ПРАВИТЕЛЬСТВО ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

26 января 2022 г. № 53-П

г. Салехард

О внесении изменений в постановление Правительства Ямало-Ненецкого автономного округа от 24 ноября 2011 года № 847-П

Правительство Ямало-Ненецкого автономного округа **п о с т а н о в л я е т:**

Утвердить прилагаемые изменения, которые вносятся в постановление Правительства Ямало-Ненецкого автономного округа от 24 ноября 2011 года № 847-П «О Концепции информационной безопасности исполнительных органов государственной власти Ямало-Ненецкого автономного округа».

Губернатор
Ямало-Ненецкого автономного округа Д.А. Артюхов

ПРАВИТЕЛЬСТВО ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА
АППАРАТ ГУБЕРНАТОРА ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА
Управление по работе с правовыми актами
2

УТВЕРЖДЕНЫ

постановлением Правительства
Ямало-Ненецкого автономного округа
от 26 января 2022 года № 53-П

ИЗМЕНЕНИЯ,
которые вносятся в постановление Правительства Ямало-Ненецкого автономного округа от 24 ноября 2011 года № 847-П

1. Пункт 5 признать утратившим силу.

2. В Концепции информационной безопасности исполнительных органов государственной власти Ямало-Ненецкого автономного округа, утвержденной указанным постановлением:

2.1. в разделе I:

2.1.1. абзац четырнадцатый изложить в следующей редакции:

«Правовую основу Концепции составляют Конституция Российской Федерации, Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05 декабря 2016 года № 646, Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон от 28 декабря 2010 года № 390-ФЗ «О безопасности», Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» и иные правовые акты.»;

2.1.2. абзац семнадцатый изложить в следующей редакции:

«информационные ресурсы – информация, данные, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, в которых указанные информация и данные хранятся и обрабатываются;»;

2.1.3. дополнить абзацами следующего содержания:

«инженерно-техническое сопровождение – деятельность, направленная на обеспечение устойчивого функционирования информационной системы при ее использовании;

взаимодействующая (смежная) система – система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с системой и сетью оператора информационной системы (далее – оператор) и не включена в зону его ответственности (полномочий);

компонент информационной системы – программное, программно-аппаратное или техническое средство, входящее в состав систем и сетей.»;

2.2. абзац первый раздела II изложить в следующей редакции:

«Целью построения системы информационной безопасности исполнительных органов государственной власти автономного округа является защита объектов информационной безопасности от наиболее распространенных преднамеренных и (или) непреднамеренных угроз информационной безопасности, вызванных попытками получения несанкционированного доступа или воздействия на информационные ресурсы и (или) компоненты систем и сетей со стороны антропогенных источников угроз (нарушителей безопасности информации), а также направленных на нарушение устойчивости и надежности функционирования объектов и обусловленных воздействием техногенных источников (физических явлений, материальных объектов).»;

2.3. разделы III, IV изложить в следующей редакции:

«III. Объекты информационной безопасности

К объектам информационной безопасности исполнительных органов государственной власти автономного округа относятся:

1) информационные ресурсы исполнительных органов государственной власти автономного округа, содержащие конфиденциальную информацию (служебная тайна, коммерческая тайна, персональные данные и прочая информация ограниченного распространения), а также открытую (общедоступную) информацию;

2) системы формирования, распространения и использования информационных ресурсов, включающие в себя информационные системы различного класса и назначения, базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

3) информационная инфраструктура, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации;

4) объекты критической информационной инфраструктуры исполнительных органов государственной власти автономного округа.

Информационная безопасность всех вышеуказанных объектов создает условия надежного функционирования исполнительных органов государственной власти автономного округа.

IV. Основные угрозы информационной безопасности

Угроза информационной безопасности – совокупность факторов и условий, создающих опасность для нормального функционирования информационной инфраструктуры.

Источники угроз информационной безопасности исполнительных органов государственной власти автономного округа разделяются на внешние и внутренние.

К приоритетным типам, с точки зрения нейтрализации, относятся угрозы, связанные с попытками получения нарушителями неправомерного доступа и (или) воздействий к (на) защищаемым(ые) информационным(ые) ресурсам(ы).

К основным видам таких угроз относятся:

угрозы, связанные с утечкой (нарушением конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных;

угрозы, обусловленные попытками получения несанкционированного доступа к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;

угрозы, направленные на отказ в обслуживании отдельных компонентов или систем и сетей в целом;

угрозы модификации (подмены) защищаемой информации, системных, конфигурационных, иных служебных данных;

угрозы, обусловленные попытками несанкционированного использования вычислительных ресурсов в интересах решения несвойственных задач;

угрозы, направленные на нарушение функционирования (работоспособности) средств обработки и хранения информации.

К внешним угрозам относятся:

деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных систем;

перехват и утечка информации по техническим каналам;

неконтролируемое самопроизвольное распространение компьютерных вирусов и иных вредоносных программ;

стихийные бедствия, катастрофы, пожары и аварии.

Внутренними источниками угроз являются:

невыполнение требований законодательства и несвоевременное принятие необходимых правовых актов, регламентирующих деятельность в сфере информационной безопасности;

нарушения установленных регламентов сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, создающие предпосылки к утечке либо разглашению сведений, составляющих государственную, служебную и иную тайну;

внедрение несовершенных или устаревших информационных технологий и средств информатизации;

умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала;

отказы, сбои, неисправности, несогласованности инженерно-технических, программных и системно-прикладных средств защиты информационных и телекоммуникационных систем;

использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты и контроля информации;

привлечение к работам по созданию, развитию и защите информационных систем сторонних организаций, не имеющих прав на осуществление соответствующих видов деятельности.

Приведенная выше классификация угроз носит условный характер, не является окончательной и не ранжирована по степени приоритетности. В объективной реальности угрозы, как правило, носят комбинированный характер.

Непрерывный процесс прогнозирования, выявления, идентификации, конкретизации, анализа и выработки мер по локализации угроз является неотъемлемой задачей текущей деятельности в построении системы информационной безопасности исполнительных органов государственной власти автономного округа.»;

2.4. раздел V дополнить абзацем следующего содержания:

«10) импортозамещение – деятельность, направленная на постепенное замещение иностранного программного обеспечения, телекоммуникационного оборудования и иной радиоэлектроники, используемой для построения информационной инфраструктуры органов государственной власти автономного округа, на российское с целью повышения устойчивости и надежности функционирования объектов информационной безопасности и снижения возможных негативных воздействий вследствие нарушения иностранными производителями взятых на себя обязательств на различных этапах жизненного цикла (производства, поставки, технической поддержки, предоставления обновлений).»;

2.5. разделы VII – IX изложить в следующей редакции:

«VII. Структура подразделений, обеспечивающих информационную безопасность в исполнительных органах государственной власти автономного округа

Основываясь на принципах построения системы информационной безопасности в исполнительных органах государственной власти автономного округа, определяется исполнительный орган государственной власти автономного округа, отвечающий за обеспечение информационной безопасности во всех исполнительных органах государственной власти автономного округа, который наделяется соответствующими полномочиями и обязанностями:

разработка правовых актов по информационной безопасности для исполнительных органов государственной власти автономного округа;

проведение проверочных мероприятий по информационной безопасности в исполнительных органах государственной власти автономного округа и их подведомственных учреждениях и организациях, являющихся операторами и (или) пользователями государственных информационных систем автономного округа;

выбор и (или) согласование выбранных операторами средств обеспечения информационной безопасности информационных и телекоммуникационных систем в исполнительных органах государственной власти автономного округа и их подведомственных учреждениях и организациях, являющихся операторами и (или) пользователями государственных информационных систем автономного округа;

создание и развитие системы защиты информации в региональной межведомственной телекоммуникационной сети автономного округа;

контроль за организацией и обеспечением защиты информации в региональной межведомственной телекоммуникационной сети автономного округа;

участие в разработке (доработке) подсистем защиты информации в информационных системах исполнительных органов государственной власти автономного округа;

закупка средств защиты информации с целью реализации потребностей автономного округа и дальнейшей передачи указанных средств защиты информации исполнительным органам государственной власти автономного округа и их подведомственным учреждениям и обеспечению их систем защиты информации технической поддержкой.

В каждом исполнительном органе государственной власти автономного округа создается подразделение (либо определяется сотрудник), отвечающее за информационную безопасность. Руководитель исполнительного органа государственной власти автономного округа несет ответственность за организацию работ по обеспечению информационной безопасности.

Исполнительные органы государственной власти автономного округа обязаны согласовывать требования к внедряемым в исполнительных органах государственной власти автономного округа техническим, программным и программно-техническим средствам защиты с центральным исполнительным органом государственной власти автономного округа, ответственным за проведение государственной политики и осуществление исполнительно-распорядительной деятельности в сфере защиты государственной тайны и технической защиты информации.

