ПРАВИТЕЛЬСТВО НИЖЕГОРОДСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 17 февраля 2017 года № 151-р

Об утверждении Положения по обеспечению информационной безопасности при использовании в органах исполнительной власти Нижегородской области информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц

В целях обеспечения необходимого уровня информационной безопасности на территории Нижегородской области:

1. Утвердить прилагаемое Положение по обеспечению информационной безопасности при использовании в органах исполнительной власти Нижегородской области информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц (далее - Положение).

2. Органам исполнительной власти Нижегородской области и подведомственным им организациям:

2.1. Провести до 31 марта 2017 года работы по созданию автоматизированной системы доступа к ресурсам информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") в соответствии с требованиями Положения.

2.2. Учитывать требования Положения при использовании сети "Интернет".

3. Рекомендовать органам местного самоуправления городских округов и муниципальных районов Нижегородской области и подведомственным им организациям, организациям, в уставном (складочном) капитале которых доля (вклад) Нижегородской области и (или) муниципальных образований Нижегородской области составляет 50% (пятьдесят процентов) и более, и расположенным на территории Нижегородской области:

3.1. Провести до 31 марта 2017 года работы по созданию автоматизированной системы доступа к ресурсам сети "Интернет" в соответствии с требованиями Положения.

3.2. Учитывать требования Положения при использовании сети "Интернет".

4. Контроль за исполнением настоящего распоряжения возложить на заместителя Губернатора, заместителя Председателя Правительства Нижегородской области Р.В.Антонова.

И.о.Губернатора Е.Б.Люлин

УТВЕРЖДЕНО
распоряжением Правительства
Нижегородской области
от 17 февраля 2017 года № 151-р

Положение по обеспечению информационной безопасности при использовании в органах исполнительной власти Нижегородской области информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц

(далее - Положение)

I. Общие положения

1.1. Настоящее Положение определяет условия и порядок предоставления доступа и использования в органах исполнительной власти Нижегородской области, подведомственных им организациях, организациях, в уставном (складочном) капитале которых доля (вклад) Нижегородской области составляет 50% (пятьдесят процентов) и более, и расположенных на территории Нижегородской области (далее - соответственно Органы, Подведомственные организации, Организации) информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, и позволяющих обрабатывать информацию с использованием информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), и их ресурсов, правила работы в сети "Интернет", правила подключения информационных систем, локальных сетей и средств вычислительной техники Органа (Подведомственной организации, Организации) к сети "Интернет", угрозы безопасности информации и меры обеспечения безопасности информации при использовании сети "Интернет", права, обязанности и ответственность их сотрудников (далее - пользователи) в рамках настоящего Положения.

1.2. Настоящее Положение разработано на основе:

Федерального закона от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 года № 646;

Указа Президента Российской Федерации от 22 мая 2015 года № 260 "О некоторых вопросах информационной безопасности Российской Федерации" (далее - Указ № 260);

Указа 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" (далее - Указ № 351);

Концепции информационной безопасности Нижегородской области, утвержденной постановлением Правительства Нижегородской области от 31 декабря 2015 года № 920.

1.3. В настоящем Положении применяются понятия, установленные действующим законодательством Российской Федерации в области информации, информационных технологий и защиты информации, а также следующие понятия, определения и сокращения:

"КСПД" - корпоративная сеть передачи данных, функционирующая в соответствии с постановлением Правительства Нижегородской области от 29 августа 2008 года № 365 "О корпоративной сети передачи данных" (далее - постановление № 365);

"RSNet" - российский сегмент сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации;

"АРМ" - выделенное автоматизированное рабочее место доступа к сети "Интернет", входящее в контролируемую зону Органа (Подведомственной организации, Организации) и имеющее доступ к сети "Интернет", предоставленный пользователю за счет Органа (Подведомственной организации, Организации);

"ЭПУ" - электронное переносное устройство (портативное Интернет-устройство), с которого осуществляется доступ в сеть "Интернет", предоставленный пользователю за счет Органа (Подведомственной организации, Организации);

"ресурс" - информационная система и информационный ресурс;

"локальная сеть" - локальная информационно-телекоммуникационная (вычислительная) сеть Органа (Подведомственной организации, Организации).

