УТВЕРЖДЕНА
решением Правления
АО «Корпорация «МСП»
« 30 » сентября 2022 г.
(протокол № 2356/22)

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АКЦИОНЕРНОГО ОБЩЕСТВА «ФЕДЕРАЛЬНАЯ КОРПОРАЦИЯ ПО РАЗВИТИЮ МАЛОГО И СРЕДНЕГО ПРЕДПРИНИМАТЕЛЬСТВА»

Москва

Содержание

1. Термины и определения

Бизнес-процесс – последовательность технологически связанных операций по предоставлению продуктов (услуг) акционерного общества «Федеральная корпорация по развитию малого и среднего предпринимательства» (далее – Корпорация) и (или) осуществлению конкретного вида обеспечивающей деятельности Корпорации.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Злоумышленник – субъект, оказывающий воздействия на информационный процесс с целью вызвать его отклонение от условий нормального протекания.

Информационная безопасность Корпорации (ИБ) – состояние защищенности информационных активов Корпорации в условиях угроз в информационной сфере.

Информационная система Корпорации – совокупность программно-аппаратных комплексов Корпорации, применяемых для обеспечения бизнес-процессов.

Информационный актив Корпорации – материальный или нематериальный объект, который:

- является информацией или содержит информацию;
- служит для обработки, хранения или передачи информации;
- имеет ценность для Корпорации.

Информационный процесс – процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

Информация, составляющая коммерческую тайну, – сведения любого характера (производственные, технические, экономические,

организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Инцидент информационной безопасности – появление одного или нескольких рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

Конфиденциальная информация (КИ) – информация, определенная в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», а также информация, предусмотренная перечнем сведений ограниченного распространения акционерного общества «Федеральная корпорация по развитию малого и среднего предпринимательства», утвержденным решением Правления Корпорации.

Модель угроз – описательное представление свойств или характеристик угроз безопасности информации.

Нарушитель информационной безопасности – лицо, которое в результате предумышленных или непредумышленных действий обеспечивает реализацию угроз информационной безопасности.

Общедоступная информация – общеизвестные сведения и иная информация, доступ к которой не ограничен законом.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы – физическое лицо, обладающее возможностью доступа к информационной системе Корпорации.

Рисковое событие информационной безопасности – событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Корпорации и произошедшее по причине ошибочности или сбоя бизнес-процессов, действий людей (информационных систем), а также по причине внешних событий.

Режим конфиденциальности информации – совокупность правовых, организационных, технических и иных принимаемых обладателем КИ мер по охране ее конфиденциальности в соответствии с законодательством Российской Федерации, включающих:

– определение перечня информации, составляющей КИ в соответствии с перечнем сведений ограниченного распространения акционерного общества «Федеральная корпорация по развитию малого и среднего предпринимательства», утвержденным решением Правления Корпорации;

– ограничение доступа к КИ путем установления порядка обращения с этой информацией в соответствии с требованиями Положения о сведениях ограниченного распространения акционерного общества «Федеральная корпорация по развитию малого и среднего предпринимательства» и контроля за соблюдением такого порядка;

– учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;

– регулирование отношений по использованию КИ работниками Корпорации на основании трудовых договоров и контрагентами Корпорации на основании договоров гражданско-правового характера и соглашений.

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

2. Общие положения

2.1. Политика информационной безопасности акционерного общества «Федеральная корпорация по развитию малого и среднего предпринимательства» (далее – Политика) является основополагающим документом, регулирующим деятельность Корпорации в области информационной безопасности.

2.2. Настоящая Политика устанавливает цели, задачи, основные подходы и принципы деятельности по обеспечению информационной безопасности Корпорации.

2.3. Настоящая Политика разработана в соответствии с требованиями следующих нормативных правовых актов Российской Федерации:

– Конституция Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Уголовный кодекс Российской Федерации;

– Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646;

– Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне»;

– Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи».

2.4. Корпорация осознает важность и необходимость принятия, развития и совершенствования правовых, организационных и технических мер обеспечения информационной безопасности. Соблюдение требований информационной безопасности позволит обеспечить информационную безопасность Корпорации, а также соответствие ее деятельности правовым, регулятивным и договорным требованиям.

