**ИВАНОВСКАЯ ОБЛАСТЬ**

**ЛУХСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ ПОРЗДНЕВСКОГО**

**СЕЛЬСКОГО ПОСЕЛЕНИЯ**

# ПОСТАНОВЛЕНИЕ

**26.12.2022 г. №67**

О защите информации в администрации Порздневского сельского поселения

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» администрация Порздневского сельского поселения постановляет:

1. Утвердить инструкцию по организации антивирусной защиты в администрации Порздневского сельского поселения (Приложение 1);

2. Утвердить инструкцию по организации парольной защиты (Приложение 2);

3. Утвердить правила обеспечение информационной безопасности при использовании в работе персональных компьютеров и локальной вычислительной сети (приложение 3);

4. Утвердить правила работы с электронной почтой (Приложение 4);

5. Утвердить правила обеспечения информационной безопасности при использовании в работе глобальной вычислительной сети интернет и «социальных сетей» (Приложение 5).

7. Ведущему специалисту администрации ознакомить с настоящими Правилами всех работников администрации Порздневского сельского поселения под личную роспись.

8. Настоящее постановление вступает в силу с момента подписания.

9. Контроль за исполнением данного постановления возложить на ведущего специалиста администрации.

Глава Порздневского сельского поселения Костюнин С.Б.

Исп. Абрамова О.А.

Приложение 1

к постановлению администрации Порздневского

сельского поселения от 26.12.2022 №67

**Инструкция по организации антивирусной защиты в администрации Порздневского сельского поселения**

1. Общие положения

1. Настоящая Инструкция определяет требования к организации антивирусной защиты в администрации Порздневского сельского поселения (далее: Администрация).
2. Настоящая Инструкция предназначена для уполномоченных работников Администрации: ответственного за обеспечение информационной безопасности, администратора безопасности информации и пользователей автоматизированных рабочих мест (далее - АРМ).
3. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях из сторонних организаций.
4. Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационной системы.

Вредоносная программа способна выполнять ряд функций, в том числе:

* скрывать признаки своего присутствия в программной среде рабочей станции;
* обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
* разрушать (искажать произвольным образом) код программ в оперативной памяти;
* сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
* искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

1. Основными задачами системы обеспечения антивирусной защиты являются:

* исключение или существенное затруднение противоправных действий в отношении информационной системы, содержащей защищаемую информацию;
* обеспечение условий для устойчивой бесперебойной работы АРМ.

1. Объектом защиты от воздействия вредоносных программ являются АРМ, оборудование, входящее в состав оборудования, подключенного к АРМ и машинные носители информации.
2. Обеспечение антивирусной защиты включает:

* регулярные профилактические работы;
* анализ ситуации проявления вредоносных программ и причины их появления;
* уничтожение вредоносных программ на АРМ;
* принятие мер по предотвращению причин появления вредоносных программ.

1.8. Для выполнения требований по антивирусной защите информационной системы используется специализированное программное обеспечение (ПО), обеспечивающее надежную ежедневную автоматическую антивирусную защиту и контроль чистоты информационных массивов данных от вредоносных программ.

* 1. 1.9. При возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь АРМ самостоятельно или с привлечением администратор безопасности информации проводит внеочередной антивирусный контроль рабочей станции.

1.10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан приостановить работу и немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности и администратора безопасности информации.

1.11. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя технологического оборудования и информационных массивов, проводится служебное расследование.

1.12. Результаты расследования причин появления и последствий воздействия вредоносных программ на рабочую станцию докладываются руководителю Организации с предложениями по принятию мер, предотвращающими в будущем повторение подобных фактов.

