

АДМИНИСТРАЦИЯ

ПРОВИДЕНСКОГО ГОРОДСКОГО ОКРУГА

**ПОСТАНОВЛЕНИЕ**

|  |  |  |
| --- | --- | --- |
| от 16 августа 2016 г. | № 210 | п. Провидения |

|  |
| --- |
| Об утверждении муниципальной программы  «Защита информации администрации Провиденского городского округа город  на 2017-2018 годы» |

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.10.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказами Федеральной службы по техническому и экспортному контролю от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Руководствуясь Уставом Провиденского городского округа, администрация Провиденского городского округа

**ПОСТАНОВЛЯЕТ:**

1. Утвердить муниципальной программы  «Защита информации администрации Провиденского городского округа на 2017-2018 годы», согласно Приложению к настоящему постановлению.
2. Настоящее постановление вступает в силу с 01 января 2017 года.
3. Обнародовать настоящее постановление на официальном сайте администрации Провиденского городского округа.
4. Контроль за исполнением настоящего постановления возложить на Организационно-правовое управление (Рекун Д.В.).

Глава администрации С.А. Шестопалов

Приложение к постановлению администрации Провиденского городского округа от 16.08.2016 г.

№ 210

**Муниципальная программа**

**«Защита информации администрации Провиденского городского округа**

**на 2017-2018 годы»**

I.Паспорт программы

|  |  |
| --- | --- |
| Наименование муниципальной программы | Муниципальная программа «Защита информации органов местного самоуправления Провиденского городского округа на 2016-2017 годы» (далее – Программа) |
| Дата и номер муниципального правового акта об утверждении муниципальной программы | Постановление администрации Провиденского городского округа от 146.08.2016 г. № 210 «Об утверждении муниципальной программы  «Защита информации администрации Провиденского городского округа город  на 2017-2018 годы» |
| Разработчики программы | Организационно-правовое управление |
| Исполнители программы | Администрация Провиденского городского округа |
| Координатор программы | Организационно-правовое управление |
| Цели программы | Предотвращение, или существенное снижение ущерба органам местного самоуправления от утечки информации по техническим каналам и несанкционированного доступа к ней, преднамеренного воздействия на информацию с целью её разрушения, уничтожения, модификации или блокирования.  Обеспечение условий, способствующих реализации государственной политики в сфере информационной безопасности на территории автономного округа. |
| Задачи программы | 1. Организация обеспечения безопасности информации ограниченного доступа не содержащей государственной тайны.  2. Техническая защита персональных данных.  3. Подготовка кадров по вопросам защиты информации.  4. Проведение в соответствие с требованиями защиты информации объекта информатизации (каб. 19 каб. 14). |
| Перечень подпрограмм муниципальной программы и основных мероприятий | Мероприятия указаны в приложении 1 к настоящей программе |
| Нормативные документы, на основании которых принята программа | Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01.10.2012 №1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,  Постановление Правительства Российской Федерации от 21.12.2012 №211 «Об утверждении перечня мер, направленных на обеспечения выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановление Правительства Чукотского автономного округа от 03.08.2015 г. № 427 «О порядке создания, функционирования и требований к защите информации государственных информационных систем, Распоряжение главы администрации Провиденского муниципального района от 03.08.2015 г. № 189 «Об утверждении Плана мероприятий по защите муниципальных информационных систем, создаваемых и приобретаемых за счет бюджета Провиденского муниципального района, Постановление администрации Провиденского муниципального района от 03.08.2015 г. № 184 «Об утверждении Положения о порядке создания, функционирования и использования муниципальных информационных систем органов местного самоуправления и муниципальных органов Провиденского муниципального района |
| Сроки и этапы реализации программы | 2017-2018 годы:  1 этап – 2017 год;  2 этап – 2018 год; |
| Финансовое обеспечение муниципальной программы | Общий объём финансовых затрат на реализацию программы из местного бюджета 2000 тыс.руб., в том числе:  - на 2017 год – 1050 тыс. рублей;  - на 2018 год – 950 тыс. рублей; |
| Важнейшие целевые индикаторы и показатели муниципальной программы (непосредственные) | Количество информационных систем, защищенных согласно требованиям по безопасности информации ограниченного доступа не содержащей государственной тайны и персональных данных-3. Количество муниципальных служащих, и иных работников органов местного самоуправления, ответственных за защиту информации ограниченного доступа не содержащей государственной тайны и персональных данных, прошедших обучение - 2. |
| Ожидаемые результаты реализации программы и показатели эффективности | -Доля защищённых информационных систем обрабатывающих персональные данные - 100%  -Доля муниципальных служащих и иных работников, ответственных за защиту информации и персональных данных, прошедших обучение – 100 % |