2.5. Стратегия Корпорации в области обеспечения информационной безопасности и защиты информации включает выполнение в практической деятельности требований законодательства Российской Федерации в области защиты информации, составляющей государственную тайну, обеспечение безопасности персональных данных, коммерческой тайны, банковской тайны, иной конфиденциальной информации, а также общедоступной информации, предназначенной для размещения на публичных ресурсах Корпорации.

2.6. Настоящая Политика обязательна для исполнения всеми работниками Корпорации, а также пользователями ее информационных систем.

2.7. Положения настоящей Политики должны быть учтены при разработке внутренних документов Корпорации, дочерних и аффилированных организаций Корпорации, а также при заключении договоров и соглашений с контрагентами, стороной которых является Корпорация.

3. Цели и задачи деятельности по обеспечению информационной безопасности

Целями деятельности по обеспечению информационной безопасности Корпорации являются:

– защита информации, составляющей государственную тайну, информации, содержащей коммерческую тайну, банковскую тайну, персональные данные физических лиц, иной конфиденциальной информации

(сведений ограниченного распространения), а также общедоступной информации, предназначенной для размещения на публичных ресурсах Корпорации;

– обеспечение эффективности и непрерывности работы Корпорации при осуществлении ею деятельности, предусмотренной Федеральным законом от 24.07.2007 № 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации», иными нормативными правовыми актами Российской Федерации, Уставом акционерного общества «Федеральная корпорация по развитию малого и среднего предпринимательства»;

– защита информационных активов Корпорации (в том числе информационных систем Корпорации, баз данных, технических и программных средств, каналов информационного обмена, систем и средств защиты информации);

– обеспечение режима безопасности на объектах и в помещениях, в которых размещены информационные активы Корпорации;

– обеспечение соответствия деятельности Корпорации требованиям законодательства Российской Федерации в части информационной безопасности;

– снижение вероятности реализации репутационных рисков Корпорации;

– повышение корпоративной культуры Корпорации;

– стратегическое управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью Корпорации.

Основными задачами деятельности по обеспечению информационной безопасности Корпорации являются:

– выявление потенциальных угроз информационной безопасности и уязвимостей информационных ресурсов;

– предотвращение инцидентов информационной безопасности;

– исключение либо минимизация выявленных угроз информационной безопасности;

– вовлечение работников Корпорации в процесс обеспечения информационной безопасности;

– повышение осведомленности работников Корпорации в вопросах обеспечения информационной безопасности Корпорации;

– постоянное совершенствование системы менеджмента информационной безопасности.

4. Основные подходы к обеспечению информационной безопасности Корпорации

4.1. Стратегия Корпорации в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий работников Корпорации.

4.2. Угрозы информационной безопасности могут быть вызваны ошибками работников Корпорации, некорректным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение работоспособности каналов информационного обмена и т. п.) либо преднамеренными действиями злоумышленников, приводящими к нарушению конфиденциальности, целостности или доступности информационных активов Корпорации.

4.3. Корпорация придерживается процессного подхода в построении системы менеджмента информационной безопасности.

Система менеджмента информационной безопасности Корпорации основывается на осуществлении в виде непрерывного цикла следующих основных процессов, направленных на постоянное совершенствование

деятельности по обеспечению информационной безопасности Корпорации и повышение ее эффективности:

– планирование защитных мер;

– реализация и эксплуатация защитных мер;

– проверка (мониторинг и анализ) эффективности защитных мер;

– совершенствование принятых мер.

4.4. При планировании мероприятий и принятии мер по обеспечению информационной безопасности в Корпорации осуществляется:

4.4.1. Распределение ролей работников, связанных с обеспечением информационной безопасности Корпорации (ролей информационной безопасности);

4.4.2. Оценка важности информационных активов Корпорации;

4.4.3. Менеджмент рисков информационной безопасности, включающий:

– выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;

– определение моделей угроз информационной безопасности;

– выявление, анализ и оценка значимых для Корпорации угроз информационной безопасности;

– выявление возможных негативных последствий для Корпорации, наступающих в результате проявления факторов риска информационной безопасности (ущерб, угроза, уязвимость и т. д.), в том числе связанных с нарушением свойств безопасности информационных активов Корпорации;

– оценку рисков информационной безопасности;

– обработку результатов оценки рисков информационной безопасности;

– оптимизацию рисков информационной безопасности за счет выбора и применения организационных, правовых и технических защитных мер, противодействующих проявлениям факторов риска и минимизирующих

возможные негативные последствия для Корпорации в случае наступления рисковых событий;

– оценку влияния защитных мер на цели и задачи деятельности Корпорации;

– оценку затрат на реализацию защитных мер;

– рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности Корпорации;

– разработку плана управления рисками, предусматривающего защитные меры и способы их применения;

– документальное оформление целей и задач обеспечения информационной безопасности Корпорации, поддержку в актуальном состоянии внутренних документов Корпорации, регламентирующих вопросы обеспечения информационной безопасности.

4.5. В рамках реализации и эксплуатации защитных мер по обеспечению информационной безопасности в Корпорации осуществляется:

– сбор информации о событиях информационной безопасности;

– выявление и анализ инцидентов информационной безопасности;

– расследование инцидентов информационной безопасности;

– реагирование на инциденты информационной безопасности;

– минимизация негативных последствий инцидентов информационной безопасности;

– доведение до сведения руководства Корпорации информации об инцидентах и принятие решений по ним;

– контроль исполнения принятых решений по инцидентам информационной безопасности;

– пересмотр требований, мер и механизмов по обеспечению информационной безопасности по результатам расследования инцидентов информационной безопасности;

– повышение уровня осведомленности работников Корпорации в вопросах обеспечения информационной безопасности;

– регламентация и управление доступом к программным и техническим средствам и сервисам информационных систем Корпорации и информации, обрабатываемой в них;

– применение средств криптографической защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области защиты информации;

– обеспечение бесперебойности и отказоустойчивости информационных систем и каналов связи Корпорации;

– обеспечение возобновления работы информационных систем Корпорации после нештатных ситуаций;

– применение сертифицированных средств антивирусной защиты от воздействия на информационные системы Корпорации вредоносного программного обеспечения и вирусов:

– обеспечение информационной безопасности на всех стадиях жизненного цикла информационных систем Корпорации, связанных с проектированием, разработкой, приобретением, поставкой, вводом в промышленную эксплуатацию, сопровождением (сервисным обслуживанием);

– обеспечение защиты информации от утечки по техническим каналам связи;

– контроль доступа в помещения Корпорации.

4.6. В целях проверки эффективности защитных мер по обеспечению информационной безопасности в Корпорации осуществляется контроль правильности реализации и эксплуатации защитных мер, аттестация информационных систем и выделенных помещений, а также контроль

реализации и выполнения работниками Корпорации требований внутренних документов по обеспечению информационной безопасности Корпорации.

4.7. В целях совершенствования принятых мер по обеспечению информационной безопасности осуществляется уточнение (пересмотр) целей и задач обеспечения информационной безопасности Корпорации.

5. Принципы обеспечения информационной безопасности Корпорации

5.1. Принцип системности.

В Корпорации информационные активы рассматриваются как взаимосвязанные компоненты единой системы. Система защиты строится с учетом не только всех известных каналов получения несанкционированного доступа к информации, но и возможности появления новых средств реализации угроз безопасности.

5.2. Принцип полноты (комплексности)

Комплексное использование мер, методов и средств защиты информации позволяет построить целостную систему защиты и перекрывать все существующие каналы угроз информационной безопасности.

5.3. Принцип непрерывности.

Обеспечение информационной безопасности Корпорации является непрерывным целенаправленным процессом, предполагающим принятие правовых, организационных и технических мер на всех этапах жизненного цикла информационных активов Корпорации.

5.4. Принцип разумной достаточности.

На основе проведения анализа рисков Корпорацией осуществляется выбор средств защиты информационных активов, адекватных существующим угрозам.

5.5. Принцип законности.

При выборе и реализации мер и средств обеспечения информационной безопасности Корпорацией соблюдаются требования нормативных правовых

актов Российской Федерации в области обеспечения информационной безопасности, требования внутренних документов Корпорации.

5.6. Принцип управляемости.

Все процессы обеспечения информационной безопасности Корпорации должны быть управляемыми, то есть должна быть предусмотрена возможность их мониторинга, а также своевременного выявления нарушений информационной безопасности и принятия мер по их профилактике и устранению.

5.7. Принцип персональной ответственности.

Ответственность за обеспечение безопасности информационных активов возлагается на каждого работника Корпорации в пределах его полномочий.

