АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
«БОЛЬШЕКЛЮЧИЩЕНСКОЕ СЕЛЬСКОЕ ПОСЕЛЕНИЕ»
УЛЬЯНОВСКОГО РАЙОНА УЛЬЯНОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

13.05.2020г. № 35

с. Большие Ключищи

Об утверждении Положения
о порядке организации и проведения
работ по защите конфиденциальной
информации в Администрации
МО «Большеключищенское
сельское поселение»

В соответствии с ч. 4 ст. 16 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановляет:

1. Утвердить Положения о порядке организации и проведения работ по защите конфиденциальной информации в Администрации МО «Большеключищенское сельское поселение» (приложение № 1).
2. Утвердить Инструкцию пользователя по обеспечению информационной безопасности в Администрации МО «Большеключищенское сельское поселение» (приложение № 2).
3. Настоящее постановление вступает в силу на следующий день после дня его обнародования.
4. Контроль за выполнением настоящего постановления оставляю за собой.

Глава администрации
МО «Большеключищенское
сельское поселение» А.А. Дмитриев

Приложение № 1
к постановлению администрации
муниципального образования
«Большеключищенское сельское поселение»
от 13.05.2020г. № 35

Положение о порядке организации и проведения работ по защите конфиденциальной информации в Администрации МО «Большеключищенское сельское поселение»

1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в администрации МО «Большеключищенское сельское поселение» (далее - Администрация).

1.2. Мероприятия по защите конфиденциальной информации являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Информационные системы и ресурсы, являющиеся собственностью государства, подлежат обязательному учету и защите.

1.4. Режим защиты конфиденциальной информации устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством.

1.5. Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке. Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для технической защиты конфиденциальной информации.

1.6.Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении. Для сведений, составляющих служебную тайну не ниже требований, установленных данным документом и государственными стандартами Российской Федерации.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.7. Объектами защиты являются:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию - далее основные технические средства и системы (ОТСС);

- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальной информация - далее

вспомогательные технические средства и системы (ВТСС);

- помещения (служебные кабинеты, актовые, конференц-залы и т.п.), специально предназначенные для проведения конфиденциальных мероприятий – защищаемые помещения (ЗП).

1.8. Ответственность за выполнение требований настоящего Положения возлагается на Главу администрации, начальников отделов, а также на специалистов Администрации, допущенных к обработке, передаче и хранению на технических средствах информации, содержащей конфиденциальную информацию (далее – уполномоченные сотрудники).

2. Охраняемые сведения

2.1. Сведения, составляющие конфиденциальную информацию, определяются Перечнем сведений конфиденциального характера в соответствии с Указом Президента РФ от 6 марта 1997 года №188.

2.2. К охраняемым сведениям, защищаемым информационным ресурсам и процессам на всех этапах жизненного цикла объектов информатизации администрации относятся:

- речевая информация, содержащая сведения конфиденциального характера;
- информационные ресурсы, содержащие сведения конфиденциального характера, представленные в виде бумажных носителей информации, носителей на магнитной и оптической основе, информативных электрических сигналов, информационных массивов и баз данных.

2.3. К объектам информатизации администрации, подлежащим защите по требованиям обеспечения безопасности защиты информации, относятся:

- защищаемые помещения, в которых обсуждается информация, содержащая сведения конфиденциального характера, утечка, которой может нанести ущерб администрации, персоналу, материальным ценностям или отдельным гражданам.
- системы информатизации и связи, предназначенные для обработки информации, содержащей сведения конфиденциального характера:
  - локальные вычислительные сети (далее – ЛВС) и отдельные автоматизированные рабочие места (далее - АРМ);
  - средства изготовления, размножения и тиражирования документов;
  - программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);
  - система звукоусиления и звукозаписи, предназначенная для использования при проведении совещаний по конфиденциальным вопросам;
  - средства связи;
- вспомогательные технические средства и системы (далее - ВТСС), размещенные в защищаемых помещениях, а также совместно с техническими средствами и системами, обрабатывающими информацию конфиденциального характера.

3. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее.

3.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

– несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;

– утечки конфиденциальной информации по техническим каналам.

4.Оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации

4.1. Для добывания конфиденциальных сведений могут использоваться:

- портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН);

- автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;

- компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

Угроза компьютерной разведки объектам защиты возможна в случае подключения АС, обрабатывающим информацию ограниченного доступа к внешним, в первую очередь - глобальным сетям.

Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи зданий.

Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных, или перехвата информации в непосредственной близости от защищаемых объектов.

Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

4.2. Несанкционированный доступ к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.

