РОССИЙСКАЯ ФЕДЕРАЦИЯ

РАСПОРЯЖЕНИЕ

ГЛАВЫ КАРАЧАЕВО-ЧЕРКЕССКОЙ РЕСПУБЛИКИ

О порядке создания и обеспечения технической защиты информации информационно-телекоммуникационной сети Администрации Главы и Правительства Карачаево-Черкесской Республики и органов исполнительной власти Карачаево-Черкесской Республики

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации», Доктриной информационной безопасности Российской Федерации», утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646:

1. Управлению Главы Карачаево-Черкесской Республики по технической защите информации и системному администрированию организовать создание и обеспечить техническую защиту информации информационно-телекоммуникационной сети Администрации Главы и Правительства Карачаево-Черкесской Республики и органов исполнительной власти Карачаево-Черкесской Республики (далее - ИТС КЧР) на базе технологии VipNet, действующей сети № 742 Администрации Главы и Правительства Карачаево-Черкесской Республики.

2. Образовать постоянно действующую комиссию по контролю за вводом в эксплуатацию, функционированием и обеспечением технической защиты информации ИТС КЧР согласно приложению 1.

3. Возложить на Управление Главы Карачаево-Черкесской Республики по технической защите информации и системному администрированию функции технического сопровождения и администрирования ИТС КЧР.

4. Утвердить Порядок работы в ИТС КЧР согласно приложению 2.

5. Управлению Главы и Правительства Карачаево-Черкесской Республики по кадровой политике и вопросам государственной гражданской службы организовать ознакомление с Порядком работы в ИТС КЧР государственных гражданских служащих в Администрации Главы и Правительства Карачаево-Черкесской Республики, а так же лиц, поступающих на государственную гражданскую службу в Администрацию Главы и Правительства Карачаево-Черкесской Республики, под роспись.

6. Руководителям органов исполнительной власти Карачаево-Черкесской Республики организовать ознакомление под роспись государственных гражданских служащих с Порядком работы в ИТС КЧР и обеспечить исполнение его требований.

7. Министерству финансов Карачаево-Черкесской Республики при формировании бюджета Карачаево-Черкесской Республики на очередной финансовый год и плановый период предусматривать бюджетные ассигнования на создание и обеспечение технической защиты информации ИТС КЧР.

8. Контроль за выполнением настоящего распоряжения возложить на Руководителя Администрации Главы и Правительства Карачаево-Черкесской Республики.

Глава
Карачаево-Черкесской Республики Р.Б. Темрезов

г.Черкесск
Дом Правительства
18 января 2019 года
№ 9-р

Приложение 1 к распоряжению
Главы Карачаево-Черкесской
Республики от 18.01.2019 № 9-р

С О С Т А В

постоянно действующей комиссии
по контролю за вводом в эксплуатацию, функционированием и обеспечением технической защиты информации информационно-телекоммуникационной сети Администрации Главы и Правительства Карачаево-Черкесской Республики и органов исполнительной власти Карачаево-Черкесской Республики

Руководитель Администрации Главы и Правительства Карачаево-Черкесской Республики, председатель комиссии;

начальник Управления Главы Карачаево-Черкесской Республики по технической защите информации и системному администрированию, секретарь комиссии;

Члены комиссии:

заместитель Руководителя Администрации Главы и Правительства Карачаево-Черкесской Республики, начальник Управления документационного обеспечения Главы и Правительства Карачаево-Черкесской Республики;

помощник Главы Карачаево-Черкесской Республики, курирующий вопросы технической защиты информации;

заместитель Министра финансов Карачаево-Черкесской Республики;

начальник Государственно-правового Управления Главы и Правительства Карачаево-Черкесской Республики.

Приложение 2 к распоряжению
Главы Карачаево-Черкесской
Республики от 18.01.2019 № 9-р

ПОРЯДОК РАБОТЫ

в информационно-телекоммуникационной сети Администрации Главы и Правительства Карачаево-Черкесской Республики и органов исполнительной власти Карачаево-Черкесской Республики

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Порядок работы в информационно-телекоммуникационной сети Администрации Главы и Правительства Карачаево-Черкесской Республики и органов исполнительной власти Карачаево-Черкесской Республики (далее - Порядок) предназначен и является обязательным для исполнения сотрудниками органов исполнительной власти Карачаево-Черкесской Республики (далее - органы исполнительной власти), Администрации Главы и Правительства Карачаево-Черкесской Республики (далее - Администрация) выполнение должностных обязанностей которых связано с использованием информационно-телекоммуникационной сети Администрации Главы и Правительства Карачаево-Черкесской Республики и органов исполнительной власти Карачаево-Черкесской Республики (далее - ИТС КЧР).

1.2. Порядок устанавливает правила обеспечения информационной безопасности в ИТС КЧР, распределение функций и ответственности за обеспечение информационной безопасности между структурными подразделениями Администрации и сотрудниками органов исполнительной власти, определяет их полномочия, обязанности и ответственность.