II. Цели использования сети "Интернет"

Основными целями использования сети "Интернет" в Органе (Подведомственной организации, Организации) являются:

1) обеспечение в соответствии с Федеральным законом от 9 февраля 2009 года № 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления", постановлением Правительства Российской Федерации от 10 июля 2013 года № 583 "Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети "Интернет" в форме открытых данных", постановлением Правительства Нижегородской области от 14 июля 2010 года № 422 "Об обеспечении доступа к информации о деятельности Губернатора Нижегородской области, Правительства Нижегородской области, органов исполнительной власти Нижегородской области" реализации функций и полномочий Органа, в том числе свободного доступа к информации о деятельности Органа с применением информационных технологий;

2) размещение Органом (Подведомственной организацией, Организацией) достоверной и своевременно обновленной информации о своей деятельности в сети "Интернет";

3) поиск и получение информации в сети "Интернет", необходимой для выполнения должностных

обязанностей пользователей;

4) осуществление закупок товаров, работ, услуг для обеспечения нужд Органа (Подведомственной организации, Организации);

5) обеспечение функционирования информационных систем Органа (Подведомственной организации, Организации), требующих для их корректной работы наличие подключения к сети "Интернет";

6) обеспечение в служебных целях доступа (взаимодействия) к сторонним информационным системам и их сервисам, работающим с использованием сети "Интернет";

7) передача (получение) информации в (из) сеть "Интернет" в рамках исполнения должностных обязанностей пользователей;

8) обеспечение информационного взаимодействия внутри Органа (Подведомственной организации, Организации) между собой и с иными организациями, в том числе посредством электронной почты.

III. Угрозы безопасности информации при использовании сети "Интернет"

3.1. Использование сети "Интернет" в Органе (Подведомственной организации, Организации) создает риски:

1) заражения ресурсов Органа (Подведомственной организации, Организации) программными вирусами;

2) несанкционированного доступа к информационно-вычислительным ресурсам и системам Органа (Подведомственной организации, Организации) (в том числе целенаправленные сетевые атаки);

3) внедрения в информационные системы Органа (Подведомственной организации, Организации) программных закладок;

4) загрузки трафика нежелательной корреспонденцией, массовыми, незапрашиваемыми рекламными сообщениями или коммерческими предложениями (спамом);

5) несанкционированной передачи информации ограниченного доступа в сеть "Интернет";

6) нарушения доступности информационно-вычислительных ресурсов Органа (Подведомственной организации, Организации);

7) нарушения целостности и достоверности открытых, и общедоступных ресурсов Органа (Подведомственной организации, Организации), размещаемых им в сети "Интернет" по требованиям действующего законодательства;

8) нарушения конфиденциальности, целостности и доступности информации ограниченного доступа, передаваемой по сети "Интернет".

3.2. Основными группами потенциальных угроз безопасности информации при использовании сети "Интернет" в Органе (Подведомственной организации, Организации), ведущими к реализации рисков, являются:

1) угрозы утечки информации по техническим каналам;

2) угрозы использования штатных средств информационных систем с целью совершения несанкционированного доступа к информации;

3) угрозы нарушения доступности информации;

4) угрозы нарушения целостности информации;

5) угрозы нарушения конфиденциальности информации;

6) угрозы недекларированных возможностей в системном и прикладном программном обеспечении;

7) угрозы, не являющиеся атаками;

8) угрозы несанкционированного доступа, создающие предпосылки для реализации такого доступа в результате нарушения процедуры авторизации и аутентификации;

9) угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

10) угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационных систем и их систем защиты;

11) угрозы ошибочных или деструктивных действий лиц;

12) угрозы программно-математических воздействий;

13) угрозы, связанные с использованием облачных услуг;

14) угрозы, связанные с использованием технологий виртуализации;

15) угрозы, связанные с нарушением правил эксплуатации машинных носителей;

16) угрозы, связанные с нарушением процедур установки и обновления программного обеспечения и оборудования;

17) угрозы физического доступа к компонентам информационных систем;

18) угрозы эксплуатации уязвимостей в системном и прикладном программном обеспечении, средствах защиты информации, аппаратных компонентах информационных систем, микропрограммном обеспечении;

