

**УТВЕРЖДЕНО**

Приказом МКУ «РЦ»

от 29 августа 2025 № 01-01-09/11

**ПОЛОЖЕНИЕ**

**О защите персональных данных в муниципальном казенном учреждении  
«Расчетный центр города Каменска-Уральского»**

## 1. Общие положения

- 1.1. Настоящее Положение разработано во исполнение Федерального закон от 27.07.2006 № 152-ФЗ "О персональных данных" в соответствии с Федеральным законом № 149-ФЗ от 26.07.2006 «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
- 1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты персональных данных в Учреждении.
- 1.3. Требования настоящего Положения распространяются на всех работников Учреждения, использующих в работе автоматизированное рабочее место пользователя.
- 1.4. Организационное обеспечение мероприятий антивирусного контроля, использование сети Интернет, электронной почты, мобильных устройств и носителей информации и контроль за действиями пользователей возлагается на начальника отдела информационной технологии.
- 1.5. Сотрудники Учреждения при выполнении возложенных на них обязанности принимают на себя обязательство о неразглашении персональных данных. Обязательство о неразглашении персональных данных оформляется письменно (Приложение № 1).

## 2. Основные термины, сокращения и определения

- 2.1. **АРМ** – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.
- 2.2. **Адрес IP** – уникальный идентификатор АРМ, подключенного к ИС Учреждения, а также сети Интернет.
- 2.3. **Интернет** – глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.
- 2.4. **АС** – автоматизированная система Учреждения – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
- 2.5. **ИТ** – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации с использованием средств компьютерной и другой техники.
- 2.6. **Отдел ИТ** – структурное подразделение Учреждения, сопровождающее информационные технологии.
- 2.7. **ПО** – программное обеспечение вычислительной техники, базы данных.
- 2.8. **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
- 2.9. **Пользователь** – работник Учреждения, использующий АРМ для выполнения своих должностных обязанностей.

- 2.10. **Электронная почта** – сервис обмена электронными сообщениями в рамках АС и общедоступных сетей Интернет.
- 2.11. **Электронное почтовое сообщение** – сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты.
- 2.12. **Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме.
- 2.13. **Компьютерный вирус** - программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.
- 2.14. **Зараженная программа** — это программа, содержащая внедренную в нее программу-вирус.

### 3. Порядок эксплуатации программного обеспечения

- 3.1. В целях автоматизации производственной, управленческой, вспомогательной деятельности в Учреждении разрешено применение коммерческого и бесплатного ПО необходимого для выполнения возложенных на Учреждений задач.
- 3.2. В состав каждого АРМ входит набор ПО для выполнения определенного вида деятельности. Первоначальная комплектация АРМ определяется начальником структурного подразделения совместно с начальником отдела ИТ. ПО, не входящее в состав АРМ, не может быть установлено и использовано работниками Учреждения без процедуры согласования.
- 3.3. Все сотрудники Учреждения без исключения знакомятся с составом АРМ с набором и функциями ПО,
- 3.4. Конкретный состав установленного ПО на каждом АРМ определяется на основании перечня коммерческого и бесплатного ПО и перечня информационных ресурсов Учреждения. Описание конфигурации ПК и перечень установленного ПО фиксируется начальником отдела ИТ, начальником структурного подразделения и пользователем АС в паспорте АРМ. (Приложение №2).
- 3.5. Все операции по установке, сопровождению и поддержке, удалению ПО АРМ выполняются непосредственно при участии работников отдела ИТ Учреждения. Изменение конфигурации аппаратно-программных средств без согласования с начальником отдела ИТ категорически запрещается.
- 3.6. При эксплуатации программного обеспечения необходимо:
  - 3.6.1. Соблюдать требования настоящего Положения.
  - 3.6.2. Использовать имеющиеся в распоряжении ПО исключительно для выполнения своих служебных обязанностей.
  - 3.6.4. Обеспечивать сохранность переданных в составе АРМ носителей с ключевой информацией, сертификатов подлинности коммерческого ПО.
- 3.7. При эксплуатации программного обеспечения запрещено:
  - 3.7.1. Использовать АРМ не по назначению.

3.7.2. Самостоятельно вносить изменения в конструкцию, конфигурацию, размещение АРМ ИС и другого оборудования АС.

3.7.3. Изменять состав установленного на АРМ ПО (устанавливать новое ПО, изменять состав компонент пакетов ПО и удалять ПО).

