

 Администрация Ковернинского муниципального района

Нижегородской области

**П О С Т А Н О В Л Е Н И Е**

\_\_13.12.2017\_\_ № \_1040\_

**О назначении должностных лиц, ответственных за защиту информации в Администрации Ковернинского муниципального района**

В целях создания системы защиты информации ограниченного доступа в Администрации Ковернинского муниципального района, руководствуясь Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", постановлением Правительства Российской Федерации от 01.11. 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Администрация Ковернинского муниципального района Нижегородской области

 **п о с т а н о в л я е т:**

1. Назначить ответственным за организацию и руководство работами по защите информации Администрации Ковернинского муниципального района специалиста по технической защите информации сектора информационных технологий, связи и технической защиты информации Богаткова Евгения Сергеевича.

 2. Утвердить:

 2.1. Положение о системе защиты информации ограниченного доступа в Администрации Ковернинского муниципального района (Приложение №1);

2.2. Инструкцию по антивирусному контролю в Администрации Ковернинского муниципального района (Приложение №2);

2.3. Инструкцию по работе на персональном компьютере, в локальной сети и сети Интернет (Приложение №3).

3. Руководителям структурных подразделений Администрации Ковернинского муниципального района ознакомить всех сотрудников с указанным Положением и Инструкциями, обеспечить его исполнение.

4. Контроль за исполнением настоящего постановления оставляю за собой.

Глава местного самоуправления О.П. Шмелев

СОГЛАСОВАНО:

Зам.главы администрации по социальным вопросам О.В. Лоскунина

# Начальник Финансового управления В.Н. Соколова

Зав. организационно-правовым отделом С.В. Некрасова

Коррупциогенные факторы:

выявлены/невыявлены \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Зав.орг-правовым отделом С.В. Некрасова/

Отпечатано в 24 экз.:

1. В дело – 1
2. В прокуратуру – 1
3. В АПИ – 1
4. В ГПД – 1
5. В отдел экономики - 1
6. В Финансовое управление – 1
7. В сектор информационных технологий – 1
8. В отдел образования – 1
9. В комитет имущественных отношений – 1
10. В ОКС – 1
11. В Управление сельского хозяйства – 1
12. В организационно-правовой отдел – 1
13. В отдел культуры и кино – 1
14. В отдел по физкультуре и спорту – 1
15. В поселковую и сельские администрации – 6
16. В АХГ – 1
17. В сектор ГО и ЧС – 1
18. В Земское собрание – 1
19. В комитет по охране труда (Клюганов С.П.) - 1

Вагин А.С.

8 (83157) 2-14-66

Приложение №1

 к постановлению Администрации

 Ковернинского муниципального района Нижегородской области

 от «13» декабря 2017 года № 1040

**ПОЛОЖЕНИЕ**

**о системе защиты информации ограниченного доступа в**

**Администрации Ковернинского муниципального района**

 1. Общие положения

1.1. Настоящее Положение определяет принципы обеспечения информационной безопасности Администрации Ковернинского муниципального района (далее - Администрации), структуру системы защиты и порядок защиты информации ограниченного доступа, регламентирует основы организации технической защиты информации ограниченного доступа в Администрации.

1.2. Настоящее Положение является документом, обязательным для исполнения в структурных подразделениях администрации, имеющих или обрабатывающих информацию ограниченного доступа при проведении работ по технической защите информации ограниченного доступа (далее - ИОД) от утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий в целях ее уничтожения, искажения и блокирования.

1.3. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации", Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденным Постановлением Совета Министров - Правительства Российской Федерации от 15.09.93 № 912-51.

1.4. Настоящее Положение не распространяется на информацию, отнесенную в установленном порядке к сведениям, составляющим государственную тайну.

 2. Структура системы защиты ИОД

2.1. Систему защиты ИОД Администрации возглавляет Глава местного самоуправления.

2.2. Ответственность за организацию и состояние защиты ИОД в структурных подразделениях Администрации возлагается на их руководителей.

2.3. В каждом подразделении, выполняющем хранение или обработку ИОД, приказом руководителя подразделения назначается сотрудник, ответственный за реализацию мероприятий по защите ИОД, и определяется перечень лиц, допущенных к обработке ИОД.

