#

# ВОЛОГОДСКАЯ ОБЛАСТЬ

**КОНТРОЛЬНО-СЧЕТНАЯ ПАЛАТА ГОРОДА ЧЕРЕПОВЦА**

**ПРИКАЗ**

**ПРЕДСЕДАТЕЛЯ КОНТРОЛЬНО-СЧЕТНОЙ ПАЛАТЫ ГОРОДА ЧЕРЕПОВЦА**

01.04.2014 № 14

Об утверждении Положения,

инструкций, форм расписок

по защите информации в

контрольно-счетной палате города Череповца

В соответствии с федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», 27 июля 2006 года № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии при Президенте Российской Федерации от 30 августа 2002 года № 282

ПРИКАЗЫВАЮ:

 1. Утвердить

 Положение о порядке организации и проведения работ по защите информации ограниченного доступа, не относящейся к государственной тайне, в контрольно-счетной палате города Череповца (приложение 1);

 Инструкцию по организации учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, в контрольно-счетной палате города Череповца (приложение 2);

 Инструкцию по организации обработки информации ограниченного доступа, не относящейся к государственной тайне, в электронном виде в контрольно-счетной палате города Череповца (приложение 3);

 Инструкцию пользователя персональным компьютером и компьютером, подключенным к локальной вычислительной сети контрольно-счетной палаты города Череповца (приложение 4);

 Инструкцию по организации антивирусной защиты на объектах информатизации контрольно-счетной палаты города Череповца (приложение 5);

 форму расписки о неразглашении информации ограниченного доступа, не относящейся к государственной тайне (сведений конфиденциального характера) и иной служебной информации (приложение 6);

 форму расписки при увольнении с работы о неразглашении информации ограниченного доступа, не относящейся к государственной тайне (сведений конфиденциального характера) и иной служебной информации (приложение 7).

 2. Заместителю председателя контрольно-счетной палаты города Череповца М.В.Усатовой ознакомить муниципальных служащих контрольно-счетной палаты города Череповца с настоящим приказом под роспись.

 3. Контроль за исполнением настоящего приказа возложить на заместителя председателя контрольно-счетной палаты города Череповца М.В.Усатову.

Председатель С.С.Ивахненко

Приложение 1

к приказу председателя

контрольно-счетной палаты

города Череповца

от 01.04.2014 № 14

ПОЛОЖЕНИЕ

о порядке организации и проведения работ по защите информации ограниченного доступа, не относящейся к государственной тайне,

в контрольно-счетной палате города Череповца

1. Сокращения и определения, используемые в настоящем Положении

ФСТЭК – Федеральная служба по техническому и экспортному контролю России.

АС – автоматизированная система.

СВТ – средства вычислительной техники.

ЛВС – локальная вычислительная сеть.

Аттестация объектов информатизации – комплекс организационно-технических мероприятий, в результате которых аттестатом соответствия подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по требованиям безопасности информации, утвержденных Гостехкомиссией России и ФСТЭК.

Система защиты информации (далее – СЗИ) – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Конфиденциальная информация – информация ограниченного доступа, не относящаяся к государственной тайне.

К сведениям конфиденциального характера в контрольно-счетной палате города Череповца относится информация, соответствующая Перечню сведений конфиденциального характера, утвержденному Указом Президента России от 6 марта 1997 года № 188.

МУ «ЦМИРиТ» – муниципальное учреждение «Центр муниципальных информационных ресурсов и технологий».

2. Общие положения

Положение определяет содержание и порядок осуществления мероприятий по защите конфиденциальной информации на объектах информатизации контрольно-счетной палаты города Череповца (далее – контрольно-счетная палата).

Ограничение доступа к информации устанавливается федеральными законами. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Требования настоящего Положения являются обязательными для исполнения всеми специалистами контрольно-счетной палаты при организации и проведении работ на данных объектах информатизации, связанных с обработкой сведений конфиденциального характера.

Мероприятия по защите конфиденциальной информации являются неотъемлемой составной частью деятельности на объектах информатизации контрольно-счетной палаты.

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 информации и величины ущерба, который может быть нанесен обладателю информационных ресурсов.

Объектами информатизации контрольно-счетной палаты являются АС, ЛВС, средства и системы связи и передачи информации, другие технические средства, используемые для обработки, хранения, размножения и передачи информации, а также помещения для ведения конфиденциальных переговоров.

Защита информации на объектах информатизации контрольно-счетной палаты достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также обеспечения работоспособности технических средств.

Основное внимание при обеспечении информационной безопасности контрольно-счетной палаты уделяется защите информации, в отношении которой угрозы безопасности реализуются без применения сложных технических средств, а именно информации:

обрабатываемой СВТ от несанкционированного доступа и несанкционированных действий;

выводимой на экраны мониторов;

хранящейся на физических носителях;

передаваемой по каналам связи, выходящим за пределы контролируемой зоны.