1.3. Основные термины и определения:

1.3.1. Администратор безопасности ИТС КЧР - сотрудник Управления Главы Карачаево-Черкесской Республики по технической защите информации и системному администрированию (далее – Управление Главы КЧР по ТЗИ и СА), отвечающий за поддержание работоспособности ИТС КЧР и разграничение доступа к информационным ресурсам этой сети.

1.3.2. Автоматизированное рабочее место (далее - АРМ) - рабочее место сотрудника Администрации, органа исполнительной власти, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных.

1.3.3. Информационная безопасность – состояние защищённости информационной среды, обеспечивающее минимизацию ущерба,

вызванного возможной утечкой защищаемой информации, а также несанкционированных и непреднамеренных воздействий.

1.3.4. ИТС КЧР - технологическая система, организованная на базе технологии VipNet, действующей сети № 742 Администрации, предназначенная для передачи информации по линиям связи, доступ к которой осуществляется с использованием средств вычислительной техники.

1.3.5. Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

1.3.6. Несанкционированный доступ - нарушение регламентированного доступа к объекту защиты.

1.3.7. Накопитель на жёстких магнитных дисках (далее - НЖМД) - энергонезависимое, перезаписываемое компьютерное запоминающее устройство. Является основным накопителем данных в персональных компьютерах.

1.3.8. Обработка информации – совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

1.3.9. Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для конфиденциальных переговоров.

1.3.10. Пользователь – сотрудник Администрации, органа исполнительной власти, выполнение должностных обязанностей которого связано с использованием АРМ в ИТС КЧР.

1.3.11. Системный администратор – штатный сотрудник органа исполнительной власти, в должностные обязанности которого входит техническое обслуживание и защита информации АРМ пользователей.

1.3.12. Сеть RSNet - элемент российской части информационно-телекоммуникационной сети Интернет, который включает в себя информационные системы и информационно-телекоммуникационные сети, находящиеся в ведении Федеральной службы охраны Российской Федерации.

1.3.13. Утечка информации - неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

1.4. Иные понятия и термины, используемые в настоящем порядке применяются в значениях, определенных федеральным законодательством.

1.5. Пользователи, администраторы безопасности ИТС КЧР и системные администраторы должны быть ознакомлены и знать нормативные правовые акты, касающиеся вопросов информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов, в части касающейся.

1.6. Руководители органов исполнительной власти, структурных подразделений Администрации в обязательном порядке организуют ознакомление пользователей своего подразделения с положениями настоящего Порядка.

2. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТС КЧР

2.1. Управление Главы КЧР по ТЗИ и СА осуществляет управление, общее руководство и контроль системы информационной безопасности ИТС КЧР и принятие всех решений по вопросам ее функционирования.

2.2. Руководители органов исполнительной власти, лица, ответственные за организацию работы по информационной безопасности, руководители структурных подразделений по вопросам технической защиты информации несут персональную ответственность за организацию системы информационной безопасности в органе исполнительной власти, структурном подразделении Администрации и решают следующие задачи:

2.2.1. Осуществляют руководство работой по обеспечению информационной безопасности в органе исполнительной власти, структурном подразделении Администрации.

2.2.2. Взаимодействуют с Управлением Главы КЧР по ТЗИ и СА по вопросам организации информационной безопасности.

2.3. Администратор безопасности ИТС КЧР:

2.3.1. Контролирует выполнение пользователями ИТС КЧР установленного порядка действий по доступу к объектам информационных систем.

2.3.2. Анализирует состояние используемых пользователями информационных систем с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации.

2.3.3. Контролирует правильность использования пользователями имеющихся средств информационной защиты.

2.3.4. Отслеживает с помощью специального программного обеспечения работу пользователей в сети ИТС КЧР. На основе логов проводится анализ по следующим параметрам:

перечень используемых ресурсов;

объем ежемесячного потребляемого пользователем интернет-трафика;

вирусная активность;

использование пользователями АРМ в служебных целях;

несанкционированные действия пользователей в ИТС КЧР.

2.3.5. Администратор безопасности ИТС КЧР в случае выявления каких-либо отклонений или нарушений в системе информационной безопасности ИТС КЧР обязан немедленно принять все меры к их устранению самостоятельно. Администратор безопасности ИТС КЧР несет персональную ответственность за принятие этих мер и сообщает о происшедшем руководителю органа исполнительной власти, руководителю структурного подразделения ответственного за техническую защиту информации, руководителю структурного подразделения Администрации и начальнику Управления Главы КЧР по ТЗИ и СА.

2.4. Системный администратор взаимодействует с Управлением Главы КЧР по ТЗИ и СА по вопросам обеспечения безопасности информации, при этом решает, в пределах своих полномочий, следующие задачи:

2.4.1. Осуществляет администрирование и защиту локальной вычислительной сети от несанкционированного доступа.