II.Характеристика проблемы

На территории Провиденского городского округа системно повышается роль информационных технологий в развитии взаимодействия между органами государственной власти, местного самоуправления и гражданами. В связи с этим информационная безопасность становится социально значимым фактором, обусловленным недопущением разглашения информации ограниченного доступа, в том числе информации, касающейся частной жизни граждан.

Доступность средств вычислительной техники привела к распространению компьютерной грамотности в широких слоях населения, что закономерно привело к увеличению числа попыток неправомерного вмешательства в работу государственных автоматизированных систем. К сожалению, многие из этих попыток имеют успех и наносят значительный урон всем заинтересованным субъектам информационных отношений. Положение усугубляется тем, что нормативное правовое обеспечение защиты интересов субъектов информационных отношений отстает от потребностей личности, общества и государства. Отставание в области создания строгой и непротиворечивой системы законодательно-правового регулирования отношений в сфере использования информации создает условия для возникновения и распространения «компьютерной преступности». Еще одним весомым аргументом в пользу усиления внимания к вопросам защиты информации является бурное развитие и распространение так называемых компьютерных вирусов, способных скрытно существовать в информационно-телекоммуникационных системах и совершать потенциально любые несанкционированные действия. Особую опасность для таких систем представляют также злоумышленники, специалисты-профессионалы в области информационных технологий, досконально знающие все достоинства и слабые места вычислительных систем и располагающие подробнейшей документацией, а также самыми совершенными инструментальными и технологическими средствами для анализа и взлома механизмов защиты. Все это требует усиления государственного внимания к вопросам организации защиты информации ограниченного доступа не содержащей государственной тайны и персональных данных, принятия дополнительных мер правового и технического характера, сложных по реализации и затратных по исполнению.

Неправомерное искажение или фальсификация, уничтожение или разглашение информации ограниченного доступа не содержащей государственной тайны, а также персональных данных, равно как и дезорганизация процессов их обработки и передачи в информационно-управляющих системах наносят серьезный урон администрации городского округа, бюджетным учреждениям и другим субъектам, участвующим в процессах автоматизированного информационного взаимодействия. Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы персональная информация была бы постоянно легко доступна и, в то же время, надежно защищена от неправомерного ее использования, нежелательного разглашения, фальсификации, незаконного тиражирования или уничтожения.

Безопасность информации ограниченного доступа не содержащей государственной тайны и персональных данных должна достигаться путем исключения несанкционированного, в том числе случайного, доступа к информации ограниченного доступа не содержащей государственной тайны и персональным данным, результатом которого может стать их уничтожение, изменение, блокирование, копирование или несанкционированное распространение.

Безопасность информации ограниченного доступа не содержащей государственной тайны и персональных данных при их обработке в информационных системах (далее - ИС) должна обеспечиваться с помощью системы защиты информации ограниченного доступа не содержащей государственной тайны и персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки данных), а также используемые в информационной системе информационные технологии.

Конкретные методы и способы защиты информации в ИСПДн установлены методическими документами Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации. Средства защиты информации, применяемые в информационных системах, в установленном порядке должны проходить процедуру оценки соответствия. Оценку достаточности принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах предписано проводить на постоянной основе.

