



№ 345

ПРИКАЗ

БОЕРЫК

«25» сентябрия 2019 г.

Об утверждении инструкции
по организации парольной защиты
в Государственной жилищной инспекции Республики Татарстан

В соответствии с Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11. 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными и правовыми актами по защите информации, п р и к а з ы в а ю:


1. Утвердить:
инструкцию по организации парольной защиты в Государственной жилищной инспекции Республики Татарстан (далее - Инструкцию);
2. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник

С.А. Крайнов

СОГЛАСОВАНО:

Заместитель начальника – заместитель
главного Госжилинспектора – начальник
правового управления



В.С.Сагдаров

Начальник
юридического отдела



Н.Н. Воронская

Начальник
контрольно-аналитического отдела



И.С.Начвин

Заведующий сектора информатизации



Э.И.Хабипова

УТВЕРЖДЕНО
приказом начальника
Государственной
жилищной инспекции
Республики Татарстан
С.А. Крайнова

« 25 » сентября 2019 г. № 345

**Инструкция
по организации парольной защиты
в Государственной жилищной инспекции Республики Татарстан**

1. Общие положения

1.1 Инструкция по организации парольной защиты в Государственной жилищной инспекции Республики Татарстан (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11. 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными и правовыми актами по защите информации.

1.2 Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в локальной сети Инспекции, а также контроль за действиями пользователей при работе с паролями.

1.3 В настоящей Инструкции использованы следующие термины и определения:

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Пароль – уникальный признак субъекта доступа, который является его (субъекта) секретом.

Первичный пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые сотрудником сектора информатизации (далее - системным администратором) при создании новой учетной записи.

Основной пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику Инспекции, используемая для подтверждения подлинности владельца учетной записи.

Административный пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная системному администратору Инспекции, используемая при создании новых и настройке текущих учетных записей, при настройке служб и сервисов, установке программ на электронно-вычислительные машины, сервера Инспекции.

Правила доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированной системы (далее – АС).

1.4 Требования настоящей Инструкции обязательны для выполнения всеми сотрудниками Инспекции, ведущими обработку конфиденциальной информации, персональных данных и (или) любой другой информации с применением средств вычислительной техники.

1.5 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль за реализацией требований по обеспечению безопасности при использовании паролей возлагается на администратора безопасности информации.

2. Организация парольной защиты

2.1 Установку первичного пароля производит системный администратор при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

2.2 Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

2.3 При создании первичного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

2.4 Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

2.5 Установку основного пароля производит сотрудник Инспекции при первом входе в систему с новой учетной записью.

2.6 При выборе пароля необходимо руководствоваться «Требованиями к паролям» (Приложение 1).

2.7 В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору безопасности информации и изменить основной пароль.

2.8 Восстановление забытого основного пароля пользователя осуществляется администратором безопасности информации путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

2.9 Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

2.10 При выборе административного пароля необходимо руководствоваться «Требованиями к паролям» (Приложение №1).

2.11 Системный администратор несет персональную ответственность за сохранение в тайне административного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам Инспекции, записывать его, а так же пересылать открытым текстом в электронных сообщениях.

2.12 Системный администратор обязан не реже одного раза в месяц производить смену административного пароля, соблюдая требования настоящего документа.

2.13 В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом заведующему сектором информатизации и изменить административный пароль.

3. Порядок смены паролей

3.1. Полная плановая смена паролей всех сотрудников Инспекции должна проводиться один раз в 6 месяцев.

3.2. Полная внеплановая смена паролей всех сотрудников Инспекции должна производиться в случае прекращения полномочий системного администратора Инспекции.

3.3. Полная внеплановая смена паролей должна производиться в случае компрометации административного пароля.

3.4. В случае компрометации личного основного пароля сотрудника Инспекции необходимо немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или основного пароля.

4. Обязанности сотрудников Инспекции при работе с парольной защитой

4.1 При работе с парольной защитой сотруднику Инспекции запрещается:

- разглашать кому-либо основной пароль и прочие идентифицирующие сведения;

- предоставлять доступ от своей учетной записи к информации, хранящейся в персональном компьютере или в эксплуатируемых информационных системах посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

4.2 Хранение сотрудников Инспекции основного пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

4.3 При вводе пароля сотрудник Инспекции обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5. Случаи компрометации паролей

5.1 Под компрометацией следует понимать:

- физическая утеря носителя с информацией;
- передача идентификационной информации по открытым каналам связи;
- проникновение постороннего лица в помещение физического хранения носителя парольной информации или персонального компьютера или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

5.2 Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией и сотрудники сектора информатизации. Пароль вносится в журнал скомпрометированных паролей и учетных записей, содержащие скомпрометированные пароли и учетные записи (приложение 2).

