Муниципальное образование Октябрьский район

АДМИНИСТРАЦИЯ ОКТЯБРЬСКОГО РАЙОНА

РАСПОРЯЖЕНИЕ

« 30 » июня 2017 г. № 80-р

пгт. Октябрьское

О Политике информационной безопасности
в администрации Октябрьского района

В соответствии с Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также в целях обеспечения информационной безопасности в администрации Октябрьского района:

1. Утвердить Политику информационной безопасности в администрации Октябрьского района согласно приложению.

2. Заведующему отделом информационного обеспечения администрации Октябрьского района Кириченко Н.В. довести распоряжение до руководителей структурных подразделений администрации Октябрьского района.

3. Руководителям структурных подразделений администрации Октябрьского района:

3.1. Ознакомить работников подведомственных структурных подразделений администрации Октябрьского района с распоряжением под роспись.

3.2. Осуществлять внутренний контроль над исполнением требований Политики информационной безопасности в администрации Октябрьского района в подведомственном структурном подразделении администрации Октябрьского района.

4. Контроль за выполнением распоряжения возложить на заместителя главы администрации Октябрьского района по правовому обеспечению, управляющего делами администрации Октябрьского района Хромова Н.В.

Глава Октябрьского района А.П. Куташова

Приложение
к распоряжению администрации
Октябрьского района
от «30» июня 2017 г. № 80-р

Политика информационной безопасности в администрации Октябрьского района

1. Термины и их определения

Защищаемая информация - информация, подлежащая защите в соответствии с требованиями нормативных документов в области безопасности информации или требованиями, устанавливаемыми собственником информации.

Информационная система - система, представляющая собой совокупность информации, содержащейся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку такой информации с использованием средств автоматизации или без использования таких средств.

Нарушитель безопасности - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах.

Угроза безопасности информации - некая совокупность факторов и условий, которая создает опасность в отношении защищаемой информации.

Правила разграничения доступа - совокупность правил, регламентирующих порядок и условия доступа субъектов доступа (сотрудников, программ) к объектам доступа (информации, её носителям, процессам и другим ресурсам).

Несанкционированный доступ (несанкционированные действия, НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Контролируемая зона - это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Дополнительные устройства обмена информацией - портативные жесткие диски, съемные флэш-носители, CD, DVD - диски.

Администратор безопасности – лицо, ответственное за защиту информационных систем от несанкционированного доступа к информации.

2. Общие положения

Политика информационной безопасности в администрации Октябрьского района (далее - Политика) разработана на основе требований действующих в Российской Федерации законодательных и нормативных документов, регламентирующих вопросы защиты информации, с учетом современного состояния, целей, задач и правовых основ создания, эксплуатации и функционирования информационных систем администрации Октябрьского района (далее - Администрация), а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений Администрации.

Политика определяет основные направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих положений, правил, инструкций.

В Политике определены требования к работникам Администрации, степень их ответственности за обеспечение безопасности информации в информационных системах Администрации.

Требования настоящей Политики распространяются на всех работников Администрации (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, исполнители, поставщики и т.п.).

3. Цели и задачи политики информационной безопасности

Целью Политики является выработка единых требований и правил, обеспечивающих непрерывность основных бизнес-процессов, минимизацию возможных потерь и ущерба от нарушений в области информационной безопасности.

Основными задачами Политики являются:

- отнесение информации к категории общедоступной, ограниченного распространения, персональным данным, коммерческой и другим видам тайн, иной конфиденциальной информации, подлежащей защите;
- предотвращение несанкционированного доступа к защищаемой информации и (или) передачи её лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к защищаемой информации;
- недопущение воздействия на технические средства автоматизированной обработки защищаемой информации, в результате которого может быть нарушена её конфиденциальность, доступность, целостность;
- возможность незамедлительного восстановления защищаемой информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
постоянный контроль над обеспечением уровня защищённости информации;
- прогнозирование и своевременное выявление угроз безопасности информации, обрабатываемой в информационных системах Администрации, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования Администрации с наименьшей вероятностью реализации угроз безопасности в информационных ресурсах и нанесения ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Администрации, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности.

1. Объекты защиты информационной безопасности

Объектами защиты являются защищаемая информация, обрабатываемая в информационных системах Администрации, технические и программные средства ее обработки, передачи и защиты.

Перечень конфиденциальной информации и Перечень персональных данных, подлежащих защите, утверждаются главой Октябрьского района.

Объекты защиты включают в себя:

- обрабатываемую информацию;
- технологическую информацию;
- программно-технические средства обработки;
- программные и аппаратные средства защиты информации;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты информационных систем.

5. Угрозы безопасности защищаемой информации

Основные угрозы безопасности защищаемой информации:

- угрозы от утечки по техническим каналам;
- угрозы несанкционированного доступа к информации;
- угрозы уничтожения, хищения аппаратных средств, носителей информации путем физического доступа к элементам информационных систем;
- угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационных систем, сбоев в программном обеспечении, а также от-угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;
- угрозы преднамеренных действий внутренних нарушителей;
- угрозы несанкционированного доступа по каналам связи.