В настоящее время в вопросах защиты информации ограниченного доступа не содержащей государственной тайны и персональных данных в администрации существует ряд недостатков:

1.Не выполняются работы по анализу угроз безопасности ИСПДн (в результате этого возможные каналы утечки информации не определены, мероприятия по их закрытию не спланированы);

2. Не организованы необходимые меры защиты в ИСПДн;

3. Не внедряются сертифицированные программные и технические средства защиты;

4. Не выполняются работы по аттестации ИСПДн, согласно требованиям по безопасности информации;

5. Передача информации ограниченного доступа не содержащей государственной тайны и персональных данных осуществляется в открытом (незащищенном) режиме;

6. Отсутствую квалифицированные специалисты, ответственные за обеспечение безопасности информации.

В результате в органах местного самоуправления создаются условия для:

1.Нарушения конфиденциальности персональных данных путем перехвата техническими средствами разведки, хищения или копирования;

2.Блокирования информации (нарушения доступности);

3.Уничтожения информации;

4.Модификации (искажения) информации;

5.Нарушения адресности при передаче информации по каналам связи;

6.Отрицания подлинности информации;

7.Навязывания ложной информации.

III.Основные цели и задачи программы

1. Основными целями системы технической защиты информации являются предотвращение или существенное снижение ущерба органам власти, органам местного самоуправления и предприятиям муниципальной собственности от утечки информации по техническим каналам и несанкционированного доступа к ней, преднамеренного воздействия на информацию с целью её разрушения, уничтожения, модификации или блокирования;

2. Обеспечение условий, способствующих реализации государственной политики в сфере информационной безопасности на территории автономного округа.

Задачи программных мероприятий:

1. Организация обеспечения безопасности информации ограниченного доступа не содержащей государственной тайны и персональных данных.

2. Техническая защита персональных данных.

3. Подготовка кадров по вопросам защиты информации ограниченного доступа не содержащей государственной тайны и персональных данных.

4. Проведение в соответствие с требованиями защиты информации объектов информатизации.

Программные мероприятия включают комплекс работ в администрации Провиденского городского округа.

IV.Сроки и этапы реализации программы

Сроки реализации Программы:

1 этап – 2017 год; 2 этап – 2018 год.

V.Информация о расходах на реализацию муниципальной программы

Финансовое обеспечение Программы осуществляется из средств местного бюджета Провиденского городского округа 2000 тыс. рублей, в том числе по годам:

2017 год – 1050 тыс.рублей;

2018 год – 950 тыс.рублей;

Ежегодные объемы финансового обеспечения реализации муниципальной программы определяются в пределах действующих расходных обязательств и подлежат ежегодному уточнению в рамках подготовки проекта бюджета городского округа на очередной финансовый год и плановый период.

VI.Ожидаемые конечные, а также непосредственные результаты реализации программы

Ожидаемые конечные, а также непосредственные результаты реализации программы, приведены в приложении 2 к настоящей Программе.

VII.Обобщенная характеристика программных мероприятий

Работы по созданию системы защиты ПДн проводятся в три этапа:

1. Предпроектный этап, включающий определение перечня защищаемых информационных ресурсов и технических средств, классификацию и категорирование объектов информатизации, разработку технического задания на создание СЗПДн.

2. Стадия разработки СЗПДн;

3. Стадия ввода в действие СЗПДн, включающая закупку, установку, опытную эксплуатацию и приемосдаточные испытания средств защиты информации, а также аттестацию ИСПДн на их соответствие установленным требованиям.

На первом этапе проводятся следующие работы:

1. В администрации назначаются должностные лица, ответственные за организацию и проведение работ по созданию системы защиты информации, определяются подразделения или отдельные специалисты, непосредственно участвующие в проведении указанных работ;

2. Определяются мероприятия по обеспечению режима конфиденциальности на стадии создания СЗПДн;

3. Проводится анализ циркуляции ПДн в органах администрации, по результатам которого определяются состав технических средств и объектов информатизации, участвующих в обработке ПДн, условия их расположения, степень конфиденциальности и режимы обработки.