2.4. Координацию мероприятий по организации защиты ИОД в структурных подразделениях администрации, не обладающих статусом юридического лица, а также по взаимодействию этих подразделений с контролирующими органами осуществляет специалист по технической защите информации сектора информационных технологий, связи и технической защиты информации Администрации.

2.5. Специалист по технической защите информации сектора информационных технологий, связи и технической защиты информации Администрации отвечает за установку, настройку и администрирование технических средств защиты информации (далее - ТСЗИ) при хранении или обработке ИОД с использованием средств вычислительной техники в структурных подразделениях Администрации, не имеющих своих штатных специалистов в области информационных технологий.

 3. Порядок организации и проведения работ по защите ИОД.

3.1. Мероприятия по технической защите ИОД являются составной частью деятельности Администрации и осуществляются во взаимосвязи с другими мерами по обеспечению защиты информации и режима конфиденциальности проводимых работ с ИОД.

3.2. Проведение любых мероприятий и работ с использованием ИОД без принятия необходимых мер по ее технической защите не допускается.

3.3. Защита информации - комплекс организационно-технических мер, предотвращающих или снижающих возможность утечки информации и/или воздействия на информацию.

3.4. Комплекс мероприятий по защите ИОД основывается на определении:

- источников угроз безопасности информации и вероятности реализации этих угроз для конкретных объектов;

- средств и методов защиты информации;

- разграничения доступа к информации;

- идентификации и аутентификации пользователей для работы с ИОД.

3.5. Техническая защита ИОД осуществляется путем выполнения комплекса мероприятий, направленных на предотвращение:

- утечки ИОД по техническим каналам за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами;

- несанкционированного доступа к обрабатываемой, хранящейся в технических средствах и передаваемой по каналам связи ИОД;

- преднамеренных программно-технических воздействий с целью хищения, разрушения (уничтожения), искажения ИОД в процессе обработки, передачи и хранения;

- перехвата техническими средствами речевой ИОД из помещений.

3.6. Объектами, подлежащими технической защите, являются:

- информационные ресурсы, представленные в виде магнитных или оптических носителей, информативных физических полей, информационных массивов и баз данных и содержащие ИОД;

- технические средства обработки и передачи ИОД;

- помещения, предназначенные для обработки ИОД и проведения секретных (конфиденциальных) переговоров.

3.7. Для защиты информации в компьютерной системе принимаются следующие меры:

- организационные меры защиты - меры общего характера, затрудняющие доступ к информации злоумышленникам, вне зависимости от особенностей способа обработки информации и каналов утечки и воздействия;

- организационно-технические меры защиты - меры, связанные со спецификой каналов утечки (воздействия) и метода обработки информации, но не требующие для своей реализации нестандартных: приемов, оборудования или программных средств;

- технические (программно-технические) меры защиты - меры, жестко связанные с особенностями каналов утечки и воздействия и требующие для своей реализации специальных приемов, оборудования или программных средств.

3.8. Основными организационно-техническими мероприятиями по технической защите ИОД являются:

- определение и учет информационных систем и средств формирования, передачи, хранения, обработки и распространения ИОД, подлежащей защите;

- принятие в пределах компетенции правовых актов, регулирующих отношения в области защиты информации;

- категорирование защищаемых объектов в зависимости от их важности, степени конфиденциальности ИОД и условий эксплуатации, а также классификация автоматизированных систем по требованиям защищенности от несанкционированного доступа к ИОД;

- анализ состояния и прогнозирование источников угроз безопасности информации;

- методическое и информационное обеспечение работ по защите информации;

- разработка и внедрение решений по технической защите ИОД;

- организация при необходимости аттестации защищаемых объектов;

- обеспечение физической защиты объектов;

- обеспечение защиты ИОД от утечки по техническим каналам при ее обработке, хранении и передаче;

- обеспечение защиты ИОД от несанкционированного доступа к ней в информационных системах и локальных вычислительных сетях;

- обеспечение антивирусной защиты ИОД;

- учет носителей ИОД;

- установка и ввод в эксплуатацию средств защиты информации в соответствии с классификацией по уровню контроля Федеральной службы по техническому и экспортному контролю;

- учет применяемых ТСЗИ;

- обязательное регулярное обучение администраторов и пользователей ТСЗИ правилам работы с ними;

- организация и проведение контроля состояния технической защиты ИОД;

- модернизация системы защиты на основе анализа актуальных угроз безопасности ИОД.