2. Требования к антивирусному программному обеспечению

1. Применение только лицензионного антивирусного ПО.
2. Возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макро-вирусы, объектов ActiveX, апплетов языка Java и т.п.), а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.
3. Исчерпывающий список защищаемых точек (автоматизированные рабочие места и т.д.) возможного проникновения вредоносных программ.
4. Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО.
5. Соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники.
6. Надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы, по возможности, в русскоязычной среде.
7. Наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

3. Мероприятия по управлению средствами антивирусного контроля

1. Администратор безопасности информации выполняет:

* установку средств антивирусной защиты на рабочую станцию, добавляемые в средства защиты информационной системы, в порядке, описанном в эксплуатационной документации;
* периодический контроль актуальности версий средств антивирусной защиты на объекте антивирусной защиты;
* периодический контроль выполнения задач постоянной защиты;
* периодический контроль актуальности версий антивирусных баз и модулей сканирования ПО;

1. Пользователь АРМ:

* выполняет обязательную антивирусную проверку любой информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (flash дисках, sd картах, магнитных дисках, лентах, CD-ROM и т.п.).
* не препятствует работе средств антивирусной защиты
* немедленно сообщает о подозрении на заражение или о факте заражения АРМ ответственному за обеспечение информационной безопасности, администратору безопасности информации.

1. Процесс управления системой антивирусной защиты включает в себя следующие действия администратора безопасности информации:

* внесение изменений в политику антивирусной защиты;
* управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты;
* мониторинг событий, информация о которых поступает от средств антивирусной защиты с объекта защиты;
* анализ и обработку сведений и автоматически формируемых отчетов , поступающих от средств антивирусной защиты.
  1. В случае заражения рабочей станции вредоносными программами администратор безопасности информации выполняет следующие действия:
* обновляет антивирусную базу объекта антивирусной защиты;
* проверяет состояние объекта антивирусной защиты, наличие заражения рабочей станции в случае обнаружения пораженных узлов;
* оперативно принимает меры по предотвращению распространения заражения вредоносными программами оборудования и машинных носителей информации и при необходимости отключает их от зараженной рабочей станции;
* по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность рабочей станции и передаёт её пользователю.

4. Ответственность пользователей

* Организация мероприятий по антивирусной защите возлагается на ответственного за обеспечение информационной безопасности
* Работы по функционированию и сопровождению системы антивирусной защиты возлагается на администратора безопасности информации.
* Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции несут пользователи.

Приложение 2

к постановлению администрации Порздневского

сельского поселения от 26.12.2022 №67

Инструкция по организации парольной защиты

1. Общие положения

Настоящая инструкция устанавливает основные правила парольной защиты и регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

* Компрометация - факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
* Пароль - признак субъекта доступа, предъявляемый совместно с идентификатором субъекта в процессе идентификации.

2. Порядок работы по обеспечению парольной защиты

1. Личные пароли должны генерироваться специальными программными средствами администратора безопасности информации либо задаваться пользователем самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее шести символов;

- в числе символов пароля обязательно должны присутствовать символы из следующих категорий: строчные буквы латинского алфавита, прописные буквы латинского алфавита, десятичные цифры (алфавит пароля не менее 30 символов);

- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ADMIN, SECRET, USER и т.п.);

- использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

- использование двух и более подряд одинаковых символов недопустимо;

- срок действия пароля задается администратором информационной безопасности, субъект обязан сменить пароль по истечению срока его действия;

- при смене пароля новое значение должно отличаться от предыдущего минимум в 6-ти символах;

- пользователь обязан сохранять в тайне свой личный пароль.

1. Хранение сотрудником (исполнителем) значений своих паролей на любом носителе не допускается.
2. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля
3. При получении пользователем доступа к информационной системе (ИС) функционирующей в организации должны применяться следующие правила
   * 1. Полная плановая смена паролей пользователей ИС должна проводиться по предложению администратора информационной безопасности и на основании распоряжения руководителя структурного подразделения
     2. Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором безопасности информации немедленно после окончания последнего сеанса работы данного пользователя.
     3. Внеплановая полная смена паролей всех пользователей ИС должна производиться в случае прекращения полномочий администратора безопасности информации (увольнение, переход на другую работу внутри Организации и другие обстоятельства).
     4. В ИС должна осуществляться идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа.
     5. Администратор безопасности информации устанавливает и реализует следующие функции управления учетными записями пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения, гостевая (анонимная), временная и (или) иные типы записей);

- объединение учетных записей в группы (при необходимости);

- верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

- заведение, активация, блокирование и уничтожение учетных записей пользователей;

- настройка допустимого количества неудачных попыток входа в систему пользователем, при превышении которого учетная запись пользователя блокируется на определенное Администратором безопасности время;

- пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, установленной в Учреждении;

- порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

- оповещение Администратора информационной системы, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

- предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе.

- Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

3. Компрометация паролей

* 1. Под компрометацией следует понимать следующее:

- физическая утеря носителя с парольной информацией;

- передача идентификационной информации по открытым каналам связи вне ИСПД;

- проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма, или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);

- перехват пароля при распределении идентификаторов;

- сознательная передача информации постороннему лицу.

* 1. Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен вводятся запасной или новый пароль;

- о компрометации немедленно оповещаются все участники обмена информацией.

4. Правила работы пользователей при применении парольной зашиты

* 1. При работе с парольной защитой пользователям запрещается:
* разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
* предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПД, посторонним лицам;
* записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.
  1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля, сейфе.
  2. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5. Ответственность пользователей

5.1.Организация мероприятий по парольной защите возлагается на ответственного за обеспечение информационной безопасности.

5.2. При наличии и использовании в организации информационных систем (ИС) с разграничением доступа пользователей, организационное и техническое обеспечение процессов генерации, создания, присвоения, использования, смены и прекращения, уничтожения идентификаторов пользователей и устройств во всех используемых ИС а также контроль за действиями пользователей при работе с паролями ИС возлагается на администратора безопасности информации.

5.3. Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль на администратора безопасности информации, и лица, ответственного обеспечение информационной безопасности.

Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения парольной защиты и требований настоящей Инструкции несут пользователи

Приложение 3

к постановлению администрации Порздневского

сельского поселения от 26.12.2022 №67

Правила обеспечение информационной безопасности

при использовании в работе персональных компьютеров и

локальной вычислительной сети

1. Общие положения

Настоящие правила описывают порядок эксплуатации персональных компьютеров (далее - ПК) и локальной вычислительной сети Администрации.

Настоящие правила предназначены для уполномоченных работников организации: ответственного за обеспечение информационной безопасности, администратора безопасности информации и пользователей автоматизированных рабочих мест (далее - АРМ).

Целью настоящих Правил является регулирование работы администратора безопасности информации и пользователей для поддержания необходимого уровня защиты информации, а конкретно предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации.

К работе в системе допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж

Пользователь имеет право использовать в работе предоставленные ему сетевые. Уполномоченные лица организации 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.

Передача электронных документов внутри организации производится только посредством общих папок, а так же средствами электронной почты, без участия физических магнитных носителей

2. Требования и ограничения

Каждый пользователь обязан:

- до включения оборудования проверить правильность расположения компьютерного оборудования: кабели электропитания оборудования должны находиться с тыльной стороны рабочего места;

- до включения оборудования проверить надежность подключения к компьютеру разъемов периферийного оборудования;

- начинать работу можно только после полной загрузки операционной системы и появления сообщения о вводе имени и пароля пользователя.

- во время работы не закрывать вентиляционные отверстия компьютерного оборудования;

- во время работы при необходимости временного прекращения работы корректно закрыть все активные программы;

- при оставлении рабочего места необходимо заблокировать ПК (win-L)

- хранить в тайне свой пароль (пароли);

- немедленно вызывать администратора безопасности информации при подозрении компрометации личных паролей или их утери, а также при обнаружении:

а) нарушений целостности пломб, наклеек на аппаратных средствах ПК или иных фактов совершения в его отсутствие попыток несанкционированного доступа к ПК;

б) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ПК;

в) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПК, выхода из строя или неустойчивого функционирования узлов ПК или периферийных устройств (дисководов, принтера и т.п.);

г) неизвестных/непонятных отводов кабелей и подключенных устройств.