6. Организационная основа деятельности по обеспечению информационной безопасности

6.1. В целях выполнения задач по обеспечению информационной безопасности в Корпорации определены следующие роли:

– заместитель Генерального директора, осуществляющий руководство и контроль деятельности структурного подразделения, обеспечивающего информационную безопасность в Корпорации (далее – Куратор);

– структурное подразделение, осуществляющее функции по обеспечению информационной безопасности в Корпорации (далее – Подразделение ИБ);

– структурное подразделение, осуществляющее функции по противодействию иностранным техническим разведкам и технической защите информации, составляющей государственную тайну (далее – Подразделение ПДИТР и ТЗИ);

– структурное подразделение, осуществляющее функции по обеспечению функционирования ИТ-инфраструктуры Корпорации (далее – Подразделение ИТ);

– работник Корпорации.

6.2. Основными задачами Куратора являются:

– координация выполнения работ, связанных с использованием сведений, составляющих государственную тайну;

– обеспечение информационной безопасности, а также выполнение работ по предупреждению, выявлению и пресечению фактов нарушения информационной безопасности в Корпорации.

6.3. Основными задачами Подразделения ИБ являются:

– обеспечение сохранности сведений ограниченного распространения (КИ) Корпорации;

– обеспечение информационной безопасности Корпорации, защиты автоматизированных систем, вычислительных сетей, баз данных и иных информационных ресурсов Корпорации;

– планирование, разработка и реализация мероприятий по обеспечению информационной безопасности Корпорации;

– предотвращение ущерба, который может быть нанесен Корпорации в результате несанкционированных неправомерных действий работников Корпорации и (или) третьих лиц.

6.4. Основной задачей Подразделения ПДИТР и ТЗИ является обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, от иностранных технических разведок и предотвращение ее утечки по техническим каналам.

6.5. Основными задачами Подразделения ИТ в части обеспечения информационной безопасности Корпорации являются:

– обеспечение работоспособности и доступности информационных систем Корпорации;

– соблюдение требований законодательства Российской Федерации и внутренних документов Корпорации в области информационной безопасности при осуществлении функции по обеспечению функционирования ИТ-инфраструктуры Корпорации;

– информирование Подразделения ИБ о любых нарушениях, уязвимостях, обнаруженных в информационных системах Корпорации, и попытках незаконного проникновения в них.

6.6. Основными задачами работников Корпорации в рамках участия в деятельности по обеспечению информационной безопасности Корпорации являются:

– соблюдение требований информационной безопасности, устанавливаемых нормативными правовыми актами Российской Федерации, внутренними документами Корпорации;

– выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;

– выявление и реагирование на инциденты информационной безопасности;

– информирование работников Подразделения ИБ и своего непосредственного руководителя о выявленных угрозах и рисковых событиях информационной безопасности;

– предупреждение инцидентов информационной безопасности в пределах своей компетенции;

– мониторинг информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения – в случае если работник является руководителем структурного подразделения Корпорации).

7. Ответственность за соблюдение положений Политики

Работники Корпорации, виновные в нарушении положений настоящей Политики, привлекаются к дисциплинарной, материальной, гражданско-

правовой, административной и уголовной ответственности в порядке, установленном нормативными правовыми актами Российской Федерации.

8. Контроль за соблюдением положений Политики

Общий контроль состояния информационной безопасности Корпорации осуществляет Куратор.

Текущий контроль за соблюдением положений настоящей Политики осуществляет Подразделение ИБ путем проведения мониторинга и менеджмента инцидентов информационной безопасности Корпорации по результатам оценки состояния информационной безопасности Корпорации, а также в рамках контрольных мероприятий.

9. Заключительные положения

9.1. В Корпорации утверждены внутренние документы в области информационной безопасности, дополняющие и уточняющие настоящую Политику.

9.2. При изменении законодательства Российской Федерации настоящая Политика применяется в части, не противоречащей вновь принятым законодательным и иным нормативным правовым актам Российской Федерации. В случае указанных изменений Подразделение ИБ обеспечивает внесение соответствующих изменений в настоящую Политику.

9.3. Внесение изменений в настоящую Политику может проводиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности принимаемых мер по обеспечению информационной безопасности, результатам проведения внутренних аудитов состояния информационной безопасности в Корпорации и других контрольных мероприятий.