2.4.2. Составляет и ведет информационную схему сети (перечень программных продуктов, установленных на каждом из средств информатизации или доступных с этого средства в сети и информации, обрабатываемой этими программными продуктами; список сотрудников органа исполнительной власти, структурного подразделения Администрации с указанием закрепленных за ними средств информатизации и выделенных для них прав доступа).

2.4.3. Проводит информационные обследования сети, с целью составления полной информационной схемы объектов информатизации, помещений и пользователей сети. Обследование состоит в полной проверке всех имеющихся АРМ на наличие на них информации, средств информатизации, программных продуктов и составления комплекта документов, содержащих спецификацию этих средств с точки зрения информационной безопасности и закрепляющих их текущее состояние.

2.4.4. Эксплуатирует централизованные средства защиты информации в сети (при наличии).

2.4.5. Контролирует выполнение пользователями сети требований информационной безопасности и правильность эксплуатации пользовательских средств защиты информации (при наличии), принимает меры к устранению выявленных недостатков и сообщает о выявленных недостатках руководителю органа исполнительной власти, руководителю структурного подразделения Администрации и начальнику Управления Главы КЧР по ТЗИ и СА в письменной форме.

2.4.6. Выполняет технологические операции по предоставлению прав доступа к ресурсам сети пользователям, которым эти права предоставлены решениями руководителей органов исполнительной власти, структурных подразделений Администрации, согласованными с Управлением Главы

КЧР по ТЗИ и СА.

2.4.7. Взаимодействует с Управлением Главы КЧР по ТЗИ и СА по всем вопросам, указанным в настоящем пункте.

2.5. Пользователи ИТС КЧР несут персональную ответственность за соблюдение настоящего Порядка. Пользователи ИТС КЧР анализируют состояние своих АРМ с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации. В случае выявления таких попыток немедленно обязаны сообщить об этом администратору безопасности ИТС КЧР, своему непосредственному руководителю и системному администратору.

2.6. Контроль состояния информационной безопасности ИТС КЧР проводится с целью проверки ее организации, а также предупреждения и своевременного выявления случаев ее нарушения в следующем порядке:

2.6.1. Управление Главы КЧР по ТЗИ и СА проводит проверки организации и состояния информационной безопасности в органах исполнительной власти и структурных подразделениях Администрации;

2.6.2. Руководители органов исполнительной власти контролируют текущее состояние информационной безопасности в возглавляемых органах исполнительной власти.

2.6.3. Системный администратор ежедневно контролирует текущее состояние информационной безопасности в локальной вычислительной сети в пределах своих полномочий.

2.6.4. Пользователи ИТС КЧР контролируют текущее состояние информационной безопасности на своих АРМ.

2.7. Устанавливается следующий порядок действий в случае выявления нарушений информационной безопасности:

2.7.1. Действия, предпринимаемые в случае выявления нарушений информационной безопасности:

выявление факта нарушения;

прекращение всех операций, связанных с участком, на котором произошло нарушение, отключение АРМ от ИТС КЧР;

принятие экстренных мер для прекращения несанкционированного доступа или использования информации;

оповещение о нарушении;

восстановление работоспособности информационной системы;

расследование причин нарушения информационной безопасности;

проверка состояния информационной безопасности по факту нарушения.

2.7.2. Немедленно, после выявления нарушения, пользователь, его обнаруживший, обязан прекратить все операции по использованию информации и средств информатизации, которые выполнялись на участке, где произошло нарушение, а также, если необходимо, на смежных участках. Если выявлен несанкционированный доступ в категорированные помещения, всякий доступ в него должен быть прекращен.

2.7.3. Ответственность за адекватность принимаемых мер несут в по-

рядке привлечения пользователь, выявивший нарушение, системный администратор, руководитель органа исполнительной власти, структурного подразделения Администрации.

2.7.4. С целью минимизации ущерба от прекращения работы информационной системы, немедленно после того, как возможность дальнейшего нарушения информационной безопасности устранена, принимаются меры для восстановления ее работы. Решение на восстановление работы принимает руководитель органа исполнительной власти, структурного подразделения Администрации, на участке ответственности которого произошло нарушение, по согласованию с системным администратором, с уведомлением начальника Управления Главы КЧР по ТЗИ и СА.

2.7.5. Выявление причин нарушения информационной безопасности производится Управлением Главы КЧР по ТЗИ и СА. Пользователи ИТС КЧР обязаны оказывать содействие выявлению причин нарушения информационной безопасности. Целью является выявление истинных причин нарушения и предпосылок к нему для принятия мер к недопущению его повторения. Результаты в письменной форме предоставляются Руководителю Администрации, Председателю Правительства Карачаево-Черкесской Республики.

2.7.6. По факту нарушения Управлением Главы КЧР по ТЗИ и СА проводится проверка системы информационной безопасности ИТС КЧР на тех ее участках, где подобные нарушения возможны.

3.1. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯМ ИТС КЧР ДОСТУПА К СЕТИ ИНТЕРНЕТ

3.1. Подключение государственных информационных систем и информационно-телекоммуникационных сетей к сети Интернет осуществляется через сеть RSNet.

3.2. Подключение к сети Интернет пользователей осуществляется исключительно на АРМ с установленным лицензионным сертифицированным антивирусным программным обеспечением после ознакомления под роспись с настоящим Порядком, Памяткой абоненту сети RSNet по правилам работы в сети Интернет и о возможных последствиях обращения к ресурсам сети Интернет (приложение 1 к настоящему Порядку), Обязательствами пользователя сети RSNet (приложение 2 к настоящему Порядку).

3.3. Система контроля сети RSNet в ИТС КЧР предусматривает наличе следующих автоматических ограничений:

3.3.1. Запрет входа на сайты развлекательного характера.

3.3.2. Запрет определенных Интернет-протоколов.

3.3.3. Запрет доступа к icq, агенту mail.ru и другим интернет-пейджерам.

3.3.4. Запрет доступа к социальным сетям (odnoklassniki.ru, vkontakte.ru).

3.3.5. Запрет доступа к сайтам поиска работы (объявлений о вакансиях и резюме).

3.3.6. Автоматический отказ принимать вирусный файл, выявленный антивирусной проверкой интернет-трафика.

3.3.7. Запрет скачивания определенных типов файлов.

3.3.8. Автоматическое отключение пользователя и/или групп пользователей от ресурсов сети Интернет, при достижении ими лимита ежемесячного интернет-трафика.

3.4. Система контроля интернет-доступа осуществляет сбор статистики использования пользователей ресурсов сети Интернет. Данная статистика доступна администратору безопасности ИТС КЧР и может служить основанием отключения определенных ресурсов и принятия решений об изменении прав доступа пользователя к сети Интернет после согласования с начальником Управления Главы КЧР по ТЗИ и СА.

3.5. Доступ к ресурсам сети Интернет в ИТС КЧР предоставляется пользователю исходя из служебной необходимости после определения необходимых ограничений доступа (пункт 3.3. настоящего Порядка), на основании заявки руководителя органа исполнительной власти, структурного подразделения Администрации и резолюции Руководителя Администрации. Администратором безопасности ИТС КЧР оформляется учетная запись пользователя с назначением IP-адреса в ИТС КЧР и на прокси-сервере.

3.6. Изменение прав доступа и ограничений, а также подключение пользователя к сети Интернет после автоматического отключения (превышение лимита ежемесячного трафика), производится на основании письменного обращения руководителя органа исполнительной власти, структурного подразделения Администрации на имя начальника Управления Главы КЧР по ТЗИ и СА.

3.7. Пользователю ИТС КЧР запрещается:

3.7.1. Использовать ресурсы сети Интернет в неслужебных целях.

3.7.2. Посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтического характера, использовать доступ в Интернет в развлекательных целях.

3.7.3. Несанкционированно размещать какую-либо информацию в сети Интернет.

3.7.4. Использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом.

3.7.5. Подключаться к ресурсам сети Интернет через неслужебный канал доступа – сотовый телефон, USB-модем и другие устройства.

3.7.6. Несанкционированно загружать программы из сети Интернет и запускать их.

3.7.7. Осуществлять попытки несанкционированного доступа к защищенным ресурсам Интернет (перебор паролей, использование уязвимостей и неправильных настроек информационных систем).

3.7.8. Осуществлять несанкционированное туннелирование сетевого трафика при обращении к ресурсам сети Интернет через прокси-сервера и VPN сервера.

3.7.9. Использовать несанкционированное программное обеспечение мгновенного обмена сообщениями (InstantMessaging).

3.7.10. Использовать несанкционированные системы передачи голоса по IP-протоколу (VOIP).

3.7.11. Допускать к работе на АРМ посторонних лиц.

3.7.12. Изменять IP-адрес, определенный администратором безопасности ИТС КЧР.

3.7.13. Несанкционированно использовать компьютерные системы.

3.8. Администратор безопасности ИТС КЧР обязан:

3.8.1. Знать и правильно использовать аппаратно-программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств.

3.8.2. Производить подключение к сети Интернет только через шлюз безопасности (Ideco или аналогичные) в свою очередь подключенный только через Российский государственный сегмент информационно-телекоммуникационной сети Интернет (сеть RSNet) для обеспечения защиты сети.

3.8.3. Оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию.

3.8.4. Ежемесячно вести учет и анализ использования ресурсов сети Интернет по каждому пользователю, который по запросу предоставляется Председателю Правительства Карачаево-Черкесской Республики, Руководителю Администрации.

3.8.5. Информировать руководителей органов исполнительной власти, структурных подразделений Администрации о любых нарушениях требований настоящего Порядка и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

3.9. Администратор безопасности ИТС КЧР имеет право:

3.9.1. Запретить доступ пользователя к развлекательным сайтам и иным сайтам, не относящимся к исполнению пользователем служебных обязанностей.