Пользователям категорически запрещается:

- во время работы открывать защитные крышки компьютерного оборудования и прикасаться к элементам оборудования, ставшим доступным после вскрытия защитных крышек;

- во время работы переключать разъемы кабелей периферийного оборудования;

- удалять с корпуса наклейки с заводскими и лицензионными номерами.

- допускать посторонних на рабочее место.

- использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные и аппаратные средства,

- оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются;

- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию;

- предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок немедленно ставить в известность администратора безопасности информации.

- выкладывать важную информацию на общих ресурсах ЛВС. За размещение на общем ресурсе сети важной информации персональную ответственность несет пользователь, выложивший ее.

предпринимать какие-либо действия прямо или косвенно направленные на нарушение нормальной работы сетевого оборудования и разрушение общих информационных ресурсов.

Администратор безопасности информации обязан:

- осуществлять контроль над установленным на компьютере программным обеспечением

- принимать меры по ограничению возможностей несанкционированной установки программ (включая отключение дисководов, CD/DVD-приводов и USB-портов у пользователей, которые не должны по своим служебным обязанностям обмениваться информацией на внешних носителях

- доводить до ответственного за обеспечение информационной безопасности всю информацию о нарушениях связанных с обеспечением информационной безопасности.

3. Ответственность

Ответственный за обеспечение информационной безопасности обеспечивает контроль за ознакомлением и соблюдением работниками требований настоящих правил.

Пользователи несут персональную ответственность за обеспечение информационной безопасности при использовании ПК, и соблюдение требований настоящих правил.

Приложение 4

к постановлению администрации Порздневского

сельского поселения от 26.12.2022 №67

Правила работы с электронной почтой

1.Общие положения

Настоящие правила описывают порядок работы с электронной почтой в Администрации (ниже в тексте термин «электронная почта» следует читать - служебная электронная почта, служебный адрес электронной почты, служебный почтовый ящик и т.д.).

Настоящие правила предназначены для уполномоченных работников Администрации: ответственного за обеспечение информационной безопасности, администратора безопасности информации и пользователей автоматизированных рабочих мест (далее - АРМ).

Целью настоящих Правил является регулирование работы администратора безопасности информации и пользователей для поддержания необходимого уровня защиты информации, а конкретно предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации.

К работе в системе допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж.

Пользователь имеет право использовать в работе предоставленные ему электронную почту, средства и инструменты обработки электронной почты. Уполномоченные лица организации вправе ограничивать доступ к электронной почте вплоть до полной блокировки.

Электронная почта является собственностью Администрации и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика может быть проверено без предварительного уведомления сотрудника по требованию непосредственного либо вышестоящего руководителя.

2. Требования и ограничения

Каждый пользователь обязан:

- проводить проверку вложений во входящих сообщениях антивирусными средствами, даже если отправитель письма хорошо известен;

- для работы с электронной почтой применять средства и инструменты предоставленные Администрации (не обрабатывать электронную почту сторонними, публичными или личными средствами и инструментами, без предварительного согласования с руководителем и ответственным за обеспечение информационной безопасности);

- сообщать о любом подозрении компрометации электронной почты руководителю и ответственному за обеспечение информационной безопасности.

Пользователям категорически запрещается:

- использовать адрес электронной почты для оформления подписок

- осуществлять массовую рассылку почтовых сообщений рекламного характера

- рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете;

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

- распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т. д;

- распространять информацию ограниченного доступа, представляющую коммерческую тайну;

- предоставлять третьим лицам пароль доступа к своему почтовому ящику.

3. Ответственность

Ответственный за обеспечение информационной безопасности обеспечивает контроль за ознакомлением и соблюдением работниками требований настоящих правил.

Пользователи несут персональную ответственность за обеспечение информационной безопасности при работе с электронной почтой, и соблюдение требований настоящих правил.