19) угрозы, связанные с использованием сетевых технологий;

20) угрозы инженерной инфраструктуры;

21) угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

22) угрозы, связанные с контролем защищенности информационной системы;

23) угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

IV. Меры обеспечения безопасности информации при использовании сети "Интернет"

Основными мерами по предотвращению реализации рисков и угроз, указанных в разделе III настоящего Положения, являются:

1) создание автоматизированной системы доступа к ресурсам сети "Интернет" (далее - АСД), представляющей собой комплекс программно-технических мер, предназначенных для организации стабильного гарантированного и безопасного доступа к ресурсам сети "Интернет";

2) использование в соответствии с выявленными актуальными угрозами безопасности информации актуальных версий средств защиты информации (средств межсетевого экранирования, средств контроля и анализа данных, передаваемых по сети "Интернет", средств анализа защищенности, средств защиты от несанкционированного доступа, средств антивирусной защиты, средств криптографической защиты информации, средств детектирования (предотвращения) вторжений (атак) из сети "Интернет" и вредоносного программного обеспечения, и т.п.), прошедших сертификацию в Федеральной службе безопасности Российской Федерации (далее - ФСБ России) и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России);

3) использование центра обработки данных Правительства Нижегородской области для размещения информационных систем, требующих для их корректной работы наличие подключения к сети "Интернет";

4) запрет доступа к потенциально опасным и деструктивным Интернет-сервисам и ресурсам в сети "Интернет", Интернет-сервисам, серверное оборудование которых располагается за пределами Российской Федерации, в том числе к сетевым хранилищам и облачным технологиям, функционирующим за пределами Российской Федерации;

5) использование КСПД и RSNet;

6) учет программных и технических средств для доступа к ресурсам сети "Интернет";

7) проведение при необходимости аттестационных испытаний;

8) определение актуальных угроз и возможных нарушителей безопасности информации;

9) разработка необходимой документации по обеспечению информационной безопасности;

10) определение организационных и технических мер по обеспечению информационной безопасности;

11) контроль и анализ информации, передаваемой с использованием сети "Интернет";

12) анализ сведений о работе с ресурсами сети "Интернет";

13) проведение мероприятий по оценке защищенности доступа в сеть "Интернет".

V. Условия и порядок доступа к ресурсам сети "Интернет"

5.1. Орган (Подведомственная организация, Организация) вправе использовать для доступа к сети "Интернет" проводные и беспроводные сети. При этом установка внутренних беспроводных точек доступа и прокладка проводных линий связи на территории Органа (Подведомственной организации, Организации) должны быть согласованы с подразделением по защите государственной тайны и подразделением по технической защите информации, созданными в Органе (Подведомственной организации, Организации).

5.2. В целях получения доступа к сети "Интернет" Орган (Подведомственная организация, Организация):

1) на своем уровне создает, вводит в эксплуатацию и обеспечивает функционирование АСД, использующего для подключения к сети "Интернет" КСПД, RSNet, или самостоятельно организованный доступ (подключение), подразумевающий отдельный выделенный (изолированный) канал связи в сеть "Интернет", не связанный с КСПД и RSNet на сетевом уровне;

2) приобретает у оператора связи услуги по предоставлению доступа к сети Интернет в соответствии с Федеральным законом от 7 июля 2003 года № 126-ФЗ "О связи".

5.3. Доступ к сети "Интернет" предоставляется пользователю только в целях, указанных в разделе II настоящего Положения, исходя из принципа предоставления минимально необходимых привилегий в целях исполнения им должностных обязанностей. Иное использование ресурсов сети "Интернет", решение о котором не принято в установленном порядке, должно рассматриваться как нарушение политики информационной безопасности.

5.4. Доступ пользователя к ресурсам сети "Интернет" осуществляется с закрепленного за ним АРМ (ЭПУ), входящего в АСД. Пользователю запрещается использовать АРМ и ЭПУ, не входящие в АСД, для доступа к сети "Интернет", предоставленного ему за счет Органа (Подведомственной организации, Организации).