3.7.4. Приносить на внешних носителях, загружать и не санкционированно запускать на своем или другом АРМ любые системные или прикладные программы, не согласованные с начальником отдела ИТ.

3.8. Запрос на установку ПО может быть инициирован начальником структурного подразделения по следующим основаниям:

- необходимости организации АРМ для нового работника;
- необходимости выполнения работниками новых (дополнительных) обязанностей, для которых требуется дополнительное ПО или полная замена АРМ;
- появления качественно нового (альтернативного) ПО, взамен используемого в составе АРМ.

3.9. При отсутствии в Учреждении вакантных лицензий на коммерческое ПО из перечня либо при отсутствии в перечне запрашиваемого ПО начальник структурного подразделения готовит заявку на приобретение дополнительных лицензий, либо на приобретение требуемого ПО согласно принятым в Учреждении правилам документооборота.

3.10. До начала установки ПО оно должно быть предварительно проверено на работоспособность, а также отсутствие опасных функций.

3.11. Поддержка и сопровождение ПО выполняется техническими специалистами отдела ИТ.

3.12. Поддержка и сопровождение ПО заключается в выполнении следующих видов работ:

- настройка и адаптация установленного ПО;
- установка обновлений ПО;
- регламентированное создание резервных копий (архивирование) ПО и пользовательских данных (электронных документов, баз данных);
- устранение неисправностей, связанных с использованием установленного ПО;
- консультирование пользователей ИС.

3.13. Работа по сопровождению ПО может быть инициирована пользователем АС либо непосредственно отделом ИТ.

3.14. ПО выводится из эксплуатации в следующих случаях:

- окончание лицензионного срока использования ПО;
- замена используемого ПО на альтернативное;
- прекращение использования ПО вследствие отсутствия надобности, морального старения или выхода из строя.

3.15. Вывод из эксплуатации выполняется техническими специалистами отдела ИТ.

3.16. Отдел информационных технологий в случае необходимости путем резервного копирования обеспечивает сохранность пользовательских данных, настроек, баз и банков данных, содержащихся в удаляемом ПО.

- 3.17. Резервное копирование информационной системы Учреждения в целях предотвращения утраты, блокирования персональных данных, производится не реже чем один раз в квартал.
- 3.18. В случае обнаружения несанкционированной установки ПО, данный факт рассматривается как нарушение действующего в Учреждении настоящего Положения. Несанкционированное установленное ПО подлежит немедленному удалению.
- 3.19. Плановый аудит проводится по всему парку вычислительной техники, используемой в АС Учреждения, не реже, чем один раз в год. Внеплановый аудит (полный или выборочный) проводится по мере необходимости. Необходимость, время и область проведения внеочередных аудитов определяются отделом информационных технологий в соответствии с настоящим Положением.

#### **4. Порядок использования сети Интернет и электронной почты**

- 4.1. Доступ в сеть Интернет и к электронной почте (далее – к Сервисам) в Учреждении осуществляется централизованно с применением специальных программно-технических средств защиты (межсетевых экранов).
- 4.2. Доступ к АС Учреждения с использованием мобильных устройств (мобильного интернета) не допускается.
- 4.3. На АРМ, подключенное к Сервисам, в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальной антивирусной базой.
- 4.4. Доступ к Сервисам Учреждения предоставляется ограниченному кругу сотрудников Учреждения в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам, для обмена служебной информацией в виде электронных сообщений и документов в электронном виде в интересах Учреждения после ознакомления с настоящим Положением.
- 4.5. Для доступа сотрудников Учреждения к Сервисам допускается применение коммерческого или бесплатного ПО разрешенного к использованию в Учреждении.
- 4.6. Доступ работнику Учреждения к Сервисам может быть инициирован начальником структурного подразделения в случаях:
  - необходимости организации АРМ для нового работника;
  - необходимости выполнения работником новых (дополнительных) обязанностей, для которых требуется доступ к внешним ресурсам.
- 4.7. Операции по предоставлению доступа работников Учреждения к Сервисам и их техническому обеспечению выполняются отделом информационных технологий Учреждения через заявки (служебные записки) на имя руководителя Учреждения, подписанные руководителем структурного подразделения.
- 4.8. При использовании Сервисов необходимо:
  - соблюдать требования настоящего Положения.

- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей.

4.9. Типичные угрозы при работе с Сервисами и рекомендации по их предотвращению приведены в Приложении №1.