3.9.2. При обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети, запретить доступ к сети Интернет данному пользователю.

4. ПОРЯДОК РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ

4.1. Служебная электронная почта предоставляется пользователям по заявке руководителя органа исполнительной власти, руководителя структурного подразделения в соответствии с резолюцией Руководителя Администрации и только для выполнения служебных обязанностей. Использование служебной электронной почты в личных целях запрещено.

4.2. Содержимое служебного электронного почтового ящика пользователя может быть проверено администратором безопасности ИТС КЧР без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

4.3. При работе со служебной электронной почтой пользователи должны обеспечить выполнение следующих правил:

4.3.1. Использовать служебную электронную почту только для передачи сообщений и документов (не программ).

4.3.2. Обработку электронных сообщений проводить исключительно на АРМ с установленным лицензионным антивирусным средством.

4.3.3. Не открывать и не обрабатывать электронные сообщения, заведомо не относящиеся к задачам, возложенным на служебный почтовый адрес.

4.3.4. Не осуществлять переход по ссылкам, содержащимся в тексте электронных сообщений. При этом, если электронное письмо получено от известных (доверенных) отправителей, это не является гарантией отсутствия фишинговых ссылок в тексте письма или вложения с вредоносным программным обеспечением (далее - ВПО). Отправители могут быть заражены ВПО, которое в автоматическом режиме рассылает электронные письма по списку контактов. В случае возникновения исключительной необходимости перехода по ссылке, вводить адрес легитимного сайта необходимо вручную в браузере АРМ.

4.3.5. Перед открытием файл вложения электронного письма необходимо скопировать на НЖМД АРМ и проверить его антивирусным средством. В случае наличия парольной защиты файла вложения (архивы, документы MicrosoftOffice), не производить действий по открытию файла и его обработке.

4.3.6. В случае наличия в электронном сообщении вложенных исполняемых файлов с расширениями: *.scr, *.lnk, *.exe, *.com, *.bat, *.cmd, *.vbs, не производить их загрузку и открытие.

4.3.7. Производить регулярное обновление программного обеспечения ПЭВМ, на которой происходит обработка сообщений электронной почты (например, JavaRuntimeEnvironment, AdobeFlashPlayer, AdobeReader).

4.3.8. В случае, если открытие почтового вложения сопровождается запросом о внесении изменений в программное обеспечение операционной системы, ошибкой прикладного программного обеспечения или вложение содержит неинформативный набор символов, необходимо прекратить его

обработку и направить данное почтовое сообщение на оптическом носителе информации в адрес Управления Главы КЧР по ТЗИ и СА.

4.3.9. Не допускается использование служебного почтового адреса для оформления подписок без предварительного согласования с руководителем органа исполнительной власти, структурного подразделения Администрации и администратором безопасности ИТС КЧР.

4.3.10. Не допускается использование почтовых программ, агентов, за исключением программ Outlook и MozillaThunderbird.

4.3.11. Не допускается отправление сообщений с вложенными файлами, общий объем которых превышает 16 Мегабайт. В случае если объем файлов для отправки превышает допустимый предел, документы необходимо архивировать или направлять частями.

4.3.12. Запрещается осуществлять массовую рассылку почтовых сообщений (более 20) внешним адресатам без их на то согласия.

4.3.13. Запрещается рассылать через служебную электронную почту:

материалы, содержащие вирусы или другие компьютерные коды;

файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, осуществления несанкционированного доступа;

серийные номера к коммерческим программным продуктам и программы для их генерации;

логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет;

ссылки на вышеуказанную информацию;

защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

информацию, содержание и направленность которой запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц;

информацию ограниченного доступа, составляющую государственную тайну.

4.4. Пользователям запрещено передавать сторонним лицам пароль доступа к своему служебному почтовому ящику, а также использовать публичные сервисы электронной почты (например mail.ru, hotmail.com, gmail.com) для осуществления служебных обязанностей.

5. ПОРЯДОК РАБОТЫ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

5.1. Под использованием съемных носителей информации в ИТС КЧР понимается их подключение к инфраструктуре ИТС КЧР с целью обработки, приема/передачи информации между АРМ и носителями информации.

5.2. В ИТС КЧР допускается использование только учтенных носителей информации, которые являются собственностью органа исполнительной власти и подвергаются регулярной ревизии и контролю.

5.3. К предоставленным органам исполнительной власти, структурным подразделениям Администрации носителям конфиденциальной информации предъявляются те же требования информационной безопасности, что и для стационарных АРМ.

5.4. Съемные носители информации предоставляются пользователям по инициативе руководителей органов исполнительной власти, руководителей структурных подразделений Администрации.

5.5. Все находящиеся на хранении и в обращении съемные носители со служебной, конфиденциальной информацией (персональными данными) в органе исполнительной власти, структурном подразделении Администрации подлежат учёту.