5.5. Администратор АСД, назначаемый из числа специалистов по технической защите информации соответствующего Органа (Подведомственной организации, Организации) (далее - Администратор АСД), обеспечивает ввод АСД в эксплуатацию и наличие эксплуатационной документации на АСД.

5.6. В эксплуатационной документации на АСД указываются следующие минимально необходимые сведения:

1) адрес (индекс, город, улица, дом, кабинет), по которому оборудована АСД;

2) наименование сети, посредством которой осуществляется подключение к сети "Интернет", и лицо

(организация), предоставляющие такую сеть;

3) задачи, решаемые с использованием ресурсов сети "Интернет";

4) режим подключения к сети "Интернет" (постоянный, в том числе круглосуточный, временный);

5) разрешенные прикладные сервисы (E-mail, FTP, Telnet, HTTP и т.п.);

6) тип подключения (коммутированный, выделенный, проводной, беспроводной и т.п.);

7) размещение АРМ (ЭПУ), количество организованных АРМ (ЭПУ) и их пользователей, состав оборудования АРМ (ЭПУ) (тип устройства, наименование (производитель, модель), заводской (серийный) номер, программное обеспечение), настройки сетевых подключений АРМ (ЭПУ) (IP-адрес АРМ (ЭПУ), имеющих доступ к сети "Интернет", DNS-сервера, используемые для разрешения внешних доменных имен, шлюз доступа), правила авторизации и аутентификации пользователей АРМ (ЭПУ), информация о применении средств централизованной авторизации и аутентификации пользователей, информация о применяемой парольной политике на АРМ (ЭПУ), ответственные за работу АРМ (ЭПУ);

8) перечень организационных и технических мер информационной безопасности, которые выполняются перед подключением АСД к сети "Интернет" и в процессе ее эксплуатации, в том числе правила контроля использования подключения к сети "Интернет", подразумевающее также логирование фактов использования ресурсов сети "Интернет";

9) применяемые в АСД средства защиты информации (наименование (производитель, модель), заводской (серийный) номер или номер лицензии, сведения о сертификате / аттестате соответствия ФСБ России / ФСТЭК России (дата выдачи и номер));

10) телекоммуникационная схема системы доступа к сети "Интернет" (точки выхода в сеть "Интернет", используемое для взаимодействия с сетью "Интернет" программное обеспечение и оборудование, правила разграничения доступа, способы взаимодействия, способ организации подключения к сети "Интернет");

11) режим осуществления контроля за работой АСД;

12) перечень сведений ограниченного доступа и конфиденциального характера, подлежащих передаче и получаемых с использованием сети "Интернет";

13) запреты и дополнительные рекомендации;

14) расходы, связанные с функционированием АСД, осуществляются в пределах выделяемых лимитов бюджетных средств.

5.7. Любое взаимодействие АСД и входящих в нее компонентов с сетью "Интернет" защищается Органом (Подведомственной организацией, Организацией) по требованиям безопасности информации с соблюдением норм действующего законодательства в сфере информации, информационных технологий, защиты информации и связи.

5.8. Предоставление (блокирование) доступа пользователю к определенным ресурсам сети "Интернет" осуществляется Органом (Подведомственной организацией, Организацией) по решению его руководителя, принимаемому по представлению Администратора АСД, которое содержит перечень ресурсов сети "Интернет", доступ к которым необходимо обеспечить или заблокировать, список пользователей и цели предоставления (блокирования) доступа.

5.9. Администратор шлюза доступа, определенный в соответствии с постановлением № 365, в рамках своей компетенции вправе принять решение о блокировке (открытии) в централизованном или индивидуальном порядке доступа пользователей к определенным ресурсам сети "Интернет", если доступ к сети "Интернет" предоставляется с использованием КСПД.

5.10. Решения Администратора шлюза доступа принимаются в соответствии с действующим законодательством, протоколами заседаний Совета Безопасности Российской Федерации, Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе (далее - Координационный Совет), межведомственного технического совета по защите информации Нижегородской области (далее - Техсовет).

5.11. Администратор шлюза доступа в рамках своей компетенции утверждает список запрещенных и разрешенных ресурсов сети "Интернет" (далее - Список), который доводится им до сведения Органов (Подведомственных организаций, Организаций), использующими КСПД для доступа к сети "Интернет".