4.10. Общие меры предосторожности при работе с Сервисами приведены в Приложении №2.

4.11. При использовании Сервисов запрещено:

- использовать предоставленный Учреждением доступ к Сервисам в личных целях.

- использовать специализированные аппаратные и программные средства, позволяющие работникам Учреждения получить несанкционированный доступ к Сервисам.

- публиковать, загружать и распространять материалы содержащие:

- конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, персональные данные;

- информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца;

- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;

- угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

- фальсифицировать свой IP-адрес, а также прочую служебную информацию.

- осуществлять попытки несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них.

- переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей.

- по собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений.

- использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей.

- публиковать свой электронный адрес, либо электронный адрес других работников Учреждения на общедоступных Интернет-ресурсах (форумы, конференции и т.п.).

- предоставлять третьим лицам доступ к электронному почтовому ящику Учреждения.

- запрещается отключать установленное на АРМ антивирусное программное обеспечение.

4.12. Содержание Интернет-ресурсов, а также файлы, загружаемые из Сервисов, подлежат обязательной проверке на отсутствие вредоносного ПО.

- 4.13. Информация о посещаемых работниками Учреждения Интернет-ресурсах при необходимости протоколируется для последующего анализа и может быть предоставлена Руководителям структурных подразделений, а также Руководству Учреждения для контроля.
- 4.14. Отдел информационных технологий праве блокировать или ограничивать доступ сотрудников к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей.

### **5. Порядок использования мобильных устройств и носителей информации**

- 5.1. Под использованием мобильных устройств и носителей информации в АС Учреждения понимается их подключение к инфраструктуре АС с целью обработки, приема/передачи информации между АС и мобильными устройствами, а также носителями информации.
- 5.2. В АС допускается использование только учтенных мобильных устройств и носителей информации, которые являются собственностью Учреждения и подвергаются регулярной ревизии и контролю.
- 5.3. На предоставленных Учреждением мобильных устройствах допускается использование коммерческого и свободно распространяемого ПО, входящего в Перечень разрешенного к использованию ПО.
- 5.4. К предоставленным Учреждением мобильным устройствам и носителям информации предъявляются те же требования по защите информации, что и для стационарных АРМ
- 5.5. Мобильные устройства и носители информации предоставляются работникам Учреждения по инициативе Руководителей структурных подразделений в случаях:
- необходимости выполнения вновь принятым работником своих должностных обязанностей;
  - возникновения у работника Учреждения производственной необходимости.
- 5.6. При использовании предоставленных работникам Учреждения мобильных устройств и носителей информации необходимо:
- соблюдать требования настоящего Положения.
  - использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей.
  - ставить в известность руководителя о любых фактах нарушения требований настоящего Положения.
  - эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей.
  - обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами.
  - извещать руководителя о фактах утраты (кражи) мобильных устройств и носителей информации.
- 5.7. При использовании предоставленных работникам Учреждения мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях.
  - передавать мобильные устройства и носители информации другим лицам.
  - оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.
- 5.8. Любое взаимодействие (обработка, прием/передача информации), инициированное работником Учреждения между АС и неучтенными (личными) мобильными устройствами, а также носителями информации, рассматривается как несанкционированное.
- 5.9. Информация, хранящаяся на предоставляемых Учреждением мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.
- 5.10. Съёмные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съёмных носителей с конфиденциальной информацией осуществляется комиссией. По результатам уничтожения носителей составляется акт.
- 5.11. В случае увольнения или перевода работника в другое структурное подразделение Учреждения, предоставленные ему мобильные устройства и носители информации, изымаются.

## **6. Организация системы антивирусного контроля**

- 6.1. Целью мероприятий по антивирусному контролю является предотвращение потерь информации в АС Учреждения.
- 6.2. Задачами антивирусной защиты являются:
- определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;
  - проведение профилактических работ с применением антивирусных диагностических средств;
  - непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации АС Учреждения.
- 6.3. Ответственным за проведение мероприятий по предотвращению вирусного заражения АРМ является начальник отдела информационных технологий. Ответственный за антивирусный контроль в своей работе руководствуется настоящим Положением, нормативными актами по защите информации, и другими документами.
- 6.4. К использованию в Учреждении допускаются только лицензионные антивирусные средства, централизованно закупленные Учреждением у разработчиков (поставщиков) указанных средств.
- 6.5. Установка средств антивирусной защиты и настройка их параметров в соответствии с руководствами по применению конкретных антивирусных средств на АРМ в Учреждении осуществляется отделом информационных технологий.