3.9. Конкретные методы, приемы и меры технической защиты ИОД разрабатываются в зависимости от вероятности угроз и от степени возможного ущерба в случае ее утечки, разрушения (уничтожения) на основании федеральных законов, стандартов, нормативно-методических и руководящих документов по технической защите ИОД Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

3.10. Руководители структурных подразделений Администрации, выполняющих обработку и хранение ИОД, обязаны:

- по каждой информационной системе обработки ИОД назначить приказом сотрудника, ответственного за защиту ИОД и хранение носителей ИОД;

- издать приказ о допуске лиц к обработке ИОД;

- организовать ведение журнала учета носителей ИОД;

- обеспечить хранение съемных носителей ИОД, электронных сертификатов, ключей (ключей доступа), а также журналов учета носителей ИОД в металлических шкафах-сейфах, доступ к которым закрепить приказом;

- определить приказом контролируемые зоны по каждой системе обработки ИОД и закрепить порядок доступа в них;

- ежегодно планировать актуальные мероприятия по защите ИОД подразделения и контролировать их выполнение;

- модернизацию вычислительной техники или передачу ее сторонним организациям выполнять только по согласованию со специалистом по технической защите информации сектора информационных технологий, связи и технической защиты информации после проверки информации, хранящейся на жестких дисках, гарантированного удаления с них ИОД и составления совместного акта.

3.11. Все сотрудники Администрации обязаны исполнять требования:

- настоящего Положения;

- инструкции по антивирусному контролю в Администрации,

- инструкции по работе на персональном компьютере, в локальной сети и сети Интернет для сотрудников Администрации.

4. Порядок хранения носителей, содержащих ИОД

4.1. Ответственность за организацию хранения носителей, содержащих ИОД, возлагается на руководителей подразделений Администрации, осуществляющих хранение и обработку ИОД.

4.2. Лицо, осуществляющее хранение носителей, содержащих ИОД, назначается приказом руководителя подразделения.

4.3. Лицо, осуществляющее хранение носителей ИОД, обязано:

- осуществлять хранение носителей ИОД;

- вести журнал учета носителей, содержащих ИОД, в соответствии с приложением к Положению;

- осуществлять выдачу носителей ИОД лицам, имеющим допуск к обработке данной информации, и прием носителей на хранение;

- выполнять изготовление резервных копий носителей;

- уничтожать (удалять) ИОД, утратившую свою полезность, и сами носители.

4.4. Хранение информации в материальном виде, а также на съемных носителях осуществляется в сейфах, имеющих индивидуальный доступ ответственного лица.

4.5. В журнале учета носителей ИОД регистрируется следующая информация:

- учетный номер носителя (номера носителей);

- тип (марка) носителя;

- вид ИОД;

- фамилия лица, которому выдан носитель;

- дата выдачи носителя;

- подпись лица, получившего носитель, о получении;

- дата возврата носителя (получения носителя лицом, осуществляющим хранение);

- подпись лица, ответственного за хранение носителя, о возврате.

4.6. По ИОД, хранящейся на жестких магнитных носителях "HDD", установленных в серверах и персональных компьютерах, в журнале учета носителей ИОД регистрируется следующая информация:

- учетный номер носителя (номера носителей в случае дискового массива);

- марка носителя, серийный номер, инвентарный номер сервера или персонального компьютера, в котором установлен носитель;

- вид ИОД, тип, имя базы данных, каталог расположения данных;

- фамилия лица, ответственного за персональный компьютер, или администратора сервера;

- дата вскрытия системного блока и постановки на учет;

- подпись лица, ответственного за персональный компьютер, или администратора сервера;

- дата подписи лицом, осуществляющим хранение;

- подпись лица, осуществляющего хранение.

4.7. Учетные номера присваиваются лицом, осуществляющим хранение.

4.8. В случае утраты, повреждения носителя ИОД незамедлительно уведомляется руководитель подразделения и составляется соответствующий акт. К акту прикладывается объяснительная записка лица, допустившего утрату, повреждение.

4.9. При копировании ИОД с использованием технических средств в журнале отражаются количество и вид скопированных материалов, носитель, на который было осуществлено копирование.