5.12. В случае реализации или возникновения предпосылок для реализации угроз безопасности информации при работе пользователя с определенными ресурсами сети "Интернет" Администратор шлюза доступа незамедлительно принимает самостоятельное решение о блокировании указанных ресурсов, после чего уведомляет заинтересованный Орган (Подведомственную организацию, Организацию), использующих КСПД для доступа к сети "Интернет", о предпринятых мерах. При ликвидации причин блокирования Администратор шлюза доступа организовывает работу по открытию доступа.

VI. Правила подключения информационных систем к сети "Интернет"

При необходимости подключения информационных систем к сети "Интернет" Орган (Подведомственная организация, Организация):

1) как оператор информационной системы, применяемой для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой

являются государственные органы и которая содержит сведения, составляющие служебную тайну, руководствуется требованиями Указа № 351;

2) при подключении информационных систем к сети "Интернет" через RSNet соблюдает требования Указа № 260;

3) учитывает требования постановления Правительства Нижегородской области от 20 января 2015 года № 14 "Об особенностях подключения региональных государственных информационных систем общего пользования к информационно-телекоммуникационным сетям, доступ к которым не ограничен определенным кругом лиц";

4) принимает меры по защите информации в информационных системах (при их взаимодействии с сетью "Интернет") в соответствии с требованиями действующего законодательства в сфере информации, информационных технологий и защиты информации, выявляет уязвимости программного обеспечения, которые могут эксплуатироваться нарушителем удаленно, с учетом сведений об уязвимостях, содержащихся в банке данных угроз безопасности информации, сформированном ФСТЭК России, с целью устранения уязвимостей программного обеспечения, своевременно обновляет программное обеспечение межсетевых экранов и иных классов средств защиты периметра информационных систем, использует средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в ФСБ России и (или) получивших подтверждение соответствия в ФСТЭК России;

5) проводит оценку достаточности принимаемых мер по защите информации в информационных системах Органа (Подведомственной организации, Организации), имеющих подключение к сети "Интернет", проводит при необходимости корректирующие мероприятия;

6) обеспечивает наличие эксплуатационной документации на информационную систему Органа (Подведомственной организации, Организации), имеющую подключение к сети "Интернет", содержащей физическую и логическую схемы взаимодействия информационной системы с сетью "Интернет", информацию о технологии ее подключения к сети "Интернет", перечень и формат данных, обрабатываемых в информационной системе, подключенной к сети "Интернет", перечень компонентов информационной системы, имеющих подключение к сети "Интернет", цели ее подключения к сети "Интернет", меры контроля данных, передаваемых через информационную систему, подключенную к сети "Интернет".

VII. Правила подключения локальных сетей к сети "Интернет"

7.1. При необходимости подключения локальной сети, применяемой для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к сети "Интернет" владелец данной локальной сети руководствуется требованиями Указа № 351.

7.2. При подключении локальной сети к сети "Интернет" через RSNet владелец локальной сети соблюдает требования Указа № 260.

VIII. Правила подключения средств вычислительной техники к сети "Интернет"

При необходимости подключения средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к сети "Интернет" владелец данных средств вычислительной техники руководствуется требованиями Указа Президента Российской Федерации № 351.

IX. Правила использования электронной почты

Использование электронной почты в органах исполнительной власти Нижегородской области осуществляется с соблюдением требований Правил использования электронной почты в органах исполнительной власти Нижегородской области, утвержденных приказом министерства информационных технологий, связи и средств массовой информации Нижегородской области от 26 февраля 2015 года № 13-од.

X. Правила работы в сети "Интернет"

10.1. При получении пользователем доступа к сети "Интернет" с АРМ (ЭПУ) ему запрещается:

1) заходить на ресурсы сети "Интернет", компрометирующие его как пользователя;

2) использовать ресурсы сети "Интернет" и программное обеспечение для доступа в сеть "Интернет", являющиеся потенциально опасными и деструктивными, и создающие угрозу безопасности информации (ее предпосылки);

3) использовать Интернет-сервисы и ресурсы сети "Интернет", не связанные со служебной (трудовой) деятельностью пользователя;