6. Меры безопасности

Для обеспечения физической защиты информационных ресурсов должны быть установлены границы контролируемой зоны, приняты меры для предотвращения неавторизованного (несанкционированного) доступа в помещения где происходит обработка защищаемой информации.

Кабинеты, в которых ведется обработка защищаемой информации, должны быть:

- оборудованы опечатывающим устройством;
- в кабинетах должны быть приняты меры для затруднения видимости посторонним лицам в виде штор/жалюзи;
- кабинеты в нерабочее время должны опечатываться;
- двери кабинетов должны быть закрыты и должны открываться только для прохода работников и посетителей Администрации согласно утвержденным правилам доступа в границы контролируемой зон;
- уборка в кабинетах должна производиться только в присутствии работников Администрации, с соблюдением мер, исключающих доступ к защищаемой информации и оборудованию;
- обработка защищаемой информации в помещениях Администрации должна производиться таким образом, чтобы исключать ознакомление с защищаемой информацией лицами, не имеющими прав доступа к данной информации.
- для хранения документов, содержащих защищаемую информацию, кабинеты Администрации должны быть оборудованы сейфами, металлическими шкафами с замками и опечатывающими устройствами;
- для уничтожения черновиков документов, содержащих защищаемую информацию, кабинеты должны быть оборудованы уничтожителями бумаг;
- помещение серверной должно быть оборудовано прочной дверью с замком и опечатывающим устройством, пожарно-охранной сигнализацией, кондиционером, системой пожаротушения;
- охранно-пожарная сигнализация кабинетов должна реализоваться с выводом на пульт дежурного охранника или на пульт вневедомственной охраны;
- по окончании рабочего дня работники Администрации должны закрывать двери кабинетов на ключ и опечатывать её.

Печати, предназначенные для опечатывания кабинетов, сейфов, металлических шкафов должны храниться у уполномоченных работников.

Допуск работников к ресурсам информационных систем должен быть регламентирован. Уровень полномочий каждого пользователя информационной системы должен соответствовать его должностным обязанностям. Расширение прав должно согласовываться с отделом, ответственным за данный информационный ресурс и администратором безопасности.

Обработка информации в информационных системах должна происходить в соответствии с документами, регламентирующими порядок работы в данной информационной системе.

Все неиспользуемые в работе устройства ввода-вывода информации (WiFi, COM, LPT, USB, IR порты, дисководы ГМД, CD, DVD и т.п.) на рабочих местах работников, работающих с защищаемой информацией, должны быть отключены, не нужные для работы программные средства и данные с жестких дисков удалены.

Дополнительные устройства обмена информацией могут использоваться только в целях переноса информации. Использование подобных устройств должно согласовываться с администратором безопасности. Каждое дополнительное устройство обмена информацией должно быть зарегистрировано в соответствующем журнале.

На автоматизированных рабочих местах всех пользователей локальной сети Администрации должна быть установлена антивирусная программа. Порядок управления антивирусной защитой в Администрации определяется соответствующий инструкцией.

Доступ к ресурсам информационной системы (вход в операционную систему, в прикладное программное обеспечение) должен быть организован с применением аутентификации (введение логина, пароля). Возможно использование дополнительных программно-аппаратных средств аутентификации (в том числе двух- и трехфакторной).

Требования паролей пользователей и администраторов информационных систем устанавливаются соответствующей инструкцией.

Установкой и настройкой средств защиты информации, применяемых для защиты информации в информационных системах, должен руководить администратор безопасности.

Доступ пользователей к публичным ресурсам сети Интернет определяется соответствующей инструкцией.

Передача защищаемой информации по каналам, выходящим за границы контролируемой зоны, должна осуществляться только с использованием сертифицированных ФСБ России средств криптографической защиты информации.

Правила резервного копирования и восстановления информации, обрабатываемой в информационных системах, устанавливаются соответствующей инструкцией.

7. Требования к работникам

Все пользователи информационных систем должны быть ознакомлены с организационно - распорядительными документами по обеспечению информационной безопасности в части их касающейся, знать и неукоснительно выполнять инструкции, положения, регламенты и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

При вступлении в должность нового работника, руководитель структурного подразделения обязан организовать его ознакомление с должностной инструкцией и документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных ресурсов.

Работники Администрации, использующие технические средства аутентификации, обеспечивают сохранность идентификаторов (электронных ключей), не допускают НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность персональных идентификаторов.

Работники Администрации должны соблюдать установленные процедуры поддержания режима безопасности при выборе и использовании паролей.

Работники Администрации должны знать требования по безопасности информации и неукоснительно их выполнять.

8. Ответственность за нарушение Политики

В соответствии со статьей 24 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований указанного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.