Утверждена
Решением Правления
АО «Аналитический Центр»
Протокол от “11” февраля 2022 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АКЦИОНЕРНОГО ОБЩЕСТВА «АНАЛИТИЧЕСКИЙ ЦЕНТР»

Настоящая Политика выражает позицию Руководства Акционерного Общества «Аналитический Центр» в области информационной безопасности. Принятием настоящей Политики Руководство Общества провозглашает и обязуется осуществлять все возможные меры для защиты работников, имущества, информации, деловой репутации и бизнес-процессов Общества от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Настоящая Политика разработана с целью установления целей, задач и функций Общества, определяющих общие организационные и управленческие подходы, необходимые для обеспечения и управления информационной безопасностью Общества и защиты интересов Общества от рисков и угроз информационной безопасности.

1 Общие положения

1.1. Настоящая Политика является документом, определяющим цели, задачи и функции Общества в области обеспечения информационной безопасности в Обществе.

1.2. Общество признает, что следование требованиям информационной безопасности является одним из условий успешности бизнеса, минимизации рисков деятельности Общества, прозрачности взаимодействий с партнёрами.

1.3. Каждый работник Общества несёт ответственность за безопасную работу с вверенным ему оборудованием, данными информационных систем Общества, техническими средствами, носителями информации.

2. Цели и задачи для информационной безопасности в Обществе

2.1. Целями обеспечения защиты информации Обществе являются:

2.1.1. Минимизация рисков по ведению бизнеса;

2.1.2. Соблюдение требований действующего законодательства, затрагивающего сферы деятельности Общества и имеющихся лицензий;

2.1.3. Эффективное использование активов Общества;

2.1.4. Введение риск-ориентированного подхода внутри Общества для оценки рисков своей деятельности;

2.1.5. Использование лучших мировых практик в деятельности Общества;

2.1.6. Соблюдение баланса в защите информации и ценности информации при воздействии на деятельность Общества;

2.1.7. Соблюдение баланса в осуществлении деятельности (охвате рынка) и обеспечения безопасности информации.

3. Задачи Общества по достижению целей в области информационной безопасности

3.1. Исходя из указанных целей, Обществом определены следующие задачи по информационной безопасности:

3.1.1. Организация и обеспечение мероприятий, направленных на выполнение требований законодательства Российской Федерации по защите информации и информационной безопасности при обработке персональных данных работников и клиентов Общества;

3.1.2. Организация и обеспечение мероприятий, направленных на выполнение требований законодательства Российской Федерации по защите информации и информационной безопасности при создании и выдаче сертификатов ключа проверки электронной подписи;

3.1.3. Организация и обеспечение мер по защите коммерческой тайны Общества;

3.1.4. Организация применения в Обществе лучших практик и национальных государственных стандартов по построению системы управления информационной безопасностью;

3.1.5. Получение информации по изменениям в науке, технике, методиках и подходах защиты информации и обеспечения информационной безопасности, появлении новых видов угроз и уязвимостей;

3.1.6. Организация и обеспечение внутренней информационной безопасности Общества.

4. Функции Общества по достижению целей и задач в области информационной безопасности

4.1. Для реализации Обществом определенных настоящей Политикой целей и задач в сфере информационной безопасности Общество реализует следующие функции:

4.2. Для реализации задачи пункта 3.1.1 необходимо выполнение требований к обладателям информации и организациям различных форм собственности в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и подзаконными актами к нему;

4.3. Для реализации задачи пункта 3.1.2 необходимо выполнение требований к аккредитованным удостоверяющим центрам и доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и подзаконными актами к нему;

4.4. Для реализации задачи пункта 3.1.3 необходимо выполнение требований к обладателям информации и организациям различных форм собственности в соответствии с федеральными законами от 29.07.2004 № 98-ФЗ «О коммерческой тайне», от 27.07.2006 №

149-ФЗ «Об информации, информационных технологиях и о защите информации», национальным стандартом ГОСТ Р ИСО/МЭК 27001;

4.5. Для реализации задачи пункта 3.1.4 необходимо выполнение требований национального стандарта ГОСТ Р ИСО/МЭК 27001;

4.6. Для реализации задачи пункта 3.1.5 необходимо обеспечить политику осведомлённости и обучения работников Общества в области информационной безопасности;

4.7. Для реализации задачи пункта 3.1.6 необходимо выполнить все вышеуказанные пункты, а также рассматривать защиту информации с точки зрения риск-ориентированного подхода, определить стоимость потери информации, её ценность и исходя из этого определять необходимость её защиты, внедрять технические и организационные решения, проводить внутренние аудиты по защите информации и соблюдению работниками Общества требований, определяемых политикой информационной безопасности, проводить мероприятия по вскрытым случаям нарушения информационной безопасности, предоставлять руководству Общества предложения по недопущению таких случаев впредь, обеспечить применение взысканий для работников, нарушивших правила информационной безопасности, планировать бюджет для обеспечения защиты информации в Обществе, обеспечить качественную юридическую защиту интересов Общества в информационном пространстве.

4.8. Требования в области информационной безопасности учитываются при взаимодействии Общества с партнерами, включаются и детализируются в заключаемых Обществом договорах.

5. Ответственность за исполнение настоящей Политики

5.1. Настоящая Политика обязательная для исполнения всеми работниками Общества. За неисполнение её требований работники несут предусмотренную законодательством ответственность.

5.2. Организация мер по реализации настоящей Политики в Обществе, в том числе по разработке необходимых для её реализации локальных нормативных актов и иных документов, возлагается на отдел защиты информации удостоверяющего центра (ОЗИ УЦ).

5.3. Контроль за исполнением настоящей Политики возлагается на генерального директора Общества.

5.4. В случае возникновения вопросов, связанных с информационной безопасностью Общества, они согласуются с ОЗИ УЦ.

6. Пересмотр Политики

6.1. Внесение изменений в настоящую Политику осуществляется Правлением Общества по представлению начальника ОЗИ УЦ, согласованному с генеральном директором Общества.

6.2. Пересмотр Политики осуществляется раз в три года.

7. Конфиденциальность

7.1. Настоящая Политика размещается на официальном сайте Общества в сети Интернет.

7.2. На основании статьи 6 и 9 федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Общество оставляет за собой право на ограничение доступа к информации и перевода её в разряд конфиденциальной, её защиту методами и средствами согласно положениям действующего законодательства Российской Федерации.

7.3. В развитие настоящей Политики Общество определяет перечень и виды конфиденциальности защищаемой информации, принимает меры по её защите.