4) использовать для передачи (обработки) информации ограниченного доступа Интернет-сервисы, Интернет-пейджеры (программы для мгновенного обмена сообщениями через сеть "Интернет" в режиме реального времени)

и файлообменники, не обеспечивающие конфиденциальность передаваемой информации и эксплуатируемые не только внутри Органа (Подведомственной организации, Организации) в незащищенном по требованиям безопасности информации режиме;

5) скачивать, устанавливать и обновлять на АРМ (ЭПУ) любое программное обеспечение;

6) подключать к АРМ (ЭПУ) иные средства вычислительной техники и автоматизированные системы, кроме указанных в эксплуатационной документации на АСД;

7) изменять состав и конфигурацию программных и технических средств АРМ (ЭПУ);

8) работать на АРМ (ЭПУ) под чужой учетной записью / не персонифицированной учетной записью;

9) использовать доступ к сети "Интернет" для совершения попыток на получение доступа к закрытым ресурсам, для распространения и тиражирования информации, направленной на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за незаконное распространение которой предусмотрена уголовная или административная ответственность;

10) использовать сетевые хранилища и облачные технологии, функционирующие за пределами Российской Федерации, для обработки и хранения данных (конфиденциальных, ограниченного доступа, служебных), защищаемых Органом (Подведомственной организацией, Организацией).

10.2. Пользователю запрещается самостоятельно создавать, устанавливать и использовать беспроводные сети доступа к сети "Интернет", взаимодействующие на физическом уровне с АРМ и ЭПУ, используемыми в АСД.

10.3. Пользователь использует только Интернет-браузеры, которые разрешены к использованию Администратором АСД.

10.4. При получении доступа к сети "Интернет" через КСПД Администратору АСД и пользователю необходимо дополнительно соблюдать Положение о КСПД, утвержденное постановлением № 365.

10.5. При получении доступа к сети "Интернет" через RSNet Администратору АСД и пользователю (каждому в своей части) необходимо:

1) руководствоваться Указом № 260, приказом ФСО России от 7 сентября 2016 года № 443 "Об утверждении Положения о сегменте информационно-телекоммуникационной сети "Интернет";

3) соблюдать положения соглашения о подключении к RSNet, заключенного с ФСО России, и регламента предоставления доступа к сети "Интернет" через RSNet, предоставленного ФСО России.

10.6. При получении доступа к сети "Интернет" через самостоятельно организованное подключение Администратору АСД необходимо:

1) защитить самостоятельно организованное подключение средством защиты, обеспечивающим контроль и фильтрацию сетевого трафика, и прошедшим в установленном законодательством Российской Федерации порядке сертификацию в ФСБ России и (или) получившим подтверждение соответствия в ФСТЭК России;

2) принять меры по разграничению доступа между сетями, взаимодействующими с сетью "Интернет" через самостоятельно организованное подключение, и имеющими подключение к КСПД и (или) RSNet, которые бы исключали возможность несанкционированного доступа потенциальных нарушителей безопасности информации и (или) проникновения вредоносного программного обеспечения в КСПД, RSNet, центр обработки данных Правительства Нижегородской области, локальную сеть, к ресурсам Органа (Подведомственной организации, Организации) и иным сторонним ресурсам.

10.7. При использовании беспроводных сетей доступа к сети "Интернет" запрещается пересечение на физическом и сетевом уровнях локальной сети и средств предоставления доступа по технологии беспроводного доступа к сети "Интернет". Администратором АСД блокируется возможность доступа к КСПД и RSNet через беспроводные сети.

10.8. При работе с информационными системами, локальными сетями, средствами вычислительной техники, в том числе АРМ (ЭПУ), имеющими подключение к сети "Интернет", Администратору АСД и пользователю необходимо руководствоваться следующей парольной политикой:

1) соблюдать парольную политику, установленную для конкретного ресурса (информационной системы, локальной сети и т.д.) его создателем (разработчиком) / администратором, если она не противоречит иным обязательным требованиям;

2) организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, и контроль за действиями пользователей при работе с паролями возлагается на Администратора АСД;