5.6. Каждый съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

5.7. Учет и выдачу съемных носителей информации осуществляют сотрудники органов исполнительной власти, структурных подразделений Администрации, на которых возложены функции хранения носителей информации. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей информации.

5.8. Сотрудники органа исполнительной власти, структурного подразделения Администрации получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении съемного носителя делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5.9. При использовании пользователями съемных носителей информации необходимо:

5.9.1. Соблюдать требования настоящего Порядка.

5.9.2. Использовать съемные носители информации исключительно для выполнения своих служебных обязанностей.

5.9.3. Ставить в известность системных администраторов о любых фактах нарушения требований настоящего Порядка.

5.9.4. Бережно относится к съемным носителям информации.

5.9.5. Обеспечивать физическую безопасность съемных носителей информации.

5.9.6. Извещать уполномоченного сотрудника органа исполнительной власти, структурного подразделения Администрации, системного администратора о фактах утраты (кражи) съемных носителей информации.

5.10. При использовании съемных носителей информации запрещено:

5.10.1. Использовать съемные носители информации в личных целях.

5.10.2. Передавать съемные носители информации другим лицам.

5.10.3. Оставлять без присмотра или передавать на хранение съемные носители информации другим лицам.

5.10.4. Передавать копии программ и данных, хранящихся в общедоступных каталогах, третьим лицам.

5.10.5. Выносить съемные носители информации из служебных помещений для работы с ними на дому.

5.11. Любое взаимодействие (обработка, прием/передача информации) инициированное пользователем между АРМ, входящим в ИТС КЧР и неучтенными, в том числе личными съемными носителями информации, рассматривается как несанкционированное. Администратор безопасности ИТС КЧР вправе блокировать или ограничивать использование таких съемных носителей информации.

5.12. Информация об использовании пользователем съемных носителей информации в ИТС КЧР протоколируется и, при необходимости, может быть предоставлена руководителям органов исполнительной власти, структурных подразделений Администрации, а также Руководителю Администрации, Председателю Правительства Карачаево-Черкесской Республики.

5.13. Информация, хранящаяся на служебных съемных носителях информации, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

5.14. В случае утраты или уничтожения съемных носителей информации, либо разглашении содержащихся в них сведений, немедленно ставится в известность руководитель соответствующего органа исполнительной власти, структурного подразделения Администрации. На утраченные съемные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей информации.

5.15. Съемные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей осуществляется соответствующей комиссией. По результатам уничтожения носителей составляется акт.

6. ПОРЯДОК РАБОТЫ С АНТИВИРУСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

6.1. К использованию в ИТС КЧР допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению.

6.2. Установка и настройка средств антивирусного контроля на компьютерах, серверах и рабочих станциях осуществляется системным администратором или Администратором безопасности ИТС КЧР.

6.3. Базы антивирусных средств должны обновляться в автоматическом режиме не реже одного раза в сутки.

6.4. Применение средств антивирусного контроля:

6.4.1. Полный антивирусный контроль всех дисков и файлов АРМ, а также серверов должен проводиться не реже чем раз в месяц.

6.4.2. Ежедневно, в начале рабочего дня при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль критических областей АРМ.

6.4.3. 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, лентах, CD - ROM). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

6.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

6.6. Установка (изменение) системного и прикладного программного обеспечения осуществляется системным администратором или администратором безопасности ИТС КЧР из списка, рекомендованного к использованию программного обеспечения.

6.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

6.8. 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), пользователь самостоятельно или вместе с лицом, ответственным за обеспечение безопасности информации, должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлекается системный администратор или администратор безопасности ИТС КЧР для определения ими факта наличия или отсутствия компьютерного вируса.

6.9. В случае обнаружения при проведении антивирусной проверки

зараженных компьютерными вирусами файлов, пользователи ИТС КЧР обязаны:

6.9.1. Приостановить работу и отключить компьютер от ИТС КЧР.

6.9.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения по технической защите информации, системного администратора, администратора безопасности ИТС КЧР.

6.9.3. Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

6.9.4. Провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности ИТС КЧР).

6.9.5. В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами (и необходимости сохранить данный файл), передать зараженный вирусом файл на CD диске администратору безопасности ИТС КЧР для дальнейшей отправки его в организацию, с которой заключен договор на антивирусную поддержку.

6.9.6. По факту обнаружения зараженных вирусом файлов направить в адрес начальника Управления Главы КЧР по ТЗИ и СА служебную записку, в которой указать предположительный источник (отправителя, владельца) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

7. ПОРЯДОК ПАРОЛЬНОЙ ЗАЩИТЫ

7.1. Личные пароли генерируются и распределяются централизованно системным администратором, либо выбираются пользователями самостоятельно с учетом следующих требований:

7.1.1. Пароль должен состоять не менее чем из восьми символов.