4.3. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

– непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций, защищаемых помещений и их инженерно-технических систем;

– случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;

– некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;

– просмотра информации с экранов дисплеев и других средств ее отображения.

4.4. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов Федеральной служба по техническому и экспортному контролю (далее - ФСТЭК России).

Наиболее опасной является аппаратура портативной (возимой и носимой) разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям администрации территорий, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.

4.5. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием следующих руководящих документов ФСТЭК России:

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по технической защите конфиденциальной информации.

НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к конфиденциальной информации и режимов

обработки данных в автоматизированных системах.

5. Организационные и технические мероприятия по технической защите конфиденциально информации

5.1. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

5.2. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

5.3. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на специалиста, эксплуатирующего объекты информатизации.

5.4. Техническая защита информации в защищаемых помещениях.

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

5.4.1. Определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки), в соответствии с нормативными документами ФСТЭК России.

5.4.2. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

5.4.3. Обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения. Инструктирование сотрудников, работающих в ЗП о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

5.5.5. Проведение в ЗП обязательных визуальных (непосредственно перед совещаниями) и инструментальных (перед ответственными совещаниями и периодически раз в квартал) проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов, подарков, сувениров и прочих предметов, оставляемых в ЗП.

5.5.6. Исключение неконтролируемого доступа к линиям связи, управления и сигнализации в ЗП, а также в смежных помещениях и в коридоре.

5.5.7. Оснащение телефонных аппаратов городской АТС, расположенных в ЗП, устройствами высокочастотной развязки подавления слабых сигналов, а также поддержание их в работоспособном состоянии. Для спаренных телефонов достаточно одного устройства на линию, выходящую за пределы ЗП.

5.5.8. Осуществление контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах.

5.5.9. Обеспечение требуемого уровня звукоизоляции входных дверей ЗП.

5.5.10. Обеспечение требуемого уровня звукоизоляции окон ЗП.

5.5.11. Демонтирование или заземление (с обеих сторон) лишних (незадействованных) в ЗП проводников и кабелей.

5.5.12. Отключение при проведении совещаний в ЗП всех неиспользуемых электро- и радиоприборов от сетей питания и трансляции.

5.5.13. Выполнение перед проведением совещаний следующих условий:

- окна должны быть плотно закрыты и зашторены;
- двери плотно прикрыты.

5.6. Защита информации, циркулирующей в ОТСС и наводящейся в ВТСС.

5.6.1. При эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию.

5.6.2. При невозможности обеспечения контролируемой зоны заданных размеров рекомендуется проведение следующих мероприятий:

- применение систем электромагнитного пространственного зашумления (СПЗ) в районе размещения защищаемого ОТСС;
- применение средств линейного электромагнитного зашумления (СЛЗ) линий

электропитания, радиотрансляции, заземления, связи.

5.6.3. Техническая защита информации в средствах вычислительной техники (СВТ) и автоматизированных системах (АС) от несанкционированного доступа в соответствии с требованиями руководящих документов ФСТЭК России должна обеспечиваться путем:

проведения классификации СВТ и АС;

выполнения необходимых организационных мер защиты;

установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД;

защита каналов связи, предназначенных для передачи конфиденциальной информации;

защиты информации от воздействия программ-закладок и компьютерных вирусов.

5.7. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами ФСТЭК России.

Организации антивирусной защиты информации на объектах информатизации достигается путём:

установки и применения средств антивирусной защиты информации; обновления баз данных средств антивирусной защиты информации;

действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

5.7.1. Защита информации от воздействия программных вирусов на объектах информатизации должна специалистами Администрации осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

к использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства;

входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения;

входной антивирусный контроль всей информации поступающей с электронной почтой;

входной антивирусный контроль всей поступающей информации из сети Internet;

выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;

периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

обязательная антивирусная проверка используемых в работе внешних носителей информации;

постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;

обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

5.7.2. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

5.7.3. При обнаружении на носителе информации или в полученных файлах

программных вирусов пользователи принимают меры по восстановлению работоспособности программных средств и данных:

о факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов;

перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов;

при обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты;

при функционировании АРМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети;

5.7.4. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

5.7.5. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

5.8. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на уполномоченных сотрудников.

5.8.1. Личные пароли должны генерироваться с учетом следующих требований:

- длина пароля должна быть не менее 7 символов. В числе символов пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

- пароль не должен включать в себя легко вычисляемые сочетания символов (логины, имена, фамилии и т.д.), а также общепринятые сокращения (персональный компьютер, ЛВС, USER и т.п.).