3) пароли доступа к АРМ (ЭПУ) первоначально формируются Администратором АСД, а в дальнейшем выбираются пользователями самостоятельно, но с учетом следующих требований: длина пароля должна быть не менее 8 символов; в числе символов пароля должны присутствовать прописные буквы латинского алфавита от A до Z, строчные буквы латинского алфавита от a до z, десятичные цифры (от 0 до 10), неалфавитные символы (@, #, $, &, *, % и т.п.). Исключение составляют АРМ (ЭПУ), в которых использование подобных спецсимволов недопустимо; пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd и т.п.); при смене пароля новый пароль должен отличаться от старого не менее чем двумя символами;

4) пользователь несет персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных (легкодоступных) местах;

5) в случае производственной необходимости (командировка, отпуск и т.п.), при проведении работ, требующих знания пароля пользователя, допускается раскрытие значений своего пароля Администратору АСД. По окончании производственных или проверочных работ пользователи самостоятельно производят немедленную смену значений "раскрытых" паролей;

6) в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей пользователей (в их отсутствие) допускается изменение паролей Администратором АСД. В подобных случаях пользователи, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей создать их новые значения;

7) полная плановая смена паролей пользователей должна проводиться в срок не позднее 90 дней после установления предыдущего пароля. Плановая смена должна предусматривать информирование пользователя о необходимости сменить пароль и возможность смены пароля без обращения к Администратору АСД;

8) внеплановая смена личного пароля или удаление учетной записи пользователя АРМ (ЭПУ) или информационной системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться Администратором АСД в течение 1 рабочего дня после окончания последнего сеанса работы данного пользователя с АРМ (ЭПУ) или информационной системой;

9) внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое подразделение внутри Органа (Подведомственной организации, Организации) и другие обстоятельства) Администратора АСД и других пользователей, которым по роду работы были предоставлены полномочия по управлению парольной защитой (политикой);

10) в случае длительного отсутствия пользователя АРМ (ЭПУ) (командировка, болезнь и т.п.) его учетная запись блокируется и, в случае необходимости, изменяются права доступа других пользователей в отношении ресурсов данного пользователя;

11) в случае компрометации личного пароля пользователя АРМ (ЭПУ) либо подозрении на компрометацию должны быть немедленно предприняты меры по внеплановой смене личного пароля самим пользователем с немедленным информированием Администратора АСД;

12) смена забытого пользовательского пароля производится Администратором АСД на основании сообщения пользователя с обязательной установкой параметра "Требовать смену пароля при следующем входе в систему";

13) для предотвращения угадывания паролей Администратор АСД обязан настроить механизм блокировки учетной записи на 20 минут при пятикратном неправильном вводе пароля;

14) при возникновении вопросов, связанных с использованием доменных учетных записей, пользователь АРМ (ЭПУ) обязан обратиться к Администратору АСД;

15) для предоставления временного доступа (для лиц, не являющихся сотрудниками Органа (Подведомственной организации, Организации), для пользователей, которым необходимо получить временный доступ) необходимо использовать процедуру временных учетных записей. Временная учетная запись - учетная запись, имеющая ограничение по времени действия, имеющая ограниченные права по доступу. Для временных учетных записей проводится учет их использования. Временная учетная запись создается Администратором АСД. Пользователь, получивший временную учетную запись, информируется об ограничениях, связанных с ее использованием.

XI. Размещение (публикация) в сети "Интернет" информации

11.1. Пользователь размещает (публикует) в сети "Интернет" информацию, не запрещенную к размещению (публикации) действующим законодательством.

11.2. Размещение (публикация) в сети "Интернет" информации Органов (Подведомственных организаций, Организаций) через RSNet осуществляется с соблюдением требований Указа № 260.

XII. Контроль работы пользователей с сетью "Интернет"

12.1. Для контроля работы пользователей с ресурсами сети "Интернет" проводятся организационные и технические мероприятия, в том числе применяются средства контроля доступа пользователей к ресурсам (сайтам) сети "Интернет" (далее - СКД).