4.10. При изготовлении резервной копии носителя ИОД носителю присваивается учетный номер и в журнале учета делается соответствующая запись.

4.11. В журнале учета носителей ИОД отражаются все поступающие и выбывающие, в том числе временно, с места постоянного хранения носители.

4.12. Уничтожение (удаление) ИОД с носителей, содержащих ИОД, утратившую свою полезность, осуществляется на основании приказа руководителя подразделения. Уничтожение (удаление) производится в присутствии лица, осуществляющего хранение носителей ИОД, с составлением акта об уничтожении (удалении).

4.13. Контроль за соблюдением порядка хранения носителей ИОД осуществляет руководитель структурного подразделения.

4.14. Проверке подлежат:

- журнал учета носителей ИОД;

- наличие хранимых носителей ИОД и соответствие информации о них в журнале;

- акты об уничтожении (удалении) ИОД и самих носителей;

- состояние помещения и сейфа, используемых для хранения носителей.

5. Контроль состояния защиты ИОД

5.1. Контроль за состоянием технической защиты ИОД (далее - контроль) осуществляется в целях оценки эффективности текущей защиты ИОД, своевременного выявления и предотвращения утечки ИОД по техническим каналам и несанкционированного доступа к ней.

5.2. Контроль заключается в проверке выполнения требований федерального, областного законодательства, правовых актов органа местного самоуправления Ковернинского муниципального района, регулирующих сферу технической защиты ИОД, настоящего Положения, а также в оценке достаточности принимаемых по технической защите ИОД.

5.3. Основными задачами контроля являются:

- оценка деятельности структурных подразделений Администрации в области защиты ИОД в пределах их компетенции;

- выявление технических каналов утечки ИОД, каналов санкционированного доступа к ИОД и специальных воздействий на ИОД;

- оценка эффективности проводимых мероприятий по технической защите ИОД;

- выявление и анализ нарушений норм и требований, установленных федеральным, областным законодательством, правовыми актами органа местного самоуправления Ковернинского муниципального района, принятие оперативных мер по пресечению выявленных нарушений;

- разработка рекомендаций по устранению выявленных недостатков в структурных подразделениях Администрации и ведению работ по технической защите ИОД;

- проверка устранения недостатков, выявленных в результате контроля.

5.4. Контроль проводится специалистом по технической защите информации сектора информационных технологий, связи и технической защиты информации Администрации совместно с сотрудником, ответственным за защиту ИОД структурного подразделения.

6. Ответственность за разглашение ИОД лица, допустившие разглашение ИОД, несут ответственность в соответствии с действующим законодательством.

 Приложение №2

 к постановлению администрации

 Ковернинского муниципального района

Нижегородской области

 от «\_\_» декабря 2017 года № \_\_\_\_

**ИНСТРУКЦИЯ**

**по антивирусному контролю в Администрации**

**Ковернинского муниципального района**

 1. Общие положения

Целью создания системы антивирусного контроля является обеспечение

защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

 Основополагающими требованиями к системе антивирусного контроля Администрации Ковернинского муниципального района (далее - Администрации):

- решение задачи антивирусного контроля должно осуществляться в общем виде.

Средство контроля не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего не известно;

- решение задачи антивирусного контроля должно осуществляться в реальном времени.

Мероприятия, направленные на решение задач по антивирусному контролю:

- установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение, идущее в комплекте с подлинной операционной системой, поддерживающее работу с пользовательскими профилями;

- регулярное обновление и профилактические проверки;

- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;

- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб;

- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;

- проведение регулярных проверок целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;

- внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

- следует иметь планы обеспечения бесперебойной работы Администрации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

 Технологические инструкции:

1.1. В организации руководителем должно быть назначено лицо, ответственное за антивирусный контроль, в должностные инструкции для которого должны быть прописаны порядок действия в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя организации.

1.2. В Администрации может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CDROM, DVD,flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

 2. Требования к проведению мероприятий по антивирусной защите

2.1. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей – ежедневно, в ночное время по расписанию.

2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

2.3.1. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения.

2.3.2. 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 и т.п.).

2.3.3. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

2.4. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

2.4.1. Приостановить работу.

2.4.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусного контроля (в случае его отсутствия – заведующего отделом).

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

2.4.4. Провести лечение или уничтожение зараженных файлов.

