ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ И БЛАГОПОЛУЧИЯ ЧЕЛОВЕКА

Управление Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Красноярскому краю (Управление Роспотребнадзора по Красноярскому краю)

П Р И К А З

24 ИЮЛ 2023 № 253

г. Красноярск

Об информационной безопасности

В соответствии с Федеральными законами от 27.07.2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 06.04. 2011 № 63-ФЗ «Об электронной подписи», постановлением Правительства Российской Федерации от 21.03.2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» приказываю:

1. Утвердить:

1.1. Перечень локальных нормативно-правовых актов и иных документов Управления Роспотребнадзора по Красноярскому краю по информационной безопасности (далее – Перечень)(приложение № 1);

1.2. Правила по информационной безопасности для пользователя автоматизированного рабочего места Управления Роспотребнадзора по Красноярскому (далее – Правила)(приложение № 2);

1.3. Журнал ознакомления с локальными нормативно-правовыми актами и иными документами Управления Роспотребнадзора по Красноярскому краю по информационной безопасности (далее – Журнал)(приложение № 3).

2. Начальникам отделов и территориальных отделов:

2.1. Ознакомить государственных гражданских служащих с локальными нормативно-правовыми актами и иными документами Управления Роспотребнадзора по Красноярскому краю (далее – Управление) по информаци-

онной безопасности в соответствии с пп. 1.1-1.2 настоящего приказа;

2.2. Обеспечить соблюдение государственными гражданскими служащими Правил в соответствии с п. 1.2 настоящего приказа.

3. Начальникам отделов представить Журнал по форме из п. 1.3 настоящего приказа в отдел информационных технологий до 02.10.2023.

4. Начальникам территориальных отделов:

4.1. Организовать ведение и хранение Журнала по форме из п. 1.3 настоящего приказа в подразделении;

4.2. Направить копию Журнала в отдел информационных технологий до 02.10.2023 и ежегодно до 31 декабря календарного года при последующих изменениях кадрового состава подразделения.

5. Начальнику отдела информационных технологий А.А. Гилеву:

5.1. Организовать информирование сотрудников Управления по актуальным вопросам информационной безопасности;

5.2. Обеспечить ведение и хранение Журналов и копий Журналов в отделе информационных технологий после их получения от отделов и территориальных отделов Управления;

5.3. Обеспечить ознакомление сотрудников с локальными нормативно-правовыми актами и иными документами Управления по информационной безопасности при изменениях кадрового состава отделов Управления;

5.4. Обеспечить ежегодную актуализацию документов, предусмотренных пп. 1.1.-1.2. настоящего приказа.

6. Начальнику отдела государственной службы и кадров Е.А. Прохоровой обеспечить информирование отдела информационных технологий о кадровых изменениях в Управлении: о выходе сотрудников из длительных отпусков, о новых сотрудниках.

7. Начальнику отдела информационного сопровождения деятельности С.В. Лямченковой обеспечить размещение приказа на официальном Интернет-сайте Управления в разделе «Документы\ Документы Управления\Приказы».

8. Контроль за исполнением настоящего приказа возложить на заместителя руководителя А.Ю. Олейника.

Руководитель Д.В. Горяев

Приложение № 1
к Приказу
Управления Роспотребнадзора
по Красноярскому краю
от «24» 07 2023 г. № 254

Перечень локальных нормативно-правовых актов и иных документов по информационной безопасности