4. Определяются требования по защите информации ограниченного доступа не содержащей государственной тайны и персональных данных от несанкционированного доступа (далее - НСД) при их обработке в ИСПДн;

5. На основе исходных данных, полученных в результате обследования объектов информатизации, и предъявляемых к ним требованиям по защите информации от НСД, определяется класс защищенности автоматизированных систем, участвующих в обработке данных;

6. Распоряжением (приказом) руководителя определяется контролируемая зона (КЗ), в пределах которой исключено пребывание посторонних лиц, не имеющих постоянного или разового пропуска, а также транспортных средств;

7. Проводится анализ возможных технических каналов утечки информации;

8. Проводится оценка возможностей средств технических разведок и других источников угроз, которые опасны для органов местного самоуправления, в том числе со стороны преступных группировок, частных лиц, организаций и т.п. Указанная оценка производится на основе расчетных формул и данных, приведенных в нормативных документах Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России), и реально складывающейся оперативной обстановки;

9. Составляется перечень предполагаемых к использованию сертифицированных средств защиты информации;

10. Проводится оценка материальных, трудовых и финансовых затрат на разработку и внедрение системы защиты информации;

11. Обосновывается необходимость привлечения специализированных предприятий для создания СЗПДн;

12. Разрабатывается техническое задание (ТЗ) на создание СЗПДн, в котором должны найти отражение следующие вопросы:

13. Исходные данные о создаваемой системы или иного объекта информатизации в техническом, программном, информационном и организационном аспектах;

14. Уровень защищённости информационных систем;

15. Классы защищенности автоматизированных систем (АС) по требованиям защиты от НСД;

16. Конкретизация требований к системе защиты данных на основе нормативных документов, установленных классов защищенности;

17. Перечень выходных документов по окончании создания;

18. Состав, содержание и сроки проведения работ по этапам разработки и внедрения системы защиты данных.

На втором этапе:

1. Разрабатывается перечень организационных и технических мероприятий по защите объектов информатизации в соответствии с предъявляемыми в ТЗ требованиями, направленных на предотвращение утечки информации ограниченного доступа не содержащей государственной тайны и персональных данных за пределы контролируемой зоны. Указанные мероприятия должны обеспечить устранение или ослабление (искажение) демаскирующих признаков и закрытие возможных технических каналов утечки ПДн;

2. Определяется состав серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;

3. Определяется состав технических средств, подвергаемых специальным исследованиям и проверке;

4. Разрабатывается технические паспорта на объекты информатизации;

5. Разрабатываются инструкции по обеспечению безопасности информации на этапе эксплуатации технических средств;

6. Разрабатывается план выполнения организационных и технических мероприятий по защите ИСПДн;

7. Разрабатывается проектная документация.

Третий этап включает в себя проведение следующих видов работ:

1. Проведение специальных исследований не сертифицированных технических средств и получение предписаний на их эксплуатацию;

2. Проведение (по решению руководителя) специальной проверки основных технических средств импортного производства;

3. Закупка сертифицированных серийно выпускаемых технических и программных  
средств защиты информации и их установка;

4. Монтаж и пуско-наладка технических средств, входящих в состав ИСПДн;

5. Разработка и реализация разрешительной системы доступа к средствам вычислительной техники и автоматизированным системам, участвующим в обработке данных;

6. Разработка организационно-распорядительной и рабочей документации по эксплуатации ИСПДн;

7. Опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объектов информатизации;

8. Проведение инструментального контроля эффективности средств защиты, внедренных на объектах информатизации;

9. Приемо-сдаточные испытания СЗПДн по результатам ее опытной эксплуатации;

10. Аттестация ИСНДн по требованиям защиты информации.