 3. Ответственность

3.1. Ответственность за организацию антивирусного контроля возлагается на лицо, назначенное заведующим отделом.

 3.2. Ответственность за проведение мероприятий антивирусного контроля в Администрации возлагается на ответственного за обеспечение антивирусного контроля, соблюдение требований настоящей Инструкции при работе на персональных компьютерах возлагается на пользователей данных компьютеров или руководителей структурных подразделений Администрации.

3.3. Периодический контроль за состоянием антивирусной защиты осуществляется руководителем и фиксируется Актом проверки (не реже 1 раз в квартал).

 Приложение № 3

 к постановлению администрации

 Ковернинского муниципального района

Нижегородской области

 от «\_\_\_» декабря 2017 года № \_\_\_\_

**ИНСТРУКЦИЯ**

**по работе на персональном компьютере, в локальной сети и сети Интернет**

1. Общие положения инструкции

1.1. Целью настоящей инструкции является регулирование работы системного администратора и пользователей, для эффективного использования и распределения сетевых ресурсов коллективного пользования, поддержания необходимого уровня защиты информации, ее сохранности, соблюдения прав доступа к информации, уменьшение риска умышленного или неумышленного неправильного использования сетевых ресурсов;

 1.2. К работе в системе допускаются лица, назначенные начальником соответствующего отдела и ознакомившиеся с данной инструкцией;

 1.3. По уровню ответственности и правам доступа к сети пользователи сети разделяются на следующие категории: системные администраторы и пользователи;

 1.4. Пользователь подключенного к сети компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к ней;

 1.5. Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в сети, выдаваемым системным администратором;

 В общем случае имя это фамилия и инициалы сотрудника, написанные английскими буквами (регистр букв не имеет значения). Сотрудники должны знать точное написание своего индивидуального имени.

 1.6. Системный администратор создает и изменяет пароль для входа пользователей в компьютерную сеть. Пользователи должны помнить свои пароли;

 1.7. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем (в соответствии с пунктами 1.5-1.6 настоящей инструкции по пользованию компьютером и сетевыми ресурсами) для входа в компьютер, локальную сеть и сеть Интернет, передача их кому-либо запрещена;

 1.8. В случае нарушения правил пользования сетью, связанных с используемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений;

 1.9. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо другом, пользователь должен немедленно сообщить об этом системному администратору;

 1.10. Пользователи обязаны выполнять предписания системного администратора по работе с компьютером и сетью;

 1.11. Системный администратор - лицо, обслуживающее сервер и следящее за правильным функционированием сети. Системный администратор дает разрешение на подключение компьютера к сети, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является нарушением правил пользования сетью;

 1.12. Системный администратор информирует пользователей обо всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети;

 1.13. Системный администратор имеет право отключить компьютер пользователя от сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

2. Инструкция по работе за компьютером

 2.1. Запрещено самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо обратиться к системному администратору;

 2.2. Все кабели, соединяющие системный блок с другими устройствами (особенно клавиатуры и мыши PS/2), следует вставлять и вынимать только при полностью обесточенном компьютере и выключенными дополнительными устройствами. Исключение составляют автономные USB-устройства: они могут быть подключены к включенному компьютеру;

 Полностью обесточенным считается компьютер с отключенным силовым проводом питания электросети. В помещении все электрические розетки должны соответствовать ГОСТ и иметь заземление. В случае подозрения на повреждение розетки или заземления до начала работы пользователь должен обратиться в обслуживающую данную электросеть организацию для устранения проблем. Запрещается включать мощные электроприборы (электрочайники, нагреватели, электроинструмент) в розетки, предназначенные для компьютерных устройств без письменного согласования с соответствующей организацией.