Подключение объектов информатизации контрольно-счетной палаты к сети «Интернет» осуществляется через МУ «ЦМИРиТ», где установлен сертифицированный межсетевой экран (Check Point). Необходимость и порядок подключения осуществляется по заявке составленной заместителем председателя контрольно-счетной палаты.

Организация защиты информации на объектах информатизации возлагается на заместителя председателя контрольно-счетной палаты.

 Непосредственное выполнение работ по защите информации на объектах информатизации контрольно-счетной палаты возлагается на заместителя председателя контрольно-счетной палаты.

3. Порядок определения защищаемой информации

В рамках настоящего Положения к защищаемой информации относится документированная конфиденциальная информация, обрабатываемая на объектах информатизации контрольно-счетной палаты, созданная ими или полученная от юридических или физических лиц на законных основаниях.

В соответствии с пунктом 4 статьи 8 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» не может быть ограничен доступ к:

нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

информации о состоянии окружающей среды;

информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Обоснование конфиденциальности и степени важности отдельных документов, создаваемых на объектах информатизации контрольно-счетной палаты, осуществляется председателем контрольно-счетной палаты.

4. Порядок привлечения специализированных сторонних организаций

к разработке и эксплуатации объектов информатизации и системы

защиты информации контрольно-счетной палаты, их задачи и функции на различных стадиях создания и эксплуатации объектов информатизации

Разработка объектов информатизации, в которых предполагается обрабатывать конфиденциальную информацию, осуществляется в соответствии с требованиями действующих нормативных документов по технической защите конфиденциальной информации, в том числе в соответствии с требованиями ГОСТ Р 51583-00, ГОСТ Р 51624-00.

Порядок привлечения специализированных организаций к разработке и эксплуатации объектов информатизации контрольно-счетной палаты, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации определяются при заключении двухсторонних договоров между объектами информатизации контрольно-счетной палаты и специализированными организациями.

Аттестация объектов информатизации контрольно-счетной палаты по требованиям безопасности информации осуществляется в соответствии с требованиями ФСТЭК.

5. Ответственность должностных лиц за своевременность и качество

формирования требований по защите информации, качество

и научно-технический уровень разработки СЗИ

5.1. Должностными лицами, ответственными за организацию, осуществление работ по защите информации в контрольно-счетной палате, являются:

председатель контрольно-счетной палаты;

заместитель председателя контрольно-счетной палаты.

5.2. Председатель контрольно-счетной палаты:

утверждает организационно-технические и другие документы по вопросам защиты информации;

принимает решения о финансировании мероприятий по защите информации;

координирует годовое и перспективное планирование мероприятий по защите информации;

организует разработку необходимых организационно-технических мероприятий по защите информации;

оценивает эффективность принимаемых мер защиты информации и организует работы по устранению выявленных недостатков;

в случае выявления нарушений, в результате которых имелось или имеется реальная возможность утечки конфиденциальной информации по техническим каналам, принимает решение о временном прекращении обработки информации.

5.3. Заместитель председателя контрольно-счетной палаты:

осуществляет подбор и внедрение комплекса организационных (режимных) и технических мер по защите информации;

осуществляет консультативную, методическую и техническую помощь по вопросам защиты информации;

участвует в рассмотрении проектов технических заданий на проектирование объектов информатизации в части полноты и достаточности требований и мероприятий по технической защите информации;

осуществляет контроль (в пределах своей компетенции) за выполнением требований правовых актов Российской Федерации, Вологодской области, контрольно-счетной палаты, нормативно-технических и методических документов в сфере обеспечения требований безопасности информации;

участвует в проведении контроля эффективности принятых мер по защите информации;

обеспечивает своевременную подготовку документов по категорированию и технической паспортизации объектов информатизации;

участвует в проведении разбирательств по фактам нарушений установленного порядка и правил защиты информации;

анализирует причины и условия появления нарушений по защите информации и вносит предложения по их устранению и предупреждению, контролирует устранение выявленных нарушений;

участвует в проведении работ (с привлечением сертифицированных специалистов) по подбору, монтажу, настройке и техническому обслуживанию средств и СЗИ;

осуществляет выполнение мероприятий по защите информации в соответствии с требованиями правовых актов и методических документов в области защиты информации;

обеспечивает запуск и бесперебойную работу технических и программно-аппаратных средств защиты информации на объектах информатизации;

проводит техническое обслуживание аппаратных СЗИ в соответствии с эксплуатационно-технической документацией;

проводит мероприятия по антивирусной защите ЛВС;

проводит резервное копирование информационных массивов контрольно-счетной палаты;

контролирует целостность ЛВС, ограничивает доступ к оборудованию, кабельному хозяйству и серверам;

устраняет аварийные ситуации в работе ЛВС, проверяет работоспособность СЗИ после восстановления работоспособности сети;

по указанию председателя контрольно-счетной палаты устанавливает новые версии разрешенного к эксплуатации общесистемного и специального программного обеспечения по защите информации и обеспечивает их сопровождение на серверах и отдельных рабочих станциях;

организовывает подключение новых пользователей к ЛВС, разграничивает права доступа к защищаемым информационным ресурсам контрольно-счетной палаты;

проводит смену паролей;

обеспечивает защиту информации от несанкционированного доступа;

выявляет и устраняет причины несанкционированного доступа к информационным ресурсам контрольно-счетной палаты.

Приложение 2

к приказу председателя

контрольно-счетной палаты

 города Череповца

от 01.04.2014 № 14

Инструкция

по организации учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, в контрольно-счетной палате города Череповца

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне (далее – конфиденциальная информация) в контрольно-счетной палате города Череповца (далее – контрольно-счетная палата).

1.2. Ответственность за организацию учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения конфиденциальной информации (далее – машинных носителей данных), возлагается на муниципальное учреждение «Центр муниципальных информационных ресурсов и технологий» (далее – МУ «ЦМИРиТ»).

1.3. Все машинные носители данных, используемые для обработки и хранения конфиденциальной информации, подлежат обязательной регистрации в журнале учета (далее – журнал учета), хранящемся МУ «ЦМИРиТ».

2. Учет машинных носителей данных

2.1. К машинным носителям данных относятся:

гибкие магнитные диски (ГМД);

оптические и магнитооптические диски (ОД);

флэш-карты;

съемные жесткие магнитные диски (СЖМД);

несъемные жесткие магнитные диски (НЖМД).

2.2. Каждому машинному носителю данных присваивается учетный номер, состоящий из кода машинного носителя и порядкового номера по журналу учета.

2.3. Учетный номер и гриф «конфиденциально» наносятся на машинный носитель информации. При невозможности маркировать непосредственно машинный носитель маркируется упаковка – корпус, в котором он хранится. В этом случае учетный номер записывается также на носитель машинным способом.

2.4. Несъемные жесткие магнитные диски закрепляются за специалистом контрольно-счетной палаты, ответственным за эксплуатацию средства вычислительной техники, в котором они установлены.

2.5. В случае повреждения или утраты машинных носителей данных, содержащих конфиденциальную информацию, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся заместителю председателя контрольно-счетной палаты.

2.6. Копирование конфиденциальной информации с машинных носителей данных производится специалистом МУ «ЦМИРиТ», постоянно работающим с данной копируемой информацией.

3. Порядок уничтожения машинных носителей данных, предназначенных

для обработки и хранения информации ограниченного доступа,

не относящейся к государственной тайне

3.1. Конфиденциальная информация, хранящаяся на машинных носителях данных, утратившая практическое значение или пришедшая в негодность, своевременно уничтожается по решению председателя контрольно-счетной палаты.

3.2. Уничтожение машинных носителей данных, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения с оформлением акта и записью в журнале учета. Перед уничтожением носителя информация с него должна быть стерта (уничтожена), если это позволяют физические принципы работы носителя.

3.3. После снятия с материального учета, машинные носители данных подлежат уничтожению.

Приложение 3

к приказу председателя

контрольно-счетной палаты

города Череповца

от 01.04.2014 № 14

Инструкция

 по организации обработки информации ограниченного доступа, не относящейся

к государственной тайне, в электронном виде в контрольно-счетной палате города Череповца

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации обработки информации ограниченного доступа, не относящейся к государственной тайне (далее – конфиденциальная информация), в контрольно-счетной палате города Череповца (далее – контрольно-счетная палата).

1.2. Ответственность за организацию обработки конфиденциальной информации возлагается на заместителя председателя контрольно-счетной палаты.

 1.3. Порядок доступа к данным при их накоплении, хранении и обработке на средствах вычислительной техники (далее – СВТ) устанавливает заместитель председателя контрольно-счетной палаты.

1.4. Ответственность за проведение мероприятий по разграничению доступа и защите информации несут председатель контрольно-счетной палаты, заместитель председателя контрольно-счетной палаты.

2. Обязанности специалистов контрольно-счетной палаты, обрабатывающих конфиденциальную информацию

2.1. Специалисты контрольно-счетной палаты допускаются к работе с конфиденциальной информацией только после инструктажа, проведенного заместителем председателя контрольно-счетной палаты, изучения и проверки знания настоящей Инструкции и следующих документов:

 Инструкции пользователя персональным компьютером и компьютером, подключенным к локально-вычислительной сети контрольно-счетной палаты.

 Инструкции по организации учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения конфиденциальной информации в контрольно-счетной палате.

 Инструкции по организации антивирусной защиты на объектах информатизации контрольно-счетной палаты.

2.2. Специалисты контрольно-счетной палаты, работающие с конфиденциальной информацией, обязаны:

строго соблюдать настоящую Инструкцию;

не допускать посторонних лиц к работе на установленных у них СВТ;

при выходе из кабинета не оставлять в нем посторонних лиц, блокировать клавиатуру и дисплей СВТ;

выполнять правила хранения машинных носителей данных, содержащих конфиденциальную информацию;

2.3. Специалистам контрольно-счетной палаты при работе с конфиденциальной информацией запрещается:

работать с конфиденциальной информацией в присутствии посторонних лиц;

сообщать сведения о характере обрабатываемой информации лицам, не допущенным к данной информации;

сообщать, кому бы то ни было сведения о характере выполняемой работы на СВТ, о применяемых системах защиты информации (если это не вызвано служебной необходимостью);

использовать незарегистрированные машинные носители;

работать с неучтенными экземплярами полученных на СВТ конфиденциальных документов;

делать на машинных носителях информации (или на их упаковках) надписи, раскрывающие содержание этих носителей;

самостоятельно уничтожать магнитные носители;

устанавливать на СВТ программное обеспечение без разрешения заместителя председателя контрольно-счетной палаты;

деинсталлировать или отключать установленное программное обеспечение без разрешения заместителя председателя контрольно-счетной палаты;

самостоятельно перемещать СВТ;

сообщать посторонним лицам свой пароль доступа к СВТ;

оставлять незапертой дверь в кабинет, в случае отсутствия в нем сотрудников контрольно-счетной палаты;

оставлять посторонних лиц в кабинете, где осуществляется обработка конфиденциальной информации.

3. Требования к размещению, обслуживанию СВТ и организация работы с конфиденциальной информацией.

3.1. СВТ размещаются в рабочих кабинетах специалистов контрольно-счетной палаты.

3.2. Помещения, где размещены СВТ, должны быть оборудованы охранной и пожарной сигнализациями, иметь средства защиты окон и дверей от несанкционированного проникновения в помещение.

3.3. Сетевые печатающие устройства, используемые при обработке конфиденциальной информации, необходимо располагать в помещениях ограниченного доступа.

3.4. Портативные СВТ в нерабочее время должны храниться в специальных шкафах (сейфах), которые запираются на ключ.

3.5. На СВТ должно инсталлироваться и использоваться только лицензионное, сертифицированное программное обеспечение.

3.6. В случае подключения СВТ в локальной вычислительной сети необходимо использовать аппаратно-программные средства контроля доступа к хранимой и обрабатываемой информации, исключающие возможность несанкционированного доступа к данным и нарушения их целостности.

3.7. Конфиденциальные данные, поступившие на магнитных носителях информации, перед обработкой на СВТ подлежат обязательной проверке антивирусными средствами.

4. Ответственность за нарушение правил работы с конфиденциальной информацией

4.1. Ответственность за соблюдение конфиденциальности при накоплении, хранении и обработке информации на СВТ возлагается на специалистов контрольно-счетной палаты, в чьем пользовании находятся СВТ.

4.2. Ответственность за соблюдение правил работы с конфиденциальной информацией возлагается на специалистов контрольно-счетной палаты, занимающихся ее обработкой.

4.3. Лица, виновные в нарушении правил работы с конфиденциальной информацией, несут ответственность в соответствии с законодательством Российской Федерации.

Приложение 4

к приказу председателя

контрольно-счетной палаты города Череповца

от 01.04.2014 № 14

Инструкция

пользователя персональным компьютером и компьютером, подключенным

к локально-вычислительной сети контрольно-счетной палаты города Череповца

1. Общие положения

 1.1. Настоящая Инструкция разработана в целях обеспечения успешной, длительной, безопасной эксплуатации персонального компьютера (далее – ПК) и совместного с ним оборудования.

 1.2. В настоящей Инструкции определяется порядок работы на ПК и в локально-вычислительных сетях (далее – ЛВС) контрольно-счетной палаты города Череповца (далее – контрольно-счетная палата).

 ЛВС – это комплекс технических и программных средств, обеспечивающих совместный доступ к базам данных, обмен информацией в электронном виде между специалистами контрольно-счетной палаты, получение и обмен информацией посредством подключения к удаленным ресурсам.

 ПК, подключенный к ЛВС контрольно-счетной палаты, – это пользовательский компьютер, оснащенный коммутационным устройством (сетевой адаптер, контроллер удаленного доступа), обеспечивающим подключение к серверам и другим персональным компьютерам контрольно-счетной палаты.

 1.3. Настоящая Инструкция является документом, обязательным для исполнения всеми специалистами контрольно-счетной палаты, использующими в своей деятельности средства электронно-вычислительной техники.

 1.4. Специалисты контрольно-счетной палаты допускаются к работе с ПК, подключенными к ЛВС контрольно-счетной палаты, только после ознакомления с настоящей инструкцией и проведенного инструктажа заместителем председателя контрольно-счетной палаты.

2. Руководство по эксплуатации

 2.1. Назначение ПК.

 ПК, укомплектованный необходимыми внешними устройствами, является средством автоматизации индивидуального труда при решении широкого круга задач в различных профессиональных сферах, как в автономном режиме, так и при подключении к ЛВС, глобальным информационным сетям («Интернет»), а также в режиме интеллектуального терминала и информационных вычислительных систем.

 2.2. Состав ПК.

 Основной состав ПК: системный блок, монитор, устройства ввода и вывода информации, дополнительные внешние периферийные устройства.

 2.3. Меры безопасности при работе на ПК.

 2.3.1. В целях личной безопасности и во избежание повреждения ПК запрещается:

 допускать перегибы, зажимы, скручивание, повреждение электропитающих шнуров и соединительных кабелей ПК;

 подключать к сетевому фильтру, от которого запитана ПК, отопительные приборы, электрические чайники и другое бытовое оборудование;

 при включенном компьютере отсоединять сетевые и интерфейсные кабели;

 эксплуатировать компьютер со снятой крышкой корпуса;

 закрывать системный блок, монитор, другие периферийные устройства посторонними вещами во избежание перегрева;

 вставлять различные предметы в вентиляционные отверстия системного блока и монитора, класть скрепки, другие предметы, которые могут попасть внутрь ПК;

 устанавливать в непосредственной близости к ПК горшки с цветами, вазы или графины с водой;

 размещать вблизи компьютеров и на них бытовые приборы с большими электромагнитными полями (вентиляторы, телевизоры и тому подобное);

 чистить компьютер при включенном электропитании системного блока, монитора и периферийных устройств

 использовать для чистки ПК ацетон, бензин, спиртосодержащие жидкости.

 2.3.2. При неисправности ПК незамедлительно сообщать об этом заместителю председателя контрольно-счетной палаты. Ремонт ПК осуществляется только специалистами МУ «ЦМИРиТ».

 2.4. Порядок включения компьютера.

 Сначала рекомендуется включить питание периферийных устройств (принтера, монитора и так далее), а затем включается питание системного блока.

 При наличии источника бесперебойного питания (далее – ИБП) вначале осуществляется включение ИБП, его тестирование, потом – включение питания системного блока.

 При включении питания начинается самотестирование. После завершения самотестирования выполняется загрузка операционной системы.

 Для подключения к ЛВС наберите регистрационное имя и пароль (при необходимости нужно переключить раскладку клавиатуры на английский язык).

 2.5. Порядок выключения компьютера.

 Выключение ПК производится в следующем порядке: закрываются все выполняемые программы, выключаются периферийные устройства. Затем необходимо выполнить команды: «Пуск», «Завершение работы», «Выключить компьютер».

 Во избежание повреждения программных продуктов, установленных в ПК, и потери информации запрещается выключать или перезагружать компьютер во время проведения операций чтения-записи (горит хотя бы один из индикаторов обращения к дисковым накопителям), во время работы, когда выполняется одна из программ.

 Повторное включение ПК должно производиться не ранее чем через 20 секунд после выключения.

 2.6. Обслуживание ПК.

 Специалист контрольно-счетной палаты, работающий на ПК, ежедневно должен следить за чистотой на рабочем месте. Раз в неделю проводить чистку монитора, клавиатуры, периферийных устройств специальными салфетками.

3. Организация работы на ПК в ЛВС контрольно-счетной палаты:

 3.1. Порядок предоставления доступа к ЛВС контрольно-счетной палаты.

 Для работы в ЛВС каждый пользователь должен получить соответствующий доступ. Под доступом понимается имя и пароль учетной записи ПК рабочего места пользователя.

 Доступ пользователей к работе в ЛВС контрольно-счетной палаты организует заместитель председателя контрольно-счетной палаты.

 О всех нарушениях в работе на ПК в ЛВС контрольно-счетной палате пользователи докладывают незамедлительно заместителю председателя контрольно-счетной палаты.

