АДМИНИСТРАЦИЯ ГОРОДА ЮЖНО-САХАЛИНСКА

РАСПОРЯЖЕНИЕ

от 23.03.2020 № 205-р

О проведении плановых инструктажей по информационной безопасности в администрации города Южно-Сахалинска

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФАПСИ от 13 июня 2001 г. № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" и решением совета по защите информации при Правительстве Сахалинской области от 04.12.2019 №39:

1. Утвердить:

1.1. Правила проведение инструктажа по информационной безопасности в администрации города Южно-Сахалинска (приложение №1);

1.2. Правила антивирусной защиты в администрации города Южно-Сахалинска (приложение №2);

2. Департаменту мобилизационной подготовки и защиты информации аппарата администрации города Южно-Сахалинска в срок до 01.04.2020 года:

2.1 Провести инструктаж по информационной безопасности с руководством администрации города Южно-Сахалинска и руководителями структурных подразделений аппарата и отраслевых (функциональных) органов администрации города Южно-Сахалинска.

3. Руководителям структурных подразделений аппарата и отраслевых (функциональных) органов администрации города Южно-Сахалинска, в срок до 01.05.2020 года:

3.1. Провести инструктаж по информационной безопасности с сотрудниками;

3.2. О проделанной работе сообщить в Департамент мобилизационной

подготовки и защиты информации аппарата администрации города Южно-Сахалинска до 01.06.2020.

4. Руководителям муниципальных, бюджетных и казенных учреждений, муниципальных унитарных предприятий:

4.1. Разработать и утвердить аналогичные документы, предусмотренные пунктом 1 настоящего распоряжения;

4.2. Провести инструктаж по информационной безопасности с сотрудниками учреждений и предприятий;

4.3. О проделанной работе сообщить в Департамент мобилизационной подготовки и защиты информации аппарата администрации города Южно-Сахалинска до 01.07.2020.

5. Настоящее распоряжение разместить на официальном сайте администрации города Южно-Сахалинска.

6. Контроль исполнения распоряжения администрации города возложить на директора Департамента мобилизационной подготовки и защиты информации аппарата администрации города Южно-Сахалинска.

Мэр города С.А.Надсадин

Приложение №1

Утверждены
распоряжением администрации
города Южно-Сахалинска
от 23.03.2020 № 205-р

Правила
проведения инструктажа по информационной безопасности
в администрации города Южно-Сахалинска

1. Действие настоящих Правил обеспечивается руководителями структурных подразделений аппарата, отраслевых (функциональных) органов администрации города Южно-Сахалинска, подведомственных муниципальных, бюджетных и казенных учреждений, муниципальных унитарных предприятий.

2. Сотрудники (работники) структурных подразделений аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, подведомственных муниципальных, бюджетных, казенных и автономных учреждений, муниципальных унитарных предприятий, допущенные к работе с муниципальной информационной системой «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска» (далее - пользователи ЕМТС), обязаны пройти инструктаж по вопросам информационной безопасности с целью подтверждения своих знаний по поддержанию установленного режима защиты информации.

3. Инструктаж представляет собой ознакомление пользователей ЕМТС с положением действующих нормативных документов по обеспечению информационной безопасности, в том числе:

- инструкции пользователя ЕМТС администрации города Южно-Сахалинска;
- порядка доступа сотрудников администрации города Южно-Сахалинска в помещения, в которых ведется обработка персональных данных;
- инструкции по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и криптоключами к ним;
- правилами антивирусной защиты в администрации города Южно-Сахалинска.

4. Ознакомление с положениями нормативной документации пользователь ЕМТС подтверждает своей личной подписью в Журнале инструктажа по информационной безопасности, что свидетельствует о его прохождении.

5. Контроль проведения инструктажа и периодическая проверка знания пользователей ЕМТС положений нормативной документации по вопросам информационной безопасности возлагается на Департамент мобилизационной подготовки и защиты информации аппарата администрации города Южно-Сахалинска.

6. Ответственность за проведение инструктажа возлагается на руководителей структурных подразделений аппарата, отраслевых (функциональных) органов администрации города Южно-Сахалинска, подведомственных муниципальных, бюджетных и казенных учреждений, муниципальных унитарных предприятий.

7. Пользователи ЕМТС, не прошедшие инструктаж, к работе с ЕМТС не допускаются.

8. Для вновь принятых пользователей ЕМТС инструктаж проводится перед началом работы, для всех остальных пользователей ЕМТС - не реже одного раза в год.

9. Проверка знаний пользователей ЕМТС положений нормативной документации по вопросам информационной безопасности проводится администратором информационной безопасности ЕМТС либо Департаментом мобилизационной подготовки и защиты информации в ходе периодического контроля или внутреннего контроля соблюдения режима безопасности информации.

10. Журнал инструктажа по информационной безопасности хранится в структурных подразделениях аппарата, отраслевых (функциональных) органов администрации города Южно-Сахалинска, подведомственных муниципальных учреждениях и предприятиях.

Приложение №2

Утверждены
распоряжением администрации
города Южно-Сахалинска
от 23.03.2020 № 205-р

Правила
антивирусной защиты в администрации
города Южно-Сахалинска

1. Настоящие правила определяют требования к организации защиты муниципальной информационной системы «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска» (далее — ЕМТС) от воздействия компьютерных вирусов и устанавливают ответственность за их выполнение.

2. К использованию в ЕМТС допускаются по требованиям безопасности информации сертифицированные ФСТЭК или ФСБ России средства защиты информации от вредоносных программ.

3. Под антивирусным средством в данных правилах понимается специализированное программное средство защиты информации, предназначенное для обнаружения фактов вирусного воздействия на компоненты вычислительной техники объектов информатизации.

4. Все операции по настройке, администрированию и обновлению антивирусных средств производятся администратором безопасности информации ЕМТС.

5. Обновление антивирусных баз должно производиться ежедневно.

6. Ответственность за выполнение положений данных Правил возлагается на администратора безопасности ЕМТС и пользователей ЕМТС.

7. Обязательному антивирусному контролю подлежит любая информация получаемая от сторонних лиц и организаций.

8. Устанавливаемое системное и прикладное программное обеспечение на средствах вычислительной техники должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на ПЭВМ лицом, установившим (изменившим) программное обеспечение.

9. При работе с машинными носителями информации, полученными из сторонних организаций, пользователи ЕМТС на рабочих местах обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

10. При возникновении подозрения наличия компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, исчезновение файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ЕМТС должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь администратора безопасности ЕМТС для определения им факта наличия или отсутствия компьютерного вируса.

11. В случае обнаружения компьютерного вируса пользователь ЕМТС обязан:

- приостановить работу на АРМ;
- немедленно поставить в известность о факте обнаружения файлов, зараженных вирусом, руководителя подразделения, администратора безопасности ЕМТС и владельца зараженных файлов;
- провести «лечение» зараженных вирусом файлов штатными антивирусными средствами;
- при невозможности «лечения» уничтожить зараженные вирусом файлы способом, исключающим их восстановление.

12. В случае обнаружения на съемных носителях нового вируса, не поддающегося «лечению», пользователь ЕМТС обязан поставить в известность администратора безопасности ЕМТС.

13. Пользователи ЕМТС проводят периодическое (не реже 1 раза в неделю) полное тестирование компьютера на вирусы.