- 6.6. Обновление антивирусных баз должно производиться автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную.
- 6.7. Обязательному входному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях и мобильных устройствах.
- 6.8. Файлы резервных копий, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в полгода.
- 6.9. Мероприятия по антивирусной защите на компьютерах в Учреждении включают в себя:
  - профилактика вирусного заражения;
  - анализ ситуаций;
  - применение средств антивирусной защиты;
  - проведение расследований инцидентов связанных с вирусами.
- 6.10. Анализ ситуации наличия вирусов выполняется Начальником отдела ИТ. При анализе могут дополнительно использоваться специальное программное обеспечение для обнаружения вирусов.
- 6.11. В ходе анализа ситуации обязательно требуется определить источник заражения. В случае заражения через глобальную сеть Интернет или по электронной почте следует немедленно заблокировать ресурс или адрес электронной почты – источник заражения.
- 6.12. В случае обнаружения вирусного заражения расследование допущенных нарушений производится отделом информационных технологий.
- 6.13. После уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы.
- 6.14. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС Учреждения и контроль за действиями при работе с паролями возлагается на отдел информационных технологий.
- 6.15. Пароли доступа ко всем подсистемам АС Учреждения, информационным ресурсам первоначально формируются отделом информационных технологий, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже:

Личные пароли пользователей автоматизированной системы Учреждения должны выбираться с учетом следующих требований:

  - длина пароля должна быть не менее 8 символов;
  - в числе символов пароля обязательно должны присутствовать буквы, цифры и (или) специальные символы (@, #, \$, &, \*, % и т.п.). Исключение составляют подсистемы АС Учреждения, в которых использование подобных спецсимволов недопустимо;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa\$\$w0rd, и т.п.);

- при смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами;

6.16. Пароли служебных и привилегированных учетных записей автоматизированной системы должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 12 символов;

- в числе символов пароля обязательно должны присутствовать, цифры и (или) специальные символы (@, #, \$, &, \*, % и т.п.). Исключение составляют подсистемы АС Учреждения, в которых использование подобных спецсимволов недопустимо;

- при смене пароля новый пароль должен отличаться от старого не менее, чем четырьмя символами, расположенными не подряд;

- при создании паролей служебных учетных записей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко запоминаемых паролей.

6.17. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Учреждения.

Директору Муниципального казенного  
учреждения «Расчетный центр города  
Каменска-Уральского»  
Денисовой Т.Р.

**ОБЯЗАТЕЛЬСТВО**  
**о неразглашении персональных данных**

Я, \_\_\_\_\_  
(ФИО работника)

исполняющий(ая) должностные обязанности по занимаемой должности

\_\_\_\_\_ (наименование должность)

понимаю, что при выполнении должностных обязанностей получаю доступ к персональным данным лиц получающих меры социальной поддержке по оплате жилого помещения и коммунальных услуг. Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных.

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам персональные данные собираемые, обрабатываемые и хранящиеся в Учреждении, которые мне известны или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам персональные данные, которые мне известны или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня персональные данные, сообщить об этом своему непосредственному руководителю.
4. Не использовать персональные данные с целью получения выгоды.
5. Выполнять требования нормативных правовых актов принятых в Учреждении, регламентирующих вопросы защиты персональных данных.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных собираемых, обрабатываемых, хранящихся в Учреждении я несу дисциплинарную, административную и уголовную ответственность в порядке, установленном федеральными законами.

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(фамилия, инициалы)

« \_\_\_\_\_ » 20\_\_ г.

### Паспорт автоматизированного рабочего места

Материально-ответственное лицо:	
Отдел:	
Ответственный пользователь:	
Имя компьютера:	
Домен/Рабочая группа:	

#### 1. Состав АРМ:

Наименование	Марка/модель
<i>Системный блок</i>	
Мат. плата	
Процессор	
ОЗУ	
Диск	
Видеоадаптер	
Сетевой адаптер	
<i>Монитор</i>	
<i>Клавиатура</i>	
<i>Мышь</i>	
<i>Принтер</i>	
<i>Прочее (указать что именно)</i>	

#### 2. Программное обеспечение

№ п/п	Наименование ПО, издатель	Версия	Дата установки	ФИО установившего
1	Операционная система			
2				
3				
4				
5				
6				
7				

