

**АДМИНИСТРАЦИЯ
АНУЧИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
ПРИМОРСКОГО КРАЯ**

 Р А С П О Р Я Ж Е Н И Е

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  2021 г. |  |  с. Анучино | № |  - р  |

**Об утверждении инструкций по организации антивирусной защите и парольной защите в информационных системах персональных данных в администрации Анучинского муниципального округа
Приморского края**

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ
«О персональных данных», Приказа 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», руководствуясь Федеральным законом от 06.10.2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Уставом Анучинского муниципального округа Приморского края

1. Утвердить инструкцию по организации антивирусной защиты в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края (Прилагается).
2. Утвердить инструкцию по парольной защите в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края (Прилагается).
3. Ознакомить сотрудников администрации Анучинского муниципального округа Приморского края с прилагаемыми инструкциями (Федчикова А.А.).
4. Контроль за исполнением настоящего распоряжения возложить
на А.Я. Янчука, первого заместителя главы администрации Анучинского муниципального округа.

Глава Анучинского

муниципального округа С.А. Понуровский

УТВЕРЖДЕНА

Распоряжением администрации Анучинского

муниципального округа

Приморского края

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г. № \_\_\_\_\_

**ИНСТРУКЦИЯ**

**по организации антивирусной защиты в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края**

### **Общие положения**

* 1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в администрации Анучинского муниципального округа Приморского края (далее - Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.
	2. Данная инструкция распространяется на всех пользователей и администраторов информационных систем персональных данных (далее – ИСПДн) в Администрации.

### **Установка и обновление антивирусных средств**

### Установка и настройка антивирусных средств осуществляются только Администратором информационной системы персональных данных.

### Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.

### **Требования к проведению мероприятий по антивирусной защите**

### Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, flash дисках, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

### Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.

### Контроль информации на съёмных носителях производится непосредственно перед её использованием.

### Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ ([электронно-вычислительная машина](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE-%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0)).Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность.

### Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.

### Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

### Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

### **Действия сотрудников при обнаружении компьютерного вируса**

### В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной системы персональных данных;

- провести лечение или уничтожение зараженных файлов.

### При возникновении подозрения на наличие компьютерного вируса пользователь или администратор информационной системы персональных данных должны провести внеочередной антивирусный контроль.

### **Ответственность при организации антивирусной защиты**

### Ответственность за организацию антивирусной защиты возлагается на администратора информационной системы персональных данных.

### Ответственность за выполнение требований данной Инструкции возлагается на пользователей и администратора информационной системы персональных данных.

### Периодический контроль за соблюдением положений данной инструкции возлагается на администратора информационной системы персональных данных.

Приложение к инструкции по организации антивирусной защиты

в информационных системах персональных данных в

администрации Анучинского муниципального округа

Приморского края

**ЛИСТ ОЗНАКОМЛЕНИЯ**

**с инструкцией по организации антивирусной защиты в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края**

| **№ п.п.** | **ФИО** | **Должность и отдел** | **Подпись и дата** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

УТВЕРЖДЕНА

Распоряжением администрации Анучинского

муниципального округа

Приморского края

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г. № \_\_\_\_\_

**ИНСТРУКЦИЯ**

**по парольной защите в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края**

# **Общие положения**

* 1. Пользователь информационных систем персональных данных
	(далее – Пользователь ИСПДн) осуществляет обработку персональных данных в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края (далее – администрация).
	2. Пользователем является каждый работник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
	3. Пользователь несет персональную ответственность за свои действия.
	4. Пользователь в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и другими внутренними нормативно - правовыми документами администрации по защите информации.

# **Организация парольной защиты**

# Личные пароли доступа к элементам информационных систем персональных данных создаются пользователем самостоятельно, за исключением временного пароля, который выдает Администратор информационных систем персональных данных.

# Пользователь обязан сменить временный пароль, выданный Администратором информационных систем персональных данных при первом входе в систему.

# Смена паролей должна проводиться регулярно, но не реже одного раза в квартал, самостоятельно каждым пользователем.

# В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

# Правила формирования пароля:

* Пароль не может содержать имя учетной записи пользователя или какую либо его часть.
* Пароль должен состоять не менее чем из 8 символов.
* В пароле должны присутствовать символы трех категорий из числа следующих четырех:
* прописные буквы английского алфавита от A до Z;
* строчные буквы английского алфавита от a до z;
* десятичные цифры (от 0 до 9);
* символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).
* Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
* Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
* Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
* Запрещается выбирать пароли, которые уже использовались ранее.
	1. Правила ввода пароля:
* При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).
* При неверном вводе пароля более 5 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.
	1. Правила хранения пароля:
* Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
* Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

2.8. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

1. **Ответственность**
	1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.
	2. Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за обеспечение безопасности персональных данных.
	3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение к инструкции по парольной защите

в информационных системах персональных данных в

администрации Анучинского муниципального округа

Приморского края

**ЛИСТ ОЗНАКОМЛЕНИЯ**

**с инструкцией по парольной защите в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края**

| **№ п.п.** | **ФИО** | **Должность и отдел** | **Подпись и дата** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |