рисков Компании.

5.3 В качестве методологической основы для формирования и совершенствования системы информационной безопасности в Компании использует серия международных стандартов ИСО/МЭК 27000.

5.4 Для контроля и оценки уровня зрелости процессов обеспечения и управления информационной безопасности, в качестве базовой модели выбран набор метрик, приведенных в интегрированной модели CMMI (Capability Maturity Model Integration), в соответствии с которой Компания стремится соответствовать 4 уровню зрелости.

6. Основные цели и задачи

6.1 К основным целям обеспечения информационной безопасности в Компании относятся:

1) достижение следующих стратегических целей Компании:
   - обеспечение безопасности производственного процесса;
   - поддержание существующего производства;
   - обеспечение потребностей бизнеса в сфере безопасности;
   - соответствие требованиям законодательства;
   - увеличение времени доступности оборудования;
   - своевременное и качественное предоставление и поддержка ИТ-сервисов.
2) предотвращение всевозможных негативных последствии и рисков, которые могут возникнуть при реализации внешних и внутренних угроз информационной безопасности.

6.2 Основными задачами информационной безопасности в Компании являются:

1) создание комплексной, эффективной и управляемой системы информационной безопасности, соответствующей требованиям бизнеса, российского и международного законодательства, стандартам, лучшим мировым практикам;

2) создание и непрерывное развитие системы управления информационной безопасности (СУИБ);

3) создание системы внутренних и распорядительных документов, детализирующих положения Политики и регламентирующих процессы информационной безопасности;

4) прогнозирование, выявление и противодействие угрозам и инцидентам информационной безопасности;

5) эффективное управление рисками информационной безопасности;

6) обеспечение выполнения требований законодательства и внутренних нормативных и распорядительных документов Компании;

7) постоянное повышение осведомлённости работников Группы в вопросах информационной безопасности.

7. Основные принципы

7.1 Обеспечение информационной безопасности в Компании осуществляется в соответствии со следующими принципами:

1) Бизнес-ориентированность. Информационная безопасность рассматривается как инструмент по достижению стратегических целей компании;

2) Законность. Мероприятия по информационной безопасности в отношении информации и информационных ресурсов, необходимость обеспечения безопасности которых обусловлена требованиями законодательства, должны быть реализованы в строгом

соответствии указанным требованиям;

3) Риск-ориентированность. Решение о необходимости обеспечения информационной безопасности в отношении информации и информационных ресурсов, не попадающих под требования законодательства, должно быть принято на основании оценки рисков и последствий от реализации угроз информационной безопасности в отношении указанных объектов защиты. Оценка рисков информационной безопасности должна проводиться в рамках общей системы управления рисками Компании;

4) Системность и комплексность. Достижение требуемого уровня защищенности должно быть обеспечено за счет создания комплексной системы информационной безопасности, включающую в себя все необходимые правовые, организационные и технические меры защиты информации, направленные на блокирование (нейтрализацию) всех актуальных угроз информационной безопасности.

5) Разумная достаточность. Меры защиты информации должны быть соизмеримы с требованиями законодательства и результатами оценки рисков информационной безопасности;

6) Своевременность. Меры защиты информации должны носить упреждающий характер;

7) Непрерывность. Обеспечение информационной безопасности является непрерывным процессом на всех этапах жизненного цикла объектов защиты, от создания до уничтожения;

8) Совершенствование. Система информационной безопасности должна развиваться в зависимости от появления новых угроз, обновления и развития требований законодательства и лучших мировых практик;

9) Минимизации полномочий. Предоставление доступа должно быть ограничено и управляемо в соответствии обязанностями работников;

10) Контроль и оценка. Процессы обеспечения и управления информационной безопасности должны быть подвержены регулярному внутреннему и внешнему контролю соответствия требованиям и оценке эффективности. Результаты контроля должны регулярно анализироваться;

11) Персональная ответственность. Ответственность за обеспечение безопасности информации возлагается на каждого работника в пределах его обязанностей.

8. Система ИБ

8.1 Для достижения целей Компании и реализации принципов обеспечения информационной безопасности в Компании создается Система информационной безопасности.

8.2 Система информационной безопасности состоит из:

1) СУИБ;
2) Комплекса технических средств защиты информации;
3) Отдельных подсистем информационной безопасности для каждого вида защищаемых объектов.

8.3 Внутренние и распорядительные документы Компании, регламентирующие процессы информационной безопасности на каждом из уровней системы информационной безопасности, составляют единую систему документов Компании в области информационной безопасности.

8.4 Состав и структура СУИБ (в том числе состав объектов защиты, система распределения ролей и ответственности, система документации, процессы и меры в области обеспечения информационной безопасности), а также состав подсистем информационной безопасности, определяются и регламентируются другими внутренними документами

Компания (стандарты, положения, методики, инструкции и др.), детализирующими и раскрывающими положения настоящей Политики.

9. Ответственность

9.1 Руководство Компании принимает на себя ответственность за реализацию настоящей Политики.

9.2 Руководители дирекций, подразделений, работники Компании несут ответственность за выполнение своих обязанностей по поддержанию деятельности по обеспечению и выполнению требований ИБ в соответствии с документами СУИБ, а представители третьих сторон, имеющие доступ к информационным ресурсам Компании - в соответствии с договорными обязательствами.

9.3 Ответственные подразделения Компании несут ответственность за поставленные руководством Компании цели и задачи, а также контроль выполнения требований, отраженных в внутренних нормативных документах СУИБ. Все исключения из этих требований в обязательном порядке согласовываются с ответственными подразделениями Компании.

10. Заключительные положения

10.1 Политика пересматривается в случае существенных изменений в развитии Компании, требований законодательства Российской Федерации и законодательства в местах присутствия Компании, а также других организаций группы «Уралкалий».

10.2 Политика и все изменения в ней утверждаются генеральным директором.