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях.

Владельцы паролей 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.

5.8.2. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

5.8.3. Полная плановая смена паролей пользователей должна проводиться регулярно, 1 раз в 90 дней.

5.8.4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.8.5. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.5.8.4 настоящего положения.

5.8.6 Хранение уполномоченным сотрудником значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором Touch Memory).

6. Обязанности и права должностных лиц

6.1. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

6.2. Владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения докладываются Главе администрации.

6.3. Специалист по пожарной безопасности по согласованию с Главой администрации привлекает к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

7. Контроль состояния технической защиты конфиденциальной информации

7.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня и эффективности, принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

Контроль осуществляется пользователями – непрерывно.

7.2. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, наличия соответствующих документов по технической защите конфиденциальной информации, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.

8. Взаимодействие с предприятиями, учреждениями и организациями

8.1. При проведении совместных работ с предприятиями, учреждениями и организациями должна быть обеспечена техническая защита информации, составляющей конфиденциальную или служебную тайну, независимо от места проведения работ.

8.2. В технических заданиях на выполнение совместных работ с использованием конфиденциальной информации, должны быть предусмотрены требования (или меры) по ее технической защите, которые должны выполняться каждой из сторон. Технические задания на выполнение совместных работ согласовываются с руководителем аппарата и программистом – системным администратором и взаимодействующими предприятиями (учреждениями, организациями).

8.3. Организация технической защиты информации возлагается на руководителей совместных работ, а ответственность за обеспечение технической защиты информации - на исполнителей работ (пользователей) при использовании ими технических средств для обработки и передачи информации, подлежащей защите.

Приложение № 2
к постановлению администрации
муниципального образования
«Большеключищенское сельское поселение»
от 13.05.2020г. № 35

Инструкция пользователя по обеспечению информационной безопасности в Администрации МО «Большеключищенское сельское поселение»

1. Общие положения

1.1. Настоящая Инструкция определяет основные обязанности и ответственность пользователя, допущенного к обработке конфиденциальной информации.

1.2. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность конфиденциальной информации и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. Основные обязанности пользователя:

2.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные законодательством РФ, внутренними документами организации и настоящей Инструкцией.

2.2. При работе с конфиденциальной информацией располагать во время работы экран видео монитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами.

2.3. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, базам данных, файлам и другим носителям конфиденциальной информацией при ее обработке.

2.4. После окончания обработки конфиденциальной информации в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска персонального компьютера.

2.5. В случае выявления инцидентов информационной безопасности (фактов или попыток несанкционированного доступа к информации, обрабатываемой в персональном компьютере или без использования средств автоматизации) немедленно сообщить об этом Главе администрации МО «Большеключищенское сельское поселение», принять участие в служебной проверке по данному инциденту.

2.6. Самостоятельно не устанавливать на персональный компьютер какие-либо аппаратные или программные средства.

2.7. Знать штатные режимы работы программного обеспечения, основные пути проникновения и распространения компьютерных вирусов.

2.9. Помнить личные пароли и персональные идентификаторы, хранить их в тайне, не оставлять без присмотра носители, их содержащие, и хранить в запирающемся ящике стола или сейфе. С установленной периодичностью менять свой пароль (пароли).

2.10. При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов средствами персонального компьютера.

2.11. Знать и строго выполнять правила работы с установленными на его персональном компьютере средствами защиты информации (антивирус, средства разграничения доступа, средства криптографической защиты и т.п.) в соответствии с технической документацией на эти средства.

2.12. Передавать для хранения установленным порядком свое индивидуальное устройство идентификации (Touch Memory , Smart Card , Proximity и т.п.), другие реквизиты разграничения доступа и носители ключевой информации только непосредственному

руководителю либо специалисту по делопроизводству и кадрам для хранении в сейфе.

2.13. Надежно хранить и никому не передавать личную печать.

2.14. Немедленно ставить в известность непосредственного руководителя при обнаружении:

нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к закрепленной за ним защищенном персональном компьютере;

некорректного функционирования установленных на персональный компьютер технических средств защиты;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию персонального компьютера, выхода из строя или неустойчивого функционирования узлов персонального компьютера или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения.

2.15. По завершении работ по изменению аппаратно-программной конфигурации, закрепленной за ним персонального компьютера проверять его работоспособность.

3. Обеспечение антивирусной безопасности

3.1.Основными путями проникновения вирусов в информационно-вычислительную сеть организации являются: съемные носители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные персональные компьютеры.