При положительных результатах аттестации:

1.Владельцу ИСПДн выдается «Аттестат соответствия» этого объекта требованиям безопасности информации;

2. Распоряжением главы администрации Провиденского городского округа вводится разрешение на обработку данных на тех объектах информатизации, на которые получены аттестаты соответствия.

Обучение кадров.

В целях организации и подержания требуемого уровня безопасности данных и иной информации необходим высококвалифицированный персонал. Качество решений по защите информации во многом определяется уровнем подготовки специалистов в области информационной безопасности.

За последние годы вопрос подготовки необходимого количества высококвалифицированных специалистов в сфере информационной безопасности, как государственной проблемы, существенно обострился в связи с расширением информатизации всех сторон деятельности общества и государства, ростом спектра угроз безопасности информации, возрастанием тяжести последствий их реализации.

Действующая система подготовки кадров в области информационной безопасности на территории округа носит несистемный характер (скорее отсутствует вообще). Поэтому дальнейшее развитие форм и методов подготовки специалистов по защите информации на основе внедрения новых информационных технологий, развития учебно-методической и материальной базы может рассматриваться как одно из важнейших направлений в комплексе мер по развитию системы защиты информации ограниченного доступа не содержащей государственной тайны и персональных данных.

В 2017-2018 годах необходимо организовать обучение руководителей структурных подразделений администрации, персонала, ответственного за защиту информации, в том числе пользователей на рабочих местах работе со средствами защиты информации (ознакомление с организационно-распорядительной документацией на систему защиты информации).

Систематизируя изложенное, мероприятия по обеспечению безопасности информации ограниченного доступа не содержащей государственной тайны и персональных данных формируются из 3 (трех) блоков:

1.Организация обеспечения безопасности данных (организационный блок, включающий работы по предпроектным обследования, аудиту, экспертизам ИСПДн и оценкам их защищенности, классификации ИСПДн, выявлению и учету угроз безопасности ПД, разработке технических заданий на создание системы защиты данных, проектированию ИСПДн, разработке нормативной и методической документации, а также формированию структуры системы защиты ПДн и т.д.).

2.Техническая защита информации ограниченного доступа не содержащей государственной тайны и персональных данных.

Технико-внедренческий блок, включающий защиту технических каналов утечки информации, защиту ПДн от несанкционированного доступа, закупку, монтаж и пуско-наладку средств защиты, серверного оборудования а также рабочих мест (компьютеров), аттестацию ИСПДн согласно требованиям по безопасности информации, внедрение систем контроля не декларированных возможностей, регистрации и учета, обеспечения целостности, обнаружения вторжений, криптографической и антивирусной защиты и т.д.

3.Обучение кадров.

Образовательный блок, включающий организацию курсов подготовки и переподготовки работников администрации по вопросам защиты данных, проведение обучающих семинаров, конференций и т.д.

VIII.Механизм реализации муниципальной программы

Управление ходом реализации Программы осуществляет заказчик-координатор – Организационно-правовое управление администрации Провиденского городского округа. Координатор Программы несет ответственность за реализацию Программы, уточняет сроки реализации мероприятий и объемы их финансирования.

Исполнители Программы:

Администрация Провиденского городского округа;

Реализация Программы осуществляется посредством размещения муниципальных заказов на выполнение работ, оказание услуг на основе муниципальных контрактов на оказание услуг, выполнение работ для муниципальных нужд, заключаемых с исполнителями в установленном законодательством Российской Федерации порядке.

Оценка хода исполнения мероприятий Программы основана на мониторинге ожидаемых непосредственных и конечных результатов Программы как сопоставления фактически достигнутых, так и целевых значений показателей. В соответствии с данными мониторинга по фактически достигнутым результатам реализации в Программу могут быть внесены изменения.