Приложение 5

к постановлению администрации Порздневского

сельского поселения от 26.12.2022 №67

Правила обеспечения информационной безопасности

при использовании в работе глобальной вычислительной сети интернет и «социальных сетей»

1. Общие положения

Настоящие правила описывают порядок использования сети интернет, а также ресурсов называемых «социальные сети» в Администрации.

Настоящие правила предназначены для уполномоченных работников организации: ответственного за обеспечение информационной безопасности, администратора безопасности информации и пользователей автоматизированных рабочих мест (далее - АРМ).

Целью настоящих Правил является регулирование работы администратора безопасности информации и пользователей для поддержания необходимого уровня защиты информации, а конкретно предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации.

К работе в системе допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж.

Сеть интернет используется пользователем для получения информации в рамках исполнения должностных обязанностей. Уполномоченные лица организации вправе ограничивать доступ к сети интернет нормативными документами и техническими средствами, вплоть до полной блокировки.

2. Требования и ограничения при использовании в работе глобальной вычислительной сети интернет

Каждый пользователь обязан:

- для работы в сети интернет применять средства и инструменты предоставленные Администрацией;

- при подозрении несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет, сообщить руководителю и ответственному за обеспечение информационной безопасности;

Пользователям категорически запрещается:

- осуществлять действия, запрещенные законодательством Российской Федерации;

- отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации;

- распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылки или другие ссылки на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

- самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети интернет;

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;

- открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами;

- передавать информацию, обрабатываемую в Организации, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией

3. Требования и ограничения поведения пользователей в «социальных сетях»

Вы несете личную ответственность за все, что вы публикуете в своих аккаунтах в социальных сетях или в комментариях к постам других людей, где бы то ни было.

Упоминая Администрации в социальных сетях, постах и комментариях, вы всегда должны говорить только от своего лица и использовать местоимение «Я», а не «МЫ». От лица компании могут выступать только специально уполномоченные сотрудники.

Если вы увидели, что кто-то обсуждает в Сети организацию, не вступайте в полемику от имени Администрации. По возможности постарайтесь сообщить об этом специалисту.

Пользователям категорически запрещается:

- «постить» «скрины» служебных документов и содержимое экранов рабочих мониторов сотрудников.

- высказывать заявления любой окраски по вопросам: политики, национальности, сексуальной ориентации, религии.

Минимальные рекомендации для обеспечения информационной безопасности пользователям социальных сетей:

При регистрации в социальной сети лучше придумать случайный пароль, состоящий не менее чем из 6-7 знаков. Лучше всего, если для каждого сайта в сети у вас будут разные пароли.

Для выхода в социальные сети используйте только распространенные и доказавшие свою надежность браузеры.

Никогда не принимайте и не устанавливайте неизвестные файлы от людей, которых не знаете. Не открывайте подозрительные сообщения, в которых находятся ссылки на неизвестные ресурсы, и никогда не переходите по этим ссылкам.

Не устанавливайте приложения для социальных сетей.

Старайтесь не заходить на свои аккаунты в социальных сетях с чужих компьютеров.

Осторожнее размещайте информацию о себе в социальных сетях.

Иногда сообщения, отправленные вам якобы вашими друзьями, могут быть отправлены злоумышленниками, которые взломали их аккаунты. Поэтому, если сообщение кажется, вам подозрительным или содержит подозрительную ссылку, свяжитесь с другом напрямую или по телефону, чтобы убедиться, что сообщение действительно пришло от него.

Не позволяйте социальным сетям сканировать адресную книгу вашей электронной почты.

Следите за тем, кого вы добавляете в друзья.

Постарайтесь не пользоваться социальными сетями на своем рабочем месте.

4. Ответственность

Ответственный за обеспечение информационной безопасности обеспечивает контроль за ознакомлением и соблюдением работниками требований настоящих правил.

Пользователи несут персональную ответственность за обеспечение информационной безопасности при работе с сетью интернет, а также ресурсами называемыми «социальные сети».