3.2. При возникновении подозрения на наличие компьютерного вируса (сообщение антивирусной программы, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль персонального компьютера.

3.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь ОБЯЗАН:

прекратить (приостановить) работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя;

оценить необходимость дальнейшего использования файлов, зараженных вирусом;

провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь работника организации, с которой заключен договор на обслуживание программного обеспечения).

3.4. Пользователю ЗАПРЕЩАЕТСЯ:

отключать средства антивирусной защиты информации;

без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

4. Обеспечение безопасности конфиденциальной информации, персональных данных

4.1. Каждый работник организации, участвующий в процессах обработки конфиденциальной информации, персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и базам данных системы организации, является пользователем и несет персональную ответственность за свои действия.

4.2. Пользователь ОБЯЗАН:

знать требования руководящих документов по защите конфиденциальной информации, персональных данных;

производить обработку защищаемой информации в строгом соответствии с утвержденными технологическими инструкциями;

строго соблюдать установленные правила обеспечения безопасности конфиденциальной информации, персональных данных при работе с программными и

техническими средствами.

4.3. Пользователю ЗАПРЕЩАЕТСЯ:

использовать компоненты программного и аппаратного обеспечения не по назначению (в неслужебных целях);

использовать средства разработки и отладки программного обеспечения стандартных программных средств общего назначения (MS Office и др.);

самовольно вносить какие-либо изменения в конфигурацию аппаратно — программных средств персонального компьютера или устанавливать дополнительно любые программные и аппаратные средства;

осуществлять обработку конфиденциальной информации, персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

записывать и хранить конфиденциальную информацию, персональные данные на неучтенных съемных носителях информации (гибких магнитных дисках, флэш — накопителях и т.п.), осуществлять несанкционированную распечатку конфиденциальной информации, персональных данных;

оставлять включенной без присмотра свой персональный компьютер, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, носители и распечатки, содержащие конфиденциальную информацию, персональные данные;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям безопасности конфиденциальной информации, персональных данных.

5. Обеспечение информационной безопасности при использовании ресурсов сети Интернет

5.1. Ресурсы сети Интернет могут использоваться для осуществления выполнения требований законодательства Российской Федерации, дистанционного обслуживания, получения и распространения информации, связанной с деятельностью организации (в том числе, путем создания информационного web-сайта), информационно-аналитической работы в интересах организации, обмена почтовыми сообщениями, а также ведения собственной хозяйственной деятельности. Иное использование ресурсов сети Интернет, решение о котором не принято руководством организации в установленном порядке, рассматривается как нарушение информационной безопасности.

5.2. С целью ограничения использования сети Интернет в неустановленных целях выделяется ограниченное число пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей. Наделение работников организации правами пользователя конкретного пакета выполняется в соответствии с его должностными обязанностями.

5.3.Особенности использования сети Интернет:

сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;

гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом не предоставляются.

5.4. При осуществлении электронного документооборота, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет организация применяет соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

5.5. Почтовый обмен конфиденциальной информацией через сеть Интернет осуществляется с использованием защитных мер.

5.6. Электронная почта организации подлежит периодической архивации. Доступ к архиву разрешен только должностному лицу в организации, ответственному за работу с электронной почтой. Изменения в архиве не допускаются.

5.7. При взаимодействии с сетью Интернет Администрация обеспечивает специалиста программными и аппаратными средствами противодействие атакам хакеров и распространению спама.

5.8. При пользовании ресурсами сети Интернет ЗАПРЕЩАЕТСЯ:

использовать на рабочем месте иные каналы доступа персонального компьютера к сети Интернет, кроме установленного;

проводить самостоятельное изменение конфигурации технического и программного обеспечения персонального компьютера, подключенной к сети Интернет;

осуществлять отправку электронных почтовых сообщений, содержащих конфиденциальную информацию, по открытым каналам;

использовать иные, кроме служебных, почтовые ящики для электронной переписки;

открывать файлы, пришедшие вместе с почтовым сообщением, если не известен источник этого сообщения;

осуществлять перенос полученной по сети Интернет документированной информации в электронном виде на другие компьютеры без проверки ее антивирусными программами;

скачивать из сети Интернет, в том числе средствами электронной почты, информацию, содержащую исполняемые модули, программы, драйверы и т.п., без предварительной проверки антивирусными средствами;

использовать сеть Интернет вне служебных задач, посещать интернет – сайты, не связанные с выполнением должностных обязанностей.