Для проведения текущего мониторинга реализации муниципальной программы Организационно-правовое управление представляет в Управление финансов, экономики и имущественных отношений ежемесячно, в срок не позднее 15 числа месяца, следующего за отчетным, информацию о финансовых затратах и показателях результативности муниципальной программы, в срок не позднее 25 января года, следующего за отчетным, а также по окончании срока реализации муниципальной программы отчет о ходе реализации муниципальной программы, оценку эффективности и результативности реализации муниципальной программы.

Приложение 1

к муниципальной программе

«Защита информации администрации

Провиденского городского округа

на 2017-2018 годы»

Перечень программных мероприятий муниципальной программы «Защита информации администрации Провиденского городского округа на 2017-2018 годы»

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Мероприятия программы | Источники финансирования | Исполнители мероприятий программы | Финансовые затраты на реализацию,  тыс. рублей | | |
| 2017 г. | 2018 г. | Всего расходов по программе |
|  |  | Всего по муниципальной программе |  | 1050 | 950 | 2000 |
|  |  | федеральный бюджет |  |  |  |  |
|  |  | бюджет автономного округа |  |  |  |  |
|  |  | местный бюджет |  | 1050 | 950 | 2000 |
|  |  | привлеченные средства |  |  |  |  |
| 1. | Комплексное обследование информационных систем информации ограниченного доступа не содержащей государственной тайны | местный бюджет | Администрация Провиденского городского округа | 0 | 0 | 0 |
| 2. | Разработка/корректировка организационно-распорядительных документов | местный бюджет | Администрация Провиденского городского округа | 0 | 0 | 0 |
| 3. | Разработка технического задания на систему защиты информации ограниченного доступа не содержащей государственной тайны | местный бюджет | Администрация Провиденского городского округа | 0 | 0 | 0 |
| 4. | Разработка технического проекта на систему защиты информации ограниченного доступа не содержащей государственной тайны | местный бюджет | Администрация Провиденского городского округа | 0 | 0 | 0 |
| 6. | Сопровождение системы защиты информации ограниченного доступа не содержащей государственной тайны | местный бюджет | Администрация Провиденского городского округа | 0 | 0 | 0 |
| 7. | Внедрение системы защиты информации ограниченного доступа не содержащей государственной тайны (Установка, настройка, тестовая эксплуатация), 3 ИСПДн | местный бюджет | Администрация Провиденского городского округа | 100 | 50 | 150 |
| 8. | Проведение оценки соответствия требованиям по безопасности информации ограниченного доступа не содержащей государственной тайны и персональных данных при их обработке в информационных системах персональных и иных данных с документальным подтверждением соответствия определенному уровню защиты, 3 ИСПДн | местный бюджет | Администрация Провиденского городского округа | 100 | 50 | 150 |
| 6. | Рабочее место инженера-программиста и администратора информационной безопасности | местный бюджет | Администрация Провиденского городского округа | 100 | 100 | 200 |
| 7. | Поставка программного обеспечения защиты от несанкционированного доступа к информации и средств контроля утечек конфиденциальной информации | местный бюджет | Администрация Провиденского городского округа | 100 | 100 | 200 |
| 8. | Модернизация и приобретение серверного и сетевого оборудования (3 шт.) | местный бюджет | Администрация Провиденского городского округа | 200 | 200 | 400 |
| 9. | Поставка компьютерной техники и периферийной оргтехники, отвечающей требованиям защиты от несанкционированного доступа к конфиденциальной информации и персональным данным | местный бюджет | Администрация Провиденского городского округа | 300 | 300 | 600 |
| Задача 3. Подготовка кадров по вопросам защиты информации ограниченного доступа не содержащей государственной тайны. | | | | | | |
| 1. | Обучение по вопросам защиты информации ограниченного доступа не содержащей государственной тайны | местный бюджет | Администрация Провиденского городского округа | 150 | 150 | 300 |

Подготовил: Рекун Д.В.

Согласовано: Веденьева Т.Г.

Ручинский Н.Л.

Разослано: дело, УФЭиИО, Отдел по бух. учету.