 3.2. Обязанности специалистов контрольно-счетной палаты, использующих ПК, подключенные к ЛВС:

 знать правила безопасности работы в ЛВС и меры по защите информационных ресурсов (в части, касающейся выполнения ими должностных обязанностей);

 рассматривать выполнение обязанностей по защите ЛВС контрольно-счетной палаты как обязательное условие доступа для работы в сети;

 при работе на своей рабочей станции и в ЛВС выполнять только служебные задания;

 начиная работу убедиться в исправности своего компьютера и отсутствия «вирусов» (использовать антивирусную защиту);

 при работе с посторонними лицами закрывать (сворачивать) программы и документы, чтобы избежать нежелательного ознакомления посторонних лиц с ними;

 при сообщениях тестовых программ о появлении «вирусов» немедленно сообщать об этом заместителю председателя контрольно-счетной палаты;

 обо всех неисправностях в работе ПК, периферийных устройств, ЛВС, программных средств сообщать заместителю председателя контрольно-счетной палаты;

 в случае использования гибких магнитных носителей (дискеты) и других носителей (флэш-карты) проводить проверку этих носителей на отсутствие «вирусов»;

 незамедлительно выполнять предписания и указания заместителя председателя контрольно-счетной палаты;

 предоставлять свой компьютер для контроля заместителю председателя контрольно-счетной палаты.

 3.4. Специалистам контрольно-счетной палаты запрещается:

 сообщать либо передавать свой личный пароль посторонним лицам, записывать пароль на компьютере или еще где-либо, если это создает возможность постороннему человеку узнать его;

 допускать к работе на компьютере посторонних лиц;

 сообщать дополнительную информацию о настройках и параметрах сети, серверов, телефонах дозвона и тому подобное кому бы то ни было;

 сообщать сведения о применяемых системах защиты информации, используемых серверных операционных системах контрольно-счетной палаты;

 предпринимать попытки доступа к информации и ресурсам, на которые у него нет разрешения;

 самостоятельно вскрывать корпус (снимать крышку системного блока), устанавливать и подключать дополнительные платы, модули, подключать дополнительные сетевые и интерфейсные кабели, порты ввода-вывода (USB), дополнительное оборудование;

 самостоятельно устанавливать, деинсталлировать программные продукты;

 модифицировать настройки сетевого окружения и операционной системы, менять настройки базовой системы ввода-вывода (BIOS), отключать антивирусную защиту;

 устанавливать дополнительные пароли на включение компьютера и доступа к его ресурсам;

 приносить и использовать средства электронно-вычислительной техники (ноутбук, ПК, карманный компьютер и тому подобное) граждан и организаций, подключать данные устройства к ЛВС контрольно-счетной палаты;

 использовать информацию, предоставленную на магнитных носителях, флеш-картах или полученную из сети «Интернет», без ее предварительной проверки антивирусными программами;

 переносить ПК в другие места расположения, менять и переставлять с компьютера на компьютер различные периферийные устройства (принтеры, сканеры и тому подобное);

 срывать пломбы (печати) на ПК, периферийных устройствах;

 менять самостоятельно провода подключения к ПК, осуществлять прокладку дополнительных проводов.

4. Ответственность

 Ответственность за эксплуатацию ПК, периферийных устройств, подключенных к данной ПК и соблюдение правил работы на них несет специалист контрольно-счетной палаты, в чьем пользовании находятся данные устройства.

 Пользователь ЛВС, виновный в нарушении законодательства Российской Федерации о неправомерном доступе к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в ПК или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ПК или их сети, несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 5

к приказу председателя

контрольно-счетной палаты города Череповца

от 01.04.2014 № 14

Инструкция

по организации антивирусной защиты

на объектах информатизации контрольно-счетной палаты города Череповца

1. Общие положения

Настоящая инструкция определяет требования к организации защиты автоматизированной системы (далее – АС) контрольно-счетной палаты города Череповца (далее – контрольно-счетной палаты) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность специалистов контрольно-счетной палаты, эксплуатирующих и обслуживающих АС, за их выполнение.

2. Схема построения антивирусной защиты

2.1. Технологическая схема отражает технические решения по следующим вопросам организации антивирусной защиты информации в контрольно-счетной палаты:

внедрение средств антивирусной защиты информации;

порядок обновления баз данных средств антивирусной защиты информации;

действия специалистов контрольно-счетной палаты при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

2.2. Настоящая инструкция разработана на основе:

Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Положения о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 года № 912-51;

Постановления Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации»;

Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 9 сентября 2000 года № Пр-1895.

3. Определение компьютерных вирусов и антивирусных средств

3.1. Типы вирусов.

3.1.1. Компьютерный вирус – фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом. Дублируя себя, вирус заражает другие программы. Вирус выполняется только при запуске главной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и искажению данных и программ.

3.1.2. Загрузочный вирус – компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера. Позволяет злоумышленнику полностью перехватить управление компьютером, либо активизируется, саморазрушая операционную систему и всю имеющуюся в компьютере информацию.

3.1.3. Файловый вирус – компьютерный вирус, прикрепляющий себя к файлу или программе и активизирующийся при каждом использовании файла, заражая другие открываемые пользователем файлы или программы.