 2.3. Запрещено подвергать механическим воздействиям компьютерные провода (например, ставить на них мебель, сильно перегибать, прикреплять скрепками, завязывать узлом);

 2.4. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере. Этим занимается системный администратор;

 2.5. Запрещено аварийно завершать работу компьютера кнопкой “Reset” или отключением от электросети. Завершайте работу компьютера правильно, через кнопку (Пуск) и Завершение работы;

 2.6. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям. (Нельзя сидеть на компьютере, загораживать (например, бумагами или мебелью) вентиляционные отверстия, проливать на него жидкости, просыпать семечки, скрепки, ставить у батареи и других нагревательных приборов);

 2.7. Документы необходимо сохранять на специально отведенные диски, (обычно D:\"Мои документы") или в сети в месте определенным системным администратором. Запрещено хранить нужные документы и другие данные на системном диске С:;

 2.8. Если есть подозрения, что какие - либо нужные документы уничтожены или повреждены, необходимо полностью прекратить работу с компьютером или сетевым ресурсом и незамедлительно обратиться к системному администратору;

 2.9. По завершению рабочего дня компьютер можно выключить, по требованию системного администратора компьютер может быть оставлен включенным для проведения профилактических работ в нерабочее время;

 2.10. Перед началом работы пользователь должен:

Включить выключатель сетевого фильтра. При включении кнопка должна начать светиться;

 Включить источник бесперебойного питания (ИБП) и выждать 2-4 секунды;

 Включить монитор (если выключен);

 Включить компьютер кнопкой “Power”. Дождаться загрузки операционной системы(ОС);

 Войти в систему, используя свои личные имя пользователя и пароль (Имя пользователя обычно состоит из латинских букв в формате "Фамилия-ИО").

 2.11. По завершению работы пользователь должен:

 Закрыть все открытые программы и документы, сохранив нужные изменения;

 Выйти из системы.

 2.12. При отключении электроэнергии источник бесперебойного питания (ИБП) позволяет компьютеру оставаться в рабочем состоянии от 5 до 20 минут. При отключении электроэнергии в помещении пользователь должен в немедленном порядке сохранить документы и выключить компьютер в соответствии с данной инструкцией (пункт 2.5).

 2.13. Закрыть все открытые программы и документы, сохранив нужные изменения;

 2.14. С помощью меню “Пуск -> Завершение работы” выключить компьютер и дождаться завершения работы. (Системный блок перестанет мигать и шуметь);

 2.15. При возникновении ошибок во время работы с компьютером необходимо записать текст ошибки и код ошибки, после этого, если проблему не удается решить самостоятельно, обратится к системному администратору.

3.Инструкция по работе в локальной сети

 3.1. Пользователи сети обязаны:

 3.1.1. Соблюдать правила работы в сети, оговоренные настоящей инструкцией;

 3.1.2. При доступе к внешним ресурсам сети соблюдать правила, установленные системными администраторами для используемых ресурсов;

 3.1.3. Немедленно сообщать системному администратору сети об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Администратор, при необходимости, с помощью других специалистов, должен провести расследование указанных фактов и принять соответствующие меры;

 3.1.4. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети;

 3.1.5. Обеспечивать беспрепятственный доступ системным администраторам к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;

 3.1.6. Выполнять предписания системных администраторов, направленные на обеспечение безопасности сети;

 3.1.7. В случае обнаружения неисправности (например, сильный посторонний шум или запах, необычное поведение затрудняющее работу) компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору.

 3.1.8. Удалять с сетевых ресурсов устаревшие или не используемые файлы.

 3.2. Пользователи сети имеют право:

 3.2.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Системный администратор вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;

3.2.2. Обращаться к администратору сети по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться администратором сети;

 3.2.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов сети;

 3.2.4. Вносить предложения по улучшению работы с ресурсом.

 3.3. Пользователям сети запрещено:

 3.3.1. Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключенияресурсов);

 3.3.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с администрацией и системным администратором;

 3.3.3. Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

 3.3.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;

 3.3.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с системным администратором, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет;

 3.3.6. Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;

 3.3.7. Работать с каналоемкими ресурсами (видео, аудио, радио, чаты, файлообменные сети, torrent и др.) без согласования с системным администратором сети. При сильной перегрузке канала вследствие использования каналоемких ресурсов доступ пользователя вызвавшего перегрузку, может быть прекращен;

 3.3.8. Получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую коммерческую или государственную тайну;

 3.3.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;

 3.3.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором.

 3.3.11. Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;

 3.3.12. Использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

3.4. Пользователи сети несут ответственность:

3.4.1.​ За целостность и сохранность вверенных ему информационных ресурсов;

3.4.2.​ За все действия, совершенные от его имени, с использованием его учетной записи;

3.4.3.​ За противоправные действия и действия, нарушающие нормативные акты компании, в соответствии с нормативными документами компании и законодательством РФ;

3.4.4.​ При несоблюдении пользователями условий настоящей инструкции к ним применяется административные меры наказания, вплоть до увольнения, в соответствии со степенью вины, установленной служебным расследованием.