6. Ответственность пользователей при работе с парольной защитой

6.1 Повседневный контроль за действиями сотрудников Инспекции при работе с паролями, соблюдением Инструкции их смены, хранения и использования, возлагается на системного администратора Инспекции.

6.2 Сотрудники Инспекции должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6.3 Ответственность за организацию парольной защиты возлагается на системного администратора Инспекции.

6.4 Ответственность в случае несвоевременного уведомления системного администратора о случаях утери, кражи, взлома или

компрометации основного пароля сотрудника Инспекции возлагается на сотрудника Инспекции взломанной учетной записи.

Требования к паролям

1. Основной пароль должен генерироваться и распределяться централизованно либо выбираться сотрудником Инспекции с учетом следующих требований:

- Не состоять из имени, отчества или фамилии сотрудника Инспекции ни в каком виде (т.е. написаны в строчном, в прописном, в смешанном виде, задом наперед, два раза и т.д.)

- Не состоять из идентификатора входа (login) сотрудника Инспекции ни в каком виде.

- Не включать в себя имена супруги(а) или детей сотрудника Инспекции.

- Не состоять из любой информации о себе, а именно: номера телефонов, номера в пропусках и других документах, номер или марка автомобиля, почтовый адрес и т.д. и т.п.

- Не состоять только из цифр или одинаковых букв.

- Не включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, «1234567», «QWERTY» и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

- Личный основной пароль сотрудник Инспекции не имеет права сообщать никому.

- Должны содержать строчные и прописные буквы.

- Должны содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы).

- Должны быть легко запоминаемы, чтобы не было необходимости записывать их.

- Должны быть составлены так, чтобы сотрудник Инспекции мог быстро набрать их на клавиатуре.

2. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников Инспекции в их отсутствие, такие сотрудники Инспекции обязаны сразу же после смены своих основных паролей на их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном тубусе передавать на хранение системному администратору Инспекции. Опечатанные конверты (тубусы) с паролями сотрудников Инспекции должны храниться в сейфе в секторе информатизации. Для опечатывания конвертов (тубусов) должны применяться личные печати владельцев паролей (при их наличии у сотрудников Инспекции)

3. Внеплановая смена личного основного пароля или удаление учетной записи сотрудника Инспекции или системного администратора в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться системным администратором Инспекции немедленно после окончания последнего сеанса данного сотрудника.

4. В случае компрометации личного основного пароля сотрудника Инспекции должны быть немедленно предприняты меры в соответствии с п.5 настоящей Инструкции.

5. Хранение сотрудником Инспекции значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у системного администратора или начальника Инспекции в опечатанном личной печатью тубусе.

6. Несмотря на такие жесткие требования, есть несколько способов выбора паролей, которые соответствуют этим правилам:

- Выбрать предложение из песни или стихотворения, и отобрать только первые буквы каждого слова (хотя в примере использовано английское предложение, можно воспользоваться и другими языками):

Pretty woman walking down the street становится Pwwdts.

- Выбрать два коротких слова и соединить их с помощью пунктуационных знаков и специальных символов:

Dog+rain, kid<Goat, ТОРЛгапк, дождь+зонт, стол>телефон.

УТВЕРЖДЕНО
приказом начальника
Государственной
жилищной инспекции
Республики Татарстан

С.А. Крайнов

« 25 » сентября 2019 г. № 345

ЖУРНАЛ

скомпрометированных паролей и учетных записей, содержащих скомпрометированные пароли и учетные записи
Государственной жилищной инспекции Республики Татарстан

[illegible]

ЛИСТ ОЗНАКОМЛЕНИЯ

с Приказом ГЖИ РТ от 25.09.2019 № 345

«Об утверждении инструкции по организации парольной защиты
в Государственной жилищной инспекции Республики Татарстан»

(наименование структурного подразделения)

[illegible]