VIII. Модель взаимодействия участников информационной системы

Моделирование взаимодействия участников информационной системы необходимо для описания процессов информационного взаимодействия и определения зон ответственности.

Участник информационного взаимодействия – организация независимо от её организационно-правовой формы и формы собственности, осуществляющая деятельность по обеспечению функционирования информационной системы и использованию результатов ее деятельности, включая, но не ограничиваясь, получение и передачу информации, предоставление вычислительных ресурсов для обработки информации и оказание услуг по инженерно-техническому сопровождению.

В качестве участников информационного взаимодействия для каждой создаваемой и модернизируемой информационной системы должны рассматриваться следующие категории:

1) заказчик – лицо, заключившее государственный контракт на создание информационной системы.

Зона ответственности:

формирование требований к информационной системе и системе защиты информации информационной системы;

определение порядка ввода информационной системы в эксплуатацию;

контроль за реализацией требований к организации защиты информации, обрабатываемой в информационной системе;

определение перечня и состава участников информационного взаимодействия;

2) оператор – лицо, осуществляющее деятельность по эксплуатации систем и сетей, в том числе по обработке содержащейся в них информации.

Зона ответственности:

эксплуатация информационной системы, обработка информации;

наделение полномочий по автоматизированному доступу к информационным ресурсам и компонентам информационной системы;

выполнение мероприятий по защите информации, включая формирование требований к защите информации, разработку и внедрение системы защиты информации, обеспечение защиты информации в ходе эксплуатации информационной системы;

организация и контроль за выполнением и (или) самостоятельная реализация мероприятий по оценке соответствия требованиям по безопасности информации и (или) эффективности принимаемых мер защиты информации;

3) обладатель (владелец) информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Зона ответственности:

достоверность, актуальность и своевременность предоставления информации, необходимой для достижения целей функционирования информационной системы;

определение перечня и состава участников информационного взаимодействия, включая их права на получение доступа к информационным ресурсам;

поручение на обработку информации уполномоченным лицам;

определение класса защищенности информационной системы и уровня защищенности персональных данных;

определение категории значимости информационной системы, отнесённой к объекту критической информационной инфраструктуры;

4) пользователь информационной системы (внешний или внутренний) – лицо, которому разрешено выполнять действия (операции) по обработке

информации в системе или сети и использующее результаты ее функционирования.

Зона ответственности:

соблюдение правил эксплуатации компонентов информационной системы и ее системы защиты, к которым пользователю информационной системы предоставлены полномочия по доступу;

сохранение конфиденциальности информации, полученной в процессе выполнения действий (операций) по обработке информации, необходимой для выполнения должностных и (или) трудовых обязанностей и (или) выполнения поставленных задач;

5) поставщик услуг – лицо, предоставляющее оператору и (или) обладателю (владельцу) информации на основании договора (соглашения) или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации.

Зона ответственности:

обеспечивает работоспособность вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации, предоставленных для функционирования информационной системы или ее компонентов, в рамках заключенного между оператором и поставщиком услуг договора (соглашения);

проводит оценку актуальности угроз безопасности информации в отношении ресурсов, предоставляемых для функционирования информационной системы в рамках заключенного договора (соглашения);

обеспечивает реализацию всех необходимых мер защиты информации в отношении ресурсов, предоставляемых для функционирования информационной системы в рамках заключенного договора (соглашения);

6) уполномоченное лицо – лицо, обрабатывающее информацию по поручению обладателя (владельца) информации, заказчика или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации.

В части пересечения функций поставщика услуг и уполномоченного лица по предоставлению ресурсов, необходимых для функционирования информационных систем, зоны ответственности уполномоченного лица идентичны зонам ответственности поставщика услуг.

Зона ответственности:

выполнение всех необходимых мер защиты информации в соответствии с требованиями, определяемыми положениями заключенного с обладателем (владельцем) информации или оператором договора (соглашения);

соблюдение конфиденциальности информации, полученной в процессе выполнения действий (операций) по обработке информации, связанной с выполнением заключенного с обладателем (владельцем) информации или оператором договора (соглашения);

7) лица, осуществляющие инженерно-техническое сопровождение информационной системы, и (или) обеспечивающих систем, и (или)

взаимодействующих (смежных) систем и информационно-телекоммуникационных сетей.

Зона ответственности:

соблюдение конфиденциальности информации, полученной в процессе реализации своих полномочий;

соблюдение правил эксплуатации компонентов информационной системы и ее системы защиты, к которым лицу предоставлены полномочия по доступу;

оказание методической и (или) технической поддержки, а также обеспечение работоспособности компонентов информационной системы, в отношении которых лицом взяты на себя обязательства по осуществлению сопровождения на основании заключенного договора (соглашения) или иного правового документа, устанавливающего порядок и условия осуществления такой деятельности.