Приказы Управления по информационной безопасности

1. Приказ Управления № 138 от 11.04.2014 «О введении в действие формы согласия на обработку персональных данных гражданских служащих (работников) и формы обязательства гражданского служащего (работника) Управления Роспотребнадзора по Красноярскому краю».
2. Приказ Управления № 285 от 10.08.2016 «Об организации обработки персональных данных в Управлении Роспотребнадзора по Красноярскому краю».
3. Приказ Управления № 286 от 10.08.2016 «О создании службы по организации обработки и защиты персональных данных в Управлении Роспотребнадзора по Красноярскому краю».
4. Приказ Управления № 547 от 26.12.2016 «О внедрении Положения о порядке организации и проведения работ по защите конфиденциальной информации в Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека».
5. Приказ Управления № 562 от 28.12.2016 «Об упорядочении обращения со служебной информацией ограниченного распространения в Управлении».
6. Приказ Управления № 8 от 10.01.2017 «Об организации работ по защите конфиденциальной информации в Управлении Роспотребнадзора по Красноярскому краю».
7. Приказ Управления № 443 от 28.09.2017 «Об утверждении инструкций по обеспечению безопасности информационных систем».
8. Приказ Управления № 310 от 28.10.2017 «О внедрении инструкции по организации антивирусной защиты информации, обрабатываемой с применением средств вычислительной техники, в Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека».
9. Приказ Управления № 83 от 07.03.2019 «Об утверждении политики в отношении обработки персональных данных».
10. Приказ Управления № 85 от 12.03.2019 «О вводе в эксплуатацию информационных систем персональных данных».
11. Приказ Управления № 248 от 01.07.2022 «О назначении ответственных лиц за обеспечение кибербезопасности».

12. Приказ Управления № 432 от 09.12.2022 «Об оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

Письма Управления по информационной безопасности

1. Письмо Управления от 17.03.2017 № АЕ-18013 «О работе с персональными данными».
2. Письмо Управления от 29.09.2017 № ДВ-63203 «О мероприятиях по обеспечению безопасности информационных систем».
3. Письмо Управления от 22.04.2019 № ДВ-23859 «О компьютерной безопасности».
4. Письмо Управления от 30.08.2019 № ДВ-53906 «О работе с персональными данными».
5. Письмо Управления от 09.11.2022 № 24-00-14/12893-2022 «Об использовании веб-браузеров».

Приложение № 2
к Приказу
Управления Роспотребнадзора
по Красноярскому краю
от «24» 04 2023 г. № 254

Правила по информационной безопасности для пользователя автоматизированного рабочего места Управления Роспотребнадзора по Красноярскому краю

1) Правила работы с антивирусным программным обеспечением (антивирусное ПО):

- необходимо использовать исключительно лицензионное антивирусное ПО;
- обновление баз данных антивирусного ПО рекомендуется проводиться 1-го раз в неделю, но не реже 1 раза в месяц;
- необходимо использовать версии антивирусного средства сертифицированные ФСТЭК;
- запрещается отключать лицензионное антивирусное ПО;
- запрещается устанавливать и использовать стороннее программное обеспечение, в т.ч. и антивирусное ПО;
- необходимо обязательно проверять полученные по каналам связи файлы (в том числе по электронной почте и мессенджерам), съемные носители информации (флеш-накопители, CD, DVD диски и прочее).

2) Правила парольной защиты:

- учетные записи (совокупность имени пользователя/логина и пароля) должны быть персональными;
- пароли создаются и изменяются пользователями самостоятельно либо централизованно ответственным лицом;
- смену пароля рекомендуется производить 1 раз в 3 месяца, но не реже 1 раза в 6 месяцев;
- пароль необходимо формировать в соответствии с требованиями к формированию пароля инструкции по организации парольной защиты в информационных системах Управления Роспотребнадзора по Красноярскому краю, утвержденной приказом Управления № 443 от 28.09.2017 «Об утверждении инструкций по обеспечению безопасности информационных систем»;
- пароли необходимо хранить в тайне от посторонних лиц;
- после увольнение учетная запись пользователя должна быть заблокирована незамедлительно;
- разблокировка учетных записей осуществляется либо ответственным лицом, либо администратором информационной безопасности;
- автоматическая блокировка рабочего места должна производиться че-

рез 15 минут бездействия.