7.1.2. В пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров одновременно, содержать цифры от 0 до 9, содержать специальные символы, которые отличаются от букв и цифр (@, #, $, &, *, %), не содержать имени учетной записи пользователя длинной более двух рядом стоящих знаков.

7.1.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова), последовательности символов и знаков (111, qwerty, abcd), общепринятые сокращения (ЭВМ, ЛВС, USER), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе.

7.1.4. При смене пароля, новый пароль должен отличаться от старого не менее чем в шести позициях.

7.1.5. В случае, если формирование личных паролей пользователей

осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на системного администратора.

7.1.6. При технологической необходимости использования имен и паролей некоторых пользователей в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств) такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передать на хранение ответственному за информационную безопасность. Опечатанные конверты (пеналы) с паролями пользователей должны храниться в сейфе.

7.2. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами).

7.3. Порядок смены личных паролей:

7.3.1. Смена паролей проводится регулярно, не реже одного раза в два месяца.

7.3.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой. Администратор безопасности ИТС КЧР должен сменить пароль, либо отключить учетную запись данного пользователя.

7.3.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу) администраторов информационной системы и других сотрудников, которым по роду служебной деятельности были предоставлены полномочия по управлению системой парольной защиты.

7.3.4. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

7.4. Хранение пароля:

7.4.1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя структурного подразделения в опечатанном пенале.

7.4.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

7.4.3. Запрещается сообщать личный пароль другим пользователям и регистрировать их в системе под своим паролем.

8. ЛОКАЛИЗАЦИЯ СИСТЕМЫ ВИДЕОКОНФЕРЕНЦСВЯЗИ В ИТС КЧР

8.1. Система видеоконференцсвязи (далее – ВКС) предназначена для проведения совещаний, заседаний и иных мероприятий органов исполнительной власти Карачаево-Черкесской Республики с участием органов местного самоуправления. В случае необходимости и при наличии технической возможности допускается сопряжение системы ВКС с системами ВКС других органов и организаций.

8.2. Организацию технического сопровождения, администрирования и развития системы ВКС осуществляет Управление Главы КЧР по ТЗИ и СА.

9. ЛОКАЛИЗАЦИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ДЕЛОПРОИЗВОДСТВА «ДЕЛО» В ИТС КЧР

9.1. База данных системы электронного документооборота и делопроизводства «Дело» (далее - СЭД «Дело») и серверная часть программного обеспечения располагается на серверах Администрации Главы и Правительства КЧР.

9.2. Доступ к серверу СЭД «Дело» осуществляется через ИТС КЧР.

9.3. За функционирование, обслуживание и техническое сопровождение серверов несет ответственность уполномоченный сотрудник Управления документационного обеспечения Главы и Правительства Карачаево-Черкесской Республики.

9.4. Обеспечение защиты каналов связи в СЭД «Дело» осуществляет Управление Главы КЧР по ТЗИ и СА.

10. ОТВЕТСТВЕННОСТЬ

За нарушение требований настоящего Порядка пользователь ИТС КЧР может быть отключен от ИТС КЧР и привлечен к ответственности в соответствии с действующим законодательством.

Приложение 1 к Порядку

ПАМЯТКА

пользователю ИТС КЧР по правилам работы в сети Интернет и о возможных последствиях обращения к ресурсам сети Интернет

1. В сетях связи и на АРМ, с которых ведется работа в сети Интернет, запрещается обработка сведений, составляющих государственную тайну, служебной информации ограниченного распространения, а также для которой установлены особые правила доступа.

2. Для осуществления сеанса работы в сети Интернет необходимо использовать только лицензионное программное обеспечение программ-клиентов доступа к информационным ресурсам сети.

Изменение конфигурации программного обеспечения программ-клиентов доступа к информационным ресурсам сети может проводиться системным администратором.

3. При получении файлов из сети Интернет их необходимо обработать антивирусными средствами.

При этом необходимо учитывать, что особую опасность представляют исполняемые файлы программ, доступные из конференций UseNet (особенно *.warez, *.cracks, *.hack) и на FTP-серверах, на которых распространяется нелицензионное («пиратское») программное обеспечение, а также программные средства «взлома» и нелегальной регистрации коммерческого программного обеспечения. В этих файлах могут содержаться программные закладки, программы типа «троянского коня» и другие деструктивные программы.

Во избежание утечки, искажения или разрушения обрабатываемой информации, а также повреждения операционной среды и прикладных программ не рекомендуется получать из сети Интернет исполняемые файлы программ и осуществлять их запуск.

Группа администрирования узла сети RSNet и Управление Главы КЧР по ТЗИ и СА не несут ответственности за последствия использования программных средств самостоятельно полученных пользователями по сети Интернет.

4. На некоторых WWW и FTP серверах для получения доступа к хранящейся на них информации предлагается пройти регистрацию. При этом просят ответить на ряд вопросов, касающихся названия организации, рода деятельности, круга творческих и производственных интересов. В этом случае работу с таким сервером рекомендуется прекратить.