Участник информационного взаимодействия может одновременно быть отнесен к нескольким категориям.

Все участники информационного взаимодействия вне зависимости от категории и полномочий должны принимать меры по защите информации в соответствии с установленными требованиями.

Заказчик при разработке (доработке) информационной системы взаимодействует со структурным подразделением, отвечающим за обеспечение информационной безопасности во всех исполнительных органах государственной власти автономного округа, в том числе:

1) представляет документацию на информационную систему;

2) согласует документацию на разработку (доработку) информационной системы;

3) информирует о ходе проведения работ по обеспечению информационной безопасности информационной системы.

Для государственных информационных систем обеспечение процедуры согласования документов, устанавливающих требования к защите информации, со всеми лицами и организациями, чьи интересы или деятельность (полномочия) могут быть затронуты в процессе создания и (или) ввода в действие информационной системы, возлагается на исполнительный орган государственной власти автономного округа, чьи полномочия реализуются с применением средств автоматизации указанной информационной системы, либо исполнительный орган государственной власти автономного округа, уполномоченный на создание информационной системы в соответствии с нормативным правовым актом.

Оператор взаимодействует с участниками информационного взаимодействия и лицами (структурными подразделениями), отвечающими за обеспечение информационной безопасности во всех исполнительных органах государственной власти автономного округа, в том числе:

1) представляет документы, регламентирующие порядок и условия предоставления доступа к информационной системе или отдельным ее компонентам;

2) представляет документы, регламентирующие права пользователей на доступ к информации и допустимым условиям ее обработки, включая хранение и передачу;

3) представляет документы, регламентирующие порядок и условия подключения внешних информационных систем для организации информационного взаимодействия.

IX. Меры, методы и средства обеспечения безопасности информационных систем

Анализ технических, структурных, эксплуатационных и иных особенностей информационных систем имеет важное значение для организации и внедрения надежной системы обеспечения информационной безопасности.

При выборе и использовании комплекса методов, способов и средств защиты информации, необходимых для обеспечения безопасности информации в конкретных информационных системах, должны учитываться такие факторы, как:

наличие конфиденциальной информации (персональные данные, служебная тайна и т.д.);

условия размещения и эксплуатации технических средств;

способы обработки данных в системе;

особенности обработки и пересылки информации в электронном виде;

количество пользователей и способы организации их работы с информационной системой;

способы хранения информации;

структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах;

иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

Проблема обеспечения информационной безопасности может быть решена в результате комплексного применения всех мер защиты, включающих в себя:

правовые (законодательные);

организационные;

технические, включая меры, реализуемые с использованием шифровальных (криптографических) средств.

Правовые (законодательные) меры обеспечения безопасности информационных систем

К правовым (законодательным) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения принятых в них правил.

Правовые (законодательные) меры обеспечения безопасности информационных систем выделяют правовую область, в пределах которой допускается использовать информационные ресурсы различных субъектов информационных отношений.

Организационные меры обеспечения безопасности информационных систем

Организационные меры обеспечения безопасности информационных систем – меры организационного характера, регламентирующие процессы функционирования информационных систем, использование их ресурсов, деятельность обслуживающего персонала, а также порядок обращения пользователей информации с информационными системами таким образом, чтобы в наибольшей степени затруднить либо исключить возможность реализации угроз информационной безопасности, снизить размер потерь в случае реализации угроз.

Технические меры обеспечения безопасности информационных систем

Технические меры обеспечения безопасности информационных систем должны быть основаны на использовании единых программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

При учете всех требований и принципов обеспечения безопасности информации в информационной системе в состав системы включают следующие технические и программные средства:

идентификации пользователей;

аутентификации пользователей и информационных объектов (терминалов, программных алгоритмов, элементов баз данных и т.п.), соответствующих степени конфиденциальности информации и обрабатываемых данных;

разграничения доступа к данным;

управления информационными потоками;

информационной безопасности в линиях передачи данных, в хранилищах информации;

обеспечения и контроля целостности программных и информационных ресурсов;

регистрации и контроля обращений к информации, подлежащей защите;

реагирования на попытки реализации несанкционированного доступа;

активные и пассивные средства защиты информации, обрабатываемой техническими средствами информационных систем и циркулирующей в помещениях объекта от утечки по техническим каналам.».