6. Порядок работы с носителями ключевой информации

6.1. Работнику учреждения (владельцу ключа электронной подписи (далее – ЭП)), которому в соответствии с его должностными обязанностями предоставлено право постановки на электронных документах его ЭП, выдается персональный ключевой носитель информации, на который записана уникальная ключевая информация (ключ ЭП), относящаяся к категории сведений ограниченного распространения.

6.2. Ключевые носители маркируются соответствующими этикетками, на которых отражается: регистрационный номер носителя и, при возможности размещения, дата изготовления и подпись уполномоченного сотрудника, изготовившего носитель, вид ключевой информации — эталон или рабочая копия, фамилия, имя, отчество и подпись владельца ключа ЭП.

6.3. Персональные ключевые носители (эталон и рабочую копию) владелец ключа ЭП должен хранить в специальном месте, гарантирующем их сохранность.

6.4. Ключи проверки ЭП установленным порядком регистрируются специалистом по делопроизводству и кадрам в справочнике «открытых» ключей, используемом при проверке подлинности документов по установленным на них ЭП.

6.5. Владелец ключа ОБЯЗАН:

под подпись в «Журнале учета ключевых носителей» получить ключевые носители, убедиться, что они правильно маркированы и на них установлена защита от записи;

использовать для работы только рабочую копию своего ключевого носителя;

сдавать свой персональный ключевой носитель на временное хранение непосредственному руководителю или специалисту по делопроизводству и кадрам в период отсутствия на рабочем месте (например, на время отпуска или командировки);

в случае порчи рабочей копии ключевого носителя (например, при ошибке чтения) владелец ЭП обязан обратиться в специализированную организацию для изготовления новой рабочей копии. Испорченная рабочая копия ключевого носителя должна быть

уничтожена владельцем ключа.

6.6. Владельцу ключа ЭП ЗАПРЕЩАЕТСЯ:

оставлять ключевой носитель без личного присмотра;

передавать свой ключевой носитель (эталонную или рабочую копию) другим лицам (кроме как для хранения непосредственному руководителю или специалисту по делопроизводству и кадрам);

делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск персонального компьютера), снимать защиту от записи, вносить изменения в файлы, находящиеся на ключевом носителе;

использовать ключевой носитель на заведомо неисправном дисководе и/или персональном компьютере;

подписывать своим персональным ключом ЭП любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;

сообщать третьим лицам информацию о владении ключом ЭП для данного технологического процесса.

6.7. Действия при компрометации ключей

6.7.1. Если у владельца ключа ЭП появилось подозрение, что его ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом непосредственному руководителю, сделать пометку в журнале учета ключевых носителей о причине компрометации, написать служебную записку о факте компрометации персонального ключевого носителя на имя непосредственного руководителя, уничтожить скомпрометированный ключевой носитель.

6.7.2. В случае утери ключевого носителя владелец ключа ЭП обязан немедленно сообщить непосредственному руководителю, написать объяснительную записку об утере ключевого носителя на имя Главы администрации, принять меры по блокированию ключа для ЭП и принять участие в служебной проверке по факту утери ключевого носителя.

6.7.3. По решению Главы администрации установленным порядком владелец ключа ЭП может получить новый комплект персональных ключевых носителей взамен скомпрометированных.

6.7.4. В случае перевода владельца ключа ЭП на другую работу, увольнения или прекращения трудовых отношений иным образом он обязан сдать (сразу по окончании последнего сеанса работы) свой ключевой носитель специалисту по делопроизводству и кадрам под подпись в журнале учёта.

7. Организация парольной защиты

7.1. Пароль для своей учетной записи пользователь устанавливает самостоятельно.

7.2. Запрещается использовать пароль домена локальной вычислительной сети (вводится при загрузке персонального компьютера) для входа в иные автоматизированные системы.

7.2. Длина пароля должна быть не менее 7 символов. В числе символов пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

7.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (логины, имена, фамилии и т.д.), а также общепринятые сокращения (персональный компьютер, ЛВС, USER и т.п.).

7.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях.

7.5. Пользователь обязан хранить в тайне свой личный пароль.

7.6. Пользователь должен проводить полную плановую смену паролей 1 раз в 90 дней.

8. Ответственность пользователей

8.1. Работники Администрации несут ответственность согласно действующему законодательству, за разглашение сведений, составляющих служебную, коммерческую и иную охраняемую законом тайну (в том числе персональные данные) и сведений ограниченного распространения, ставших им известными по роду работы.

8.2. Нарушения установленных правил и требований по обеспечению информационной безопасности являются основанием для применения к работнику (пользователю) мер наказания, предусмотренных трудовым законодательством.