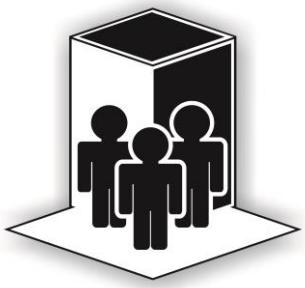

УТВЕРЖДЕНО
Приказом генерального директора
ООО МКК «Равенство»
От «01» сентября 2022г. № 33

ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ ЗАЩИТЫ КЛЮЧЕВОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ООО МКК «Равенство»

г.Сарапул

2022 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обеспечении защиты ключевой информационной инфраструктуры (далее – Положение) разработано в целях организации режима безопасности информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, в отношении которой ООО МКК «Равенство» (далее – Компания) принимает меры по защите от несанкционированного доступа третьих лиц, не имеющих право доступа к такой информации.

1.2. Положение определяет систему защиты Ключевой информационной инфраструктуры (далее – КИИ), в том числе вводит категорирование КИИ, определяет требования к субъектам КИИ, регламентирует организационные и технические меры по обеспечению безопасности КИИ, устанавливает алгоритм действий, порядок информирования Федеральной службы безопасности Российской Федерации (далее – ФСБ РФ), в случае нарушения функционирования объекта КИИ, а также определяет правила взаимодействия и оказания содействия должностным лицам ФСБ РФ в ходе расследования инцидента и ликвидации его последствий.

1.3. Защита Конфиденциальной информации осуществляется на основе принципов обеспечения безопасности КИИ: законности; непрерывности и комплексности обеспечения безопасности КИИ, достигаемые, в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов инфраструктуры; приоритета предотвращения компьютерных атак.

1.4. Деятельность Компании по обеспечению защиты КИИ не может быть использована работниками Компании для сокрытия фактов бесхозяйственности, недобросовестной конкуренции и других негативных явлений в деятельности Компании.

1.5. Настоящее Положение вступает в силу с момента его утверждения приказом руководителя Компании и действует без ограничения срока, до утверждения Положения в новой редакции.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

2.1. **Ключевая информационная инфраструктура (КИИ)** - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.

2.2. **Безопасность критической информационной инфраструктуры (БКИИ)** - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

2.3. **Категорирование объекта критической информационной инфраструктуры (КО КИИ)** – установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

2.4. **Субъект КИИ** – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, осуществляющие свою деятельность в области: здравоохранения, науки, транспорта, связи, энергетики, банковской сферы, сферы финансового рынка, топливно-энергетического комплекса, атомной энергетики, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

2.5. **Объект КИИ** – информационные системы (ИС), информационно-телекоммуникационные сети (ИТС) и автоматизированные системы управления (АСУ), имеющиеся у субъектов КИИ.

3. НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ

3.1. **Федеральный Закон** от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

3.2. **Постановление Правительства** РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

3.3. **Приказ** Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

4. ОРГАНИЗАЦИЯ РАБОТЫ ПО ЗАЩИТЕ КЛЮЧЕВОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

4.1. Защита ключевой информационной инфраструктуры осуществляется субъектом КИИ, которому на праве собственности или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в банковской сфере и иных сферах финансового рынка.

4.2. В целях обеспечения безопасности критической информационной инфраструктуры субъектами КИИ осуществляется категорирование объектов КИИ (далее – КО КИИ).

4.3. КО КИИ является процессом, включающим в себя:

- Создание комиссии;
- Утверждение перечня объектов КИИ, подлежащих категорированию;

- Проведение оценки возможных последствий компьютерных атак на объекты КИИ;
- Принятие решения о присвоении категории значимости;
- Направление решения о присвоении категории значимости в ФСТЭК России, в установленной форме.

4.4. Для проведения категорирования решением руководителя субъекта КИИ создается постоянно действующая комиссия по категорированию, в состав которой включаются:

- Руководитель субъекта КИИ или уполномоченное им лицо;
- Работники субъекта КИИ, являющиеся специалистами в области выполняемых функций в области информационных технологий и связи;
- Работники субъекта КИИ, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов КИИ;
- Работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций.

4.5. Комиссию по категорированию возглавляет руководитель субъекта КИИ или уполномоченное им лицо.

4.6. Комиссии в рамках осуществления деятельности по формированию перечня объектов КИИ, подлежащих категорированию, следует определить технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим и экологическим последствиям. В том числе провести оценку критичности их нарушения с точки зрения возможных негативных последствий.

4.7. Для формирования перечня объектов КИИ, для каждого критического процесса определяется перечень ИС, ИТС, АСУ, которые осуществляют:

- Обработку информации;
- Управление критическим процессом;
- Контроль или мониторинг критических процессов.

4.8. В случаях, когда объекты КИИ не определены и (или) отсутствуют, перечень объектов не подлежит оформлению, взамен него подлежит подготовке заключение комиссии об отсутствии объектов КИИ на основании протокола собрания комиссии по категорированию. Сведения в срок не позднее 10 (десяти) рабочих дней после утверждения руководителем Компании направляются в ФСТЭК России с приложением сопроводительного письма в произвольной форме.

4.9. В случаях, когда объекты КИИ определены, формируется перечень объектов КИИ, подлежащих категорированию. Сведения о сформированном перечне в срок не позднее 10 (десяти) рабочих дней после утверждения руководителем Компании направляются в ФСТЭК России с приложением сопроводительного письма в произвольной форме.

5. КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КЛЮЧЕВОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

5.1. Категорирование объекта КИИ выполняется постоянно действующей внутренней комиссией по категорированию, которая:

- Выявляет объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках деятельности субъекта КИИ;
- Выявляет критические процессы, нарушение или прекращение которых может привести к негативным последствиям в социальной, политической, экономической и оборонной сферах;
- Устанавливает объекты КИИ, которые обрабатывают информацию для описанных выше процессов и/или осуществляют управление, контроль или мониторинг критических процессов;
- Строит модели нарушителей и угроз, при этом комиссии следует рассматривать наихудшие сценарии атак с максимальными негативными последствиями;
- Оценивает возможные последствия, учитывая взаимосвязи между объектами и зависимости между ними;
- Присваивает каждому объекту одну из трех категорий значимости либо выносит мотивированное решение о неприсвоении такой категории, с составлением акта категорирования объекта КИИ либо акта об отсутствии необходимости присвоения ему категории значимости.

5.2. Категорирование осуществляется исходя из:

- Социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;
- Политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;
- Экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;
- Экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;
- Значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

5.3. Устанавливаются три категории значимости объектов критической информационной инфраструктуры - первая, вторая и третья.

5.4. Субъекты критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры.

5.5. Сведения о результатах присвоения объекту одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъекты направляют в письменном виде в десятидневный срок со дня принятия ими соответствующего решения в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме.

5.6. В случае, если субъектом соблюден порядок категорирования и правильно присвоена одна из категорий значимости – федеральный орган исполнительной власти вносит сведения о таком объекте в реестр значимых объектов и уведомляет об этом субъекта в десятидневный срок.

5.7. В случае, если субъектом допущена ошибка в присвоении объекту категории – федеральный орган исполнительной власти в десятидневный срок возвращает сведения в письменном виде с мотивированным обоснованием причин возврата.

5.8. Субъект информационной инфраструктуры после получения мотивированного обоснования причин возврата не более чем в десятидневный срок обязан устранить отмеченные недостатки и повторно направить такие сведения в федеральный орган исполнительной власти.

5.9. Сведения об отсутствии необходимости присвоения объекту информационной инфраструктуры одной из категорий значимости после их проверки направляются федеральным органом исполнительной власти в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о чем в десятидневный срок уведомляет субъекта ключевой информационной инфраструктуры.

6. АЛГОРИТМ ДЕЙСТВИЙ В СЛУЧАЕ НАРУШЕНИЯ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТА КЛЮЧЕВОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

6.1. Алгоритм предназначен для определения порядка действий сотрудников Компании при возникновении нештатных ситуаций информационных систем в Компании.

6.2. В случае наличия нештатной ситуации, порядок действий которой не регламентирован алгоритмом, подлежит совместному разрешению руководителем и сотрудниками Компании в индивидуальном порядке, в соответствии с учетом текущей ситуации.

6.3. Сроки и порядок оповещения должностных лиц Компании о выявлении и (или) пресечении нештатных ситуаций определены Алгоритмом, являющегося составной частью пакета документов по защите КИИ.

6.4. В целях достижения эффективной работы по предупреждению и реагированию должны проводиться регулярные тренировки по различным нештатным ситуациям, результаты которых необходимы для уточнения порядка действий.

6.5. Выявленные нештатные ситуации должны учитываться в журнале учета нештатных ситуаций либо в электронной базе данных нештатных ситуаций.

7. ПОРЯДОК ИНФОРМИРОВАНИЯ И СОДЕЙСТВИЯ ОРГАНАМ ФСБ РФ И ЦБ РФ

7.1. Субъекты критической информационной инфраструктуры Российской Федерации информируют ФСБ России обо всех компьютерных инцидентах, связанных с объектом КИИ.

7.2. Информирование осуществляется путем направления субъектом КИИ информации в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) в соответствии с определенными НКЦКИ форматами представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

7.3. Информация о компьютерном инциденте направляется субъектом КИИ в НКЦКИ незамедлительно.

7.4. Субъект КИИ осуществляет реагирование на компьютерные инциденты и принимает меры по ликвидации последствий проведенных в отношении этих объектов компьютерных атак силами лиц, которые принимают участие в обнаружении и категорировании объектов КИИ.

7.5. В целях подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом КИИ, разрабатывается алгоритм действий в случае нарушения функционирования объекта КИИ (далее – алгоритм), включающий:

- технические характеристики и состав значимых объектов КИИ;
- события (условия), при наступлении которых осуществляется ввод в действие Алгоритма;
- мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию;
- силы субъекта КИИ, ответственные за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

7.6. Субъект КИИ не реже одного раза в год организует и проводит тренировки по отработке мероприятий Алгоритма.

7.7. Субъект КИИ в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак осуществляет:

- первичный анализ компьютерных инцидентов, установление их связи с компьютерными атаками;
- проведение мероприятий в соответствии с Планом;
- определение в соответствии с Регламентом необходимости привлечения к реагированию на

компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделений и должностных лиц ФСБ России.

7.8. О результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъект КИИ в срок не позднее 48 часов после завершения мероприятий по ликвидации передает информацию о них в органы ФСБ и ЦБ РФ.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение утверждается и вводится в действие приказом руководителя и является обязательным для исполнения всеми работниками Компании.

8.2. Факт ознакомления работника с настоящим Положением возлагается на руководителя Компании.