3.1.4. Кроме вирусов опасность представляют программы-троянцы. В отличие от вирусов такие программы самостоятельно не размножаются, а обычно маскируются под полезные программы (например, просмотр рисунков, удобное средство работы с файловой системой и так далее). Кроме основной функции, программы-троянцы осуществляют скрытые функции, наносящие вред пользователю. При работе в локальных вычислительных сетях (далее – ЛВС) и сети «Интернет» программы-троянцы могут передавать злоумышленникам имена и пароли для авторизованного входа в систему пользователя, а так же файлы, документы с компьютера пользователя, следить за работой пользователя и полностью управлять его компьютером (стирать, изменять, записывать программы и файлы, включать, выключать компьютер и тому подобное).

3.2. Пути распространения вирусов.

Наиболее часто вирусы распространяются при копировании файлов с одного компьютера на другой. Если переписываемый файл оказался зараженным, то при его активации возможно заражение других файлов компьютера, в том числе системных. Файлы обычно переносятся с использованием дисков (гибких, лазерных), флэш-карт, других носителей информации.

В локальных и глобальных сетях вирусы могут распространяться при передаче данных между рабочими станциями сети. При этом в силу особенности сетевых операционных систем распространяться по сетям могут все существующие на сегодня виды вирусов.

Во время работы в сети «Интернет» возможно заражение при загрузке (скачивании) файлов, рисунков, активных элементов интернет-страниц. Используя сотовый телефон для работы в сети «Интернет», можно заразить компьютер при скачивании файлов и картинок.

Также заражение возможно при использовании нелицензионного программного обеспечения, которое может иметь недостатки или быть специально инфицированным злоумышленниками.

Большую опасность представляют собой вирусы, распространяющиеся по глобальным сетям путем рассылки сообщений электронной почты.

3.3. Классификация антивирусных средств.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы.

3.3.1. Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение.

3.3.2. Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние.

3.3.3. Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут очистить изменения версии проверяемой программы от изменений, внесенных вирусом.

3.3.4. Программы-фильтры или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

3.3.5. Вакцины или иммунизаторы – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится.

4. Организация антивирусной защиты в контрольно-счетной палате

4.1. Цель антивирусной защиты информации и порядок ее применения.

Организация антивирусной защиты информации в контрольно-счетной палате направлена на предотвращение заражения информационно-вычислительных ресурсов автоматизированных систем программными вирусами.

Защита информации от воздействия программных вирусов на объектах информатизации контрольно-счетной палате осуществляется посредством применения средств антивирусной защиты.

Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации машинных носителей информации, информационных массивов, программных средств;

периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации (дискет, лазерных дисков, флэш-карт и тому подобное) перед началом работы с ними на отсутствие программных вирусов;

внеплановая проверка магнитных носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами;

постоянная защита файловых и почтовых серверов от вирусных атак;

ежемесячная проверка всех электронных архивов файлов и баз данных.

4.2. Разграничение полномочий и ответственность за организацию антивирусной защиты информации.

Ответственность за организацию антивирусной защиты на объектах информатизации контрольно-счетной палаты возлагается на заместителя председателя контрольно-счетной палаты.

Заместитель председателя контрольно-счетной палаты осуществляет следующие функции в рамках обеспечения антивирусной защиты:

разрабатывает проекты нормативных документов по организации антивирусной защиты информации;

постоянно контролирует состояние антивирусной защиты информации в контрольно-счетной палате;

анализирует состояние работы по антивирусной защите информации и вносит предложения по ее совершенствованию;

участвует в проведении расследований по фактам заражения компьютерными вирусами автоматизированных систем и персональных компьютеров;

вносит предложения по закупкам средств антивирусной защиты информации;

осуществляет внедрение средств антивирусной защиты информации в ЛВС контрольно-счетной палате;

организует обновления баз данных средств антивирусной защиты информации.

Пользователи персональных компьютеров обязаны строго соблюдать установленные правила применения средств антивирусной защиты при работе на персональном компьютере. На них возлагается непосредственная ответственность за защиту информации от заражения программными вирусами.

Пользователям персональных компьютеров запрещается отключать постоянную антивирусную защиту, самостоятельно перенастраивать систему защиты антивирусных программ.

5. Регламент применения антивирусных средств в контрольно-счетной палате

5.1. В контрольно-счетной палате допустимо использовать только лицензионные антивирусные средства защиты информации. Предпочтительно использовать антивирусные средства защиты российского производства, сертифицированные Федеральной службой по техническому и экспортному контролю России, в связи с их большей эффективностью защиты информации от вирусов, распространенных на территории Российской Федерации.

5.2. Рекомендуется использовать комплекты программ для защиты персональных компьютеров, файловых и почтовых серверов от всех видов вирусов, троянских программ и червей, предотвращения вирусных эпидемий, Интернет-угроз, а также обеспечивающих сохранность информации. К данным продуктам относятся комплекты антивирусной защиты следующих фирм: «Dr.Web», «AVP «Лаборатории Касперского», «ADinf».