3) Правила работы с электронной почтой:

- запрещается использовать личные ящики электронной почты на рабочем месте;
- запрещается использовать служебные ящики электронной почты в личных целях;
- при получении электронных писем необходимо обязательно проверять отправителя (в том числе ответным письмом отправителю с запросом дополнительной информации с целью проверки реальности отправителя);
- запрещается открывать письма от неизвестных и сомнительных отправителей;
- запрещается открывать приложенные файлы и вводить защитные пароли к ним, полученные по электронной почте от неизвестных отправителей;
- запрещается открывать электронные письма, предназначенные не вам;
- запрещается открывать приложенные файлы с активным содержимым (например, макросы), полученные по электронной почте от неизвестных отправителей;
- запрещается переходить по ссылкам, полученным по электронной почте от неизвестных отправителей.

4) Правила работы с браузерами:

- к использованию допускаются только отечественные браузеры (В Управлении используется Яндекс Браузер);
- иностранные браузеры к использованию не допускаются и должны быть заблокированы;
- запрещается использование сторонних сайтов и ресурсов, не относящихся к рабочим, в сети Интернет.

5) Правила работы с носителями информации:

- не допускается подключение неучтенных внешних носителей, в том числе смартфонов и планшетных компьютеров без согласования с отделом информационных технологий к служебной компьютерной технике;
- обработка и хранение конфиденциальной информации осуществляется только на служебных носителях;
- использование внешних носителей допускается в соответствии с инструкцией по антивирусной защите информации.

6) Правила работы с носителями ключевой информации (например, Rutoken или eToken) и электронными подписями:

- запрещается пересылать файлы с ключевой информацией для работы в информационных системах по каналам связи, в том числе по электронной почте, сети Интернет, по внутренней электронной почте, мессенджерам и т.д., за исключением сертификатов проверки электронной подписи, которые

являются публичными;

- запрещается копировать файлы с ключевой информацией на сторонние носители информации, за исключением сертификатов проверки электронной подписи, которые являются публичными;

- в целях резервного копирования разрешается копировать файлы с ключевой информацией на учтенные носители информации, использующиеся исключительно для целей резервного копирования ключевой информации и при условии исключения доступа к носителю третьих лиц;

- запрещается предоставлять доступ к файлам с ключевой информацией посторонним лицам, за исключением сертификатов проверки электронной подписи, которые являются публичными;

- для доступа к ключевой информации, хранящейся не на ключевом носителе информации, необходимо использовать пароль, который возможно задать при генерации запроса на получение электронной подписи или при осуществлении резервного копирования ключевой информации;

- при использовании ключевого носителя информации необходимо установить пароль для доступа к ключевой информации, хранящейся на ключевом носителе информации;

- носители ключевой информации должны использоваться только их владельцем и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.);

- носитель ключевой информации должен быть вставлен в считывающее устройство (например, usb-порт) только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования, в иное время носитель ключевой информации должен быть извлечен;

- на носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

7) Правила работы с персональными данными:

- разрешается передача персональных данных с использованием каналов связи, защищенных в соответствии с требованиями регуляторов, таких как ФСТЭК и ФСБ;

- для передачи персональных данных разрешается использование факсимильной связи, почтовых отправлений;

- разрешается передача в зашифрованном виде в соответствии с требованиями регуляторов, таких как ФСТЭК и ФСБ;

- запрещается передача персональных данных в незашифрованном виде с использованием открытых каналов связи, в том числе по электронной почте, сети Интернет, по внутренней электронной почте, мессенджерам и т.д.;

- в помещения, где обрабатываются персональные данные, допускаются только сотрудники, уполномоченные на обработку персональных данных. Посторонние допускаются только в установленные часы приемы и в присутствии сотрудника, уполномоченного на обработку персональных данных;

- в помещениях, где хранятся персональные данные (в том числе носители персональных данных), должен быть исключен несанкционированный доступ.

Приложение № 3
к Приказу
Управления Роспотребнадзора
по Красноярскому краю
от «24» 04 2023 г. № 254

Журнал ознакомления с локальными нормативно-правовыми актами и иными документами Управления Роспотребнадзора по Красноярскому краю по информационной безопасности

№ п/п	ФИО	Должность	Подразделение	Дата	Подпись