Установлено антивирусное ПО:			
Установлено средство защиты от НСД:			
Установлено средство криптозащиты:			

Начальник структурного подразделения:

\_\_\_\_\_

подпись

\_\_\_\_\_

расшифровка

Начальник отдела ИТ

\_\_\_\_\_

подпись

\_\_\_\_\_

расшифровка

Ответственный пользователь:

\_\_\_\_\_

подпись

\_\_\_\_\_

расшифровка

**Типичные угрозы  
при работе с сетью Интернет и электронной почтой**

№ п/п	Угроза	Примечание	Рекомендуемые меры предосторожности
1.	Заражение компьютера вирусом.	Чаще всего заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых».	- не посещать перечисленные сайты; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
2.	Заражения компьютера вирусом при просмотре почтовых сообщений.	Обычно происходит при открытии прикрепленного к письму файла.	- не открывать письма, если электронный адрес отправителя вам не знаком или выглядит «странно»; - не открывать прикрепленные файлы, если отправитель письма вам неизвестен; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
3.	Утечка информации с рабочей станции.	Уязвимым может оказаться программное обеспечение (чаще всего таковым является свободно распространяемое ПО, а также ПО от неизвестных или малоизвестных производителей). Также причиной утечки может оказаться заражение компьютера вирусом.	- использовать только принятое к использованию в Учреждении программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
4.	Предоставление возможности удаленного управления компьютером.	Такая возможность может быть получена как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом).	- использовать только принятое к использованию в Учреждении программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
5.	Потеря функциональности (полной или частичной) рабочей станцией.	Чаще всего это происходит вследствие использования уязвимостей программного обеспечения злоумышленником или из-за заражения вирусом.	- использовать только принятое к использованию в Учреждении программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
6.	Кража личной информации.	Чаще всего к этому приводит ввод такой информации на веб-страницах, в том числе сайтах-двойниках, которые внешне идентичны настоящим сайтам (например, сайту банка), но на самом деле являются подделкой.	- не открывать письма (и особенно вложения) от незнакомых адресатов; - внимательно проверять адрес страницы, на которой вы собираетесь оставить информацию; - не сохранять пароли в формах веб-страниц.
7.	Захват адресов электронной почты, веб-страниц и т.п.	Чаще всего к этому приводит использование «слабого» пароля для доступа к ресурсу, а также подбор ответа на контрольный вопрос, используемый для восстановления пароля в случае его возможной утери.	- использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра и цифр); - не использовать в качестве ответов на контрольные вопросы (и, конечно, в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию; - никогда не раскрывать перечисленную выше информацию (если она используется для описанных целей) незнакомым людям; - не сохранять пароли в формах веб-страниц.

**Общие меры предосторожности  
при работе с сетью Интернет и электронной почтой**

№ п/п	Мера предосторожности	Примечание
1.	Использование только разрешенного отделом информационных технологий программного обеспечения.	Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя из-за ошибок в написании ПО. Ответственность возлагается на пользователя.
2.	Отслеживание появления обновлений ПО, используемого на компонентах, АС Учреждения, взаимодействующих с сетью Интернет.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.
3.	В случае обнаружения в используемом ПО критических с точки зрения безопасности уязвимостей и невозможности их устранения – приостановить эксплуатацию такого ПО.	Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.
4.	Обязательное использование и своевременное обновление антивирусного ПО на компонентах АС Учреждения, взаимодействующих с сетью Интернет, в режиме мониторинга событий.	Заражение вирусами может произойти и без «интерактивного» участия пользователя – достаточно связи с сетью Интернет.
5.	При работе с электронной почтой – не открывать письма с вложенными файлами от неизвестных авторов, перед запуском/открытием любых файлов производить их антивирусную проверку.	В последнее время наиболее распространенный канал распространения вирусов, а также кражи личной информации – электронная почта. В случае возникновения вопросов необходимо обратиться в отдел информационных технологий о дальнейших действиях. Ответственность возлагается на пользователей.
6.	Запретить автоматическое сохранение и/или запуск файлов и элементов ActiveX, скриптов из сети Интернет на рабочей станции пользователя.	Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или через сами веб-страницы, которые содержат вредоносный/опасный код. Ответственность возлагается на пользователей.
7.	Не рекомендуется сохранять пароли в формах при посещении веб-страниц.	Это может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на пользователей.