6. Инсталляция системы антивирусной защиты информации

6.1. Инсталляция средств антивирусной защиты на серверах и персональных компьютерах, а также контроль комплектности и настройки установленных компонентов осуществляется сотрудниками МУ «ЦМИРиТ».

6.2. Система обновления баз данных антивирусных средств.

Система обновления баз данных антивирусных программ предусматривает получение обновлений с помощью настройки автоматического обновления с Интернет-серверов антивирусных компаний, у которых приобретены данные программы.

Ответственность за настройку и контроль ежедневного обновления баз данных антивирусных средств возлагается на заместителя председателя.

Обновления баз данных антивирусных средств на персональных компьютерах, не подключенных к ЛВС, осуществляется автоматически, как правило, не реже одного раза в неделю либо при участии сотрудника МУ «ЦМИРиТ».

7. Действия пользователей персональных компьютеров

при обнаружении программных вирусов

7.1. Признаки появления вирусов.

К основным признакам проявления вирусов можно отнести следующие:

прекращение работы или неправильная работа ранее успешно функционировавших программ;

замедление работы компьютера;

невозможность загрузки операционной системы;

исчезновение файлов и каталогов или искажение их содержимого;

появление новых неизвестных каталогов, файлов;

изменение даты и времени модификации файлов;

изменение размера файлов;

неожиданное значительное увеличение количества файлов на диске;

существенное уменьшение размера свободной оперативной памяти;

вывод на экран непредусмотренных сообщений или изображений;

подача непредусмотренных звуковых сигналов;

частые зависания и сбои в работе компьютера.

Вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин, поэтому необходима правильная диагностика состояния компьютера.

7.2. Обнаружение программных вирусов при входном контроле.

Вся поступающая информация (файлы, программное обеспечение), полученная по ЛВС, из сети «Интернет», а также на магнитных носителях информации (дискеты, лазерные диски, флэш-карты и тому подобное) подлежит обязательной проверке на наличие программных вирусов.

При обнаружении программных вирусов специалисты контрольно-счетной палаты сообщают об этом заместителю контрольно-счетной палаты, приносят зараженные носители информации для тестирования, лечения и восстановления информации.

Запрещается переносить зараженные файлы на персональный компьютер, даже если вам срочно необходим данный зараженный документ. Перенос вируса на компьютер может привести к более тяжким последствиям.

О факте обнаружения программных вирусов сообщается в адрес, по которому поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

7.3. Обнаружение программных вирусов в процессе работы на компьютере.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на персональном компьютере и сообщить о заражении компьютера заместителю председателя.

Заместитель председателя контрольно-счетной палаты приглашает сотрудников МУ «ЦМИРиТ» для принятия мер к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты. При функционировании персонального компьютера в ЛВС контрольно-счетной палате, производится его временное отключение для локализации и удаления программных вирусов. Проводятся мероприятия по проверке ЛВС на вирусы.

Приложение 6

к приказу председателя

контрольно-счетной палаты

города Череповца

от 01.04.2014 № 14

Расписка

о неразглашении информации ограниченного доступа, не относящейся к государственной тайне (сведений конфиденциального характера),

и иной служебной информации

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (Ф.И.О)

поступая на муниципальную службу в контрольно-счетную палату города Череповца, обязуюсь:

1. Не разглашать сведения конфиденциального характера, которые мне будут доверены или станут известны при исполнении служебных обязанностей.
2. Исполнять распоряжения, инструкции, положения по работе с конфиденциальной информацией в контрольно-счетной палате города Череповца.
3. В случае попытки посторонних лиц получить от меня конфиденциальную информацию, известную мне, сообщить об этом непосредственному руководителю.
4. В случае увольнения с работы, я обязуюсь неукоснительно соблюдать требования пункта 1 настоящего обязательства.

Я предупрежден(а), что за разглашение сведений конфиденциального характера могу быть привлечен(а) к ответственности в соответствии с действующим законодательством.

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Приложение 7

к приказу председателя

контрольно-счетной палаты

города Череповца

от 01.04.2014 № 14

РАСПИСКА ПРИ УВОЛЬНЕНИИ

о неразглашении информации ограниченного доступа, не относящейся

к государственной тайне (сведений конфиденциального характера), персональных данных и служебной информации

Фамилия \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Имя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Отчество \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата увольнения « » \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Во время моей работы в должности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

я получил(а) информацию или имел(а) доступ к сведениям конфиденциального характера, персональным данным, служебной информации и иной информации, сведения которой носят конфиденциальный характер.

Я подтверждаю, что был(а) проинструктирован(а), и знаю о моих обязательствах в отношении сохранности конфиденциальной информации, персональных данных и служебной информации к которой я имел(а) доступ во время работы.

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Предупреждение объявил(а):

 «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись, фамилия)