 4.Инструкция по работе с электронной почтой

 4.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено. Создание или измение параметров почтового ящика проводится системным администратором по просьбе администрации;

 4.2. На рабочем месте допускается использовать только ящики электронной почты, предоставленные администрацией. Прямой доступ к другим почтовым системам может быть блокирован. Для получения писем с других систем допускается использовать переадресацию, которая может быть настроена с помощью системного администратора.

 4.3. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными;

 4.4. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины.

 4.5. Пользователи не должны позволять кому-либо посылать письма от чужого имени. Это касается их начальников, секретарей, ассистентов или других сослуживцев;

4.6. При работе с электронной почтой запрещается открывать сообщения сомнительного содержания, или пришедшие от неизвестного отправителя.

 4.7. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы (MS Outlook);

 4.8. Нельзя осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

4.9. Размер вложений у отправляемых писем обычно не должен превышать 10Мб. Для пересылки фотографий или больших файлов их нужно предварительно подготовить к отправке.

 5.Инструкция по работе в сети Интернет

 5.1. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей;

 5.2. По использованию ресурсов Интернет необходимо ведение статистики.

 5.3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, протоколируются и могут использоваться для принятия решения о применении к нему санкций;

 5.4. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ;

 5.5. Все программы, используемые для доступа к сети Интернет, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности;

 5.6. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;

 5.7. Запрещено обращаться к ресурсам сети Интернет, несвязанных непосредственно с выполнением своих должностных обязанностей в рабочее время, а также к ресурсам с сомнительным содержанием.

 5.8. Запрещается скачивать и запускать с любых ресурсов любые исполняемые файлы без согласования с системным администратором.

 6. Работа со съемными носителями информации (Флешки, переносные жесткие диски, цифровые фотоаппараты, телефоны и т.д)

 6.1 Подключение съемных носителей следует производить при включенном компьютере и загруженной операционной системой.

 6.2. Существует большое количество вирусов, предназначенных для повреждения информации на флэшках (эти вирусы на зараженном ПК постоянно загружены в оперативную память и отслеживают порты на предмет подключения съемных устройств), если Вам нужно скопировать информацию с Вашей флэшки на посторонний ПК, перед подключением включайте блокировку записи (если она предусмотрена конструкцией Вашей флэшки).

 6.3. Не извлекайте флэшку из ПК в момент обращения к ней, это может привести к потере данных и повреждению устройства. Если же в момент отключения флэшки от ПК выполнялась операция записи, в файловой системе флэшки неизбежно появятся ошибки.

Если при попытке извлечь флэшку через значок "Безопасное извлечение устройства" появляется диалоговое окно "Проблема при извлечении "Запоминающее устройство для USB": Устройство Универсальный том не может быть остановлено прямо сейчас. Попробуйте остановить его позже", значит, открыты какие-то файлы с флэшки. Закройте их и повторите попытку. Для сохранности данных не рекомендуется открывать файлы данных со сменных носителей.

 6.4. Рекомендуется совершать обмен файлами данных через электронную почту. Перед копированием файлов данных с внешних носителей настоятельно рекомендуется проверить носитель с помощью антивируса. Запрещается запускать или переписывать с любых внешних носителей любые исполняемые файлы (приложения или командные файлы с расширениями exe, bat, com, cmd, inf, dll, scr) без согласования с системным администратором.

 7. Работа с периферийными устройствами (принтеры, ксероксы, сканеры, копиры).

 7.1. Запрещается использовать для печати дешевую бумагу не соответствующего типа, а также использовать для печати бумагу со скрепками, наклейками или мятую бумагу.

7.2. Не разрешается вынимать картриджи из принтеров за исключением их замены.

 7.3. Не рекомендуется установка периферийной техники рядом с обогревательными приборами или на подоконнике, а также подвергать воздействию прямых солнечных лучей, влаги или пыли.

 Данная инструкция по пользованию компьютером применима и для домашних пользователей если они хотят сохранить работоспособность компьютера максимально долго.