12.2. Функционирование СКД должно осуществляться в соответствии со следующей политикой информационной безопасности:

1) для распределения политик доступа различных категорий пользователей либо отделов (структурных подразделений) к определенным ресурсам сети "Интернет" в АСД следует создавать соответствующие группы в настройках СКД;

2) за использование учетной записи кем-либо, кроме пользователя, которому она была присвоена и выдана, пользователь несет персональную ответственность;

3) пользователь несет персональную ответственность за сохранность в тайне своего персонального пароля. Сохранение пароля пользователя в Интернет-браузере (программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой), фиксация пароля

на общедоступных носителях информации (стикерах, записках, в текстовых файлах и т.д.), а также разглашение пароля неуполномоченным третьим лицам запрещены;

4) разрешается использовать лишь те ресурсы (сайты) сети "Интернет", которые необходимы для выполнения должностных обязанностей.

12.3. По мере накопления статистических данных об использовании ресурсов сети "Интернет" политика безопасности СКД может быть дополнена Администратором АСД.

XIII. Права, обязанности и ответственность

13.1. Администратор АСД:

1) обеспечивает функционирование и осуществляет контроль эксплуатации АСД с привлечением при необходимости локального администратора своего Органа (Подведомственной организации, Организации);

2) блокирует при помощи СКД доступ пользователей Органа (Подведомственной организации, Организации) к ресурсам сети "Интернет", используемым пользователем не в целях, указанных в разделе II настоящего Положения, и к ресурсам сети "Интернет" из Списка;

3) проводит инструктаж пользователей Органа (Подведомственной организации, Организации) по безопасному использованию сети "Интернет", доводит до сведения пользователей информацию о функционировании АСД своего Органа (Подведомственной организации, Организации), не разглашая конфиденциальные (служебные) данные, доступ к которым должен быть только у Администратора АСД в целях безопасности;

4) обеспечивает в рамках своей компетенции безопасный доступ своего Органа (Подведомственной организации, Организации) к ресурсам сети "Интернет";

5) в ходе создания (модернизации) и эксплуатации АСД осуществляет определение актуальных угроз и нарушителя безопасности информации, определение и реализацию на их основе предупреждающих (корректирующих) организационных и технических мер, а также мер, указанных в разделе IV настоящего Положения;

6) принимает меры по недопущению подключения к потенциально опасным и деструктивным Интернет-сервисам и ресурсам в сети "Интернет", Интернет-сервисам, серверное оборудование которых располагается за пределами Российской Федерации, в том числе к сетевым хранилищам и облачным технологиям, функционирующим за пределами Российской Федерации;

7) устанавливает, обновляет и настраивает для работы пользователей Интернет-браузеры, в том числе российские Интернет-браузеры, поддерживающие установку защищенных соединений как с односторонней, так и с двухсторонней аутентификацией, с использованием российских криптографических алгоритмов, имеющие в составе сервисные функции, предназначенные для предотвращения атак на пользователя Интернет-браузера, организованных с помощью фишинга, вредоносных (мошеннических) сайтов и перехвата личных данных, а также автоматически проверяющие загружаемые файлы с помощью антивирусных технологий, за исключением случаев, когда выполнение должностных обязанностей пользователя с использованием российского Интернет-браузера невозможно;

8) осуществляет управление обновлениями вирусных баз антивирусного программного обеспечения: устанавливает автоматический режим ежедневного обновления вирусных баз на всех АРМ (ЭПУ), имеющих подключение к сети "Интернет", на серверном оборудовании, на котором размещаются информационные системы, имеющих доступ к сети "Интернет", а также на сервере электронной почты; осуществляет проверку фактической установки обновлений вирусных баз ежедневно и устраняет ошибки их установки;

9) принимает меры по созданию резервных копий важной служебной информации, которая обрабатывается пользователями на АРМ (ЭПУ), имеющих подключение к сети "Интернет", а также в информационной системе, имеющей доступ к сети "Интернет", с установленной им периодичностью, но не реже одного раза в месяц;

10) реагирует на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения посредством сети "Интернет";

11) в целях защиты общедоступной информации, размещаемой в сети "Интернет", использует средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в ФСБ России и (или) получившие подтверждение соответствия в ФСТЭК России;

12) при необходимости может устанавливать дополнительные правила работы в сети "Интернет" для пользователей своего Органа (Подведомственной организации, Организации), не противоречащие требованиям действующего законодательства.

13.2. Пользователь несет персональную ответственность за несоблюдение запретов и ограничений, установленных настоящим Положением.