5. Запрещается осуществлять подключение АРМ пользователя к сети Интернет в категорированных помещениях, кроме случаев, разрешенных законодательством Российской Федерации.

6. Необходимо ответственно относиться к хранению своей учетной информации (идентификатор пользователя, пароль) и не использовать электронную почту для пересылки подобной информации. В случае получения писем (даже от имени Администрации сети RSNet) с требованием выслать подобную информацию, необходимо обратиться к Администрации сети RSNet.

В случае компрометации паролей пользователь обязан немедленно оповестить Управление Главы КЧР по ТЗИ и СА.

7. Несанкционированное использование компьютерных систем, неправомерный доступ к компьютерной информации, нарушение правил эксплуатации АРМ, систем АРМ или их сетей, а также создание, использование и распространение вредоносных программ для АРМ влечет уголовную и гражданскую ответственность, предусмотренную законодательством Российской Федерации.

8. Администрация сети RSNet имеет право прекратить предоставление услуг в следующих случаях:

распространения пользователем информации, оскорбляющей честь и достоинство других пользователей и персонала компьютерных сетей;

попытки получить несанкционированный доступ к компьютерам сети Интернет с использованием собственных сетевых реквизитов;

несанкционированного сканирования пользователем любого диапазона IP-адресов;

массового распространения в сети не запрошенных адресатами материалов помимо телеконференций, соответствующих этим материалам;

нарушения авторских прав на информацию, представленную в сети;

намеренного нанесения ущерба другим лицам;

вмешательство в действия других пользователей или обслуживающего персонала (например, несанкционированный доступ к компьютерам и информационным источникам);

внесения в учетную систему ИТС КЧР при регистрации ложной персональной и адресной информации.

Приложение 2 к Порядку

ОБЯЗАТЕЛЬСТВА
пользователя сети RSNet

1. Общий принцип.

Сеть RussianStateNetwork (далее - RSNet) является корпоративной подсетью сообщества сетей Интернет, включающей в себя информационные ресурсы федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, и может быть использована для информационного взаимодействия и взаимного доступа к информационным ресурсам ее участников, а также для доступа к информационным ресурсам сети Интернет.

2. Области допустимого использования сети RSNet:

2.1. Обмен информацией в соответствии с пунктом 1, с организациями, как российскими, так и зарубежными, вне зависимости от того, какой транспортной средой передачи данных они пользуются.

2.2. Получение различного рода данных из любых источников, необходимых для повышения эффективности деятельности органов государственной власти, а также для повышения профессионального уровня их сотрудников.

2.3. Проведение социологических, статистических и других исследований, если это не связано с применением их результатов в коммерческих или военных целях.

2.4. Осуществление деловой переписки.

2.5. Доступ к российским и международным информационным ресурсам.

3. Сеть RSNet запрещается использовать:

3.1. Для осуществления коммерческой деятельности, кроме той, которая направлена исключительно на развитие собственной материальной базы телекоммуникационных узлов, подключенных к сети RSNet.

3.2. Для нужд частного бизнеса и личных целей.

3.3. Для любого рода коммерческой рекламы.

3.4. Для несанкционированного доступа к информационно-вычислительным и сетевым ресурсам, принадлежащим другим пользователям или сетям.

3.5. Для совершения действий (DDoS-атаки, генерация паразитного трафика), которые могут привести к нарушению функционирования сети и сетевых ресурсов.

3.6. Для публикации или передачи информации, или программного обеспечения, которое содержит в себе компьютерные «вирусы» или способно нарушить штатную работу оборудования.

3.7. Для деятельности, противоречащей национальным интересам Российской Федерации.

3.8. Для совершения действий, запрещенных законодательством Российской Федерации.

3.9. Для подключения к сети Интернет информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, и служебная информация ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам.

4. Ответственность пользователя.

Пользователь обязуется использовать услуги сети только легальным образом и не переносить на администрацию узла сети RSNet ответственность за ущерб любого рода, понесенный пользователем или третьей стороной в ходе использования услуг сети RSNet.

4.1. Пользователь отвечает за содержание передаваемой им информации.

4.2. Пользователь несет ответственность за разглашение паролей и другой конфиденциальной информации о порядке доступа и использования сети RSNet.

4.3. Пользователь, в случае делегирования ему субдомена сети RSNet, отвечает за непрерывную работу сервиса DNS (непрерывной работой считается работа, при которой суммарное время отсутствия связи с сервером не превышает двух часов в сутки).

4.4. Администрация узла сети RSNet оказывает содействие пользователю по тестированию и восстановлению канала связи.

4.5. Пользователь должен своевременно оповещать администрацию узла сети RSNet обо всех изменениях в работе своих пользователей (изменение названия организации, структурного подразделения, адреса размещения автоматизированного рабочего места, замены ответственных лиц, отключении от сети RSNet).