УТВЕРЖДЕНА
приказом МОУ ООШ
пст. Русаново
от «17» января 2019 г. № 5
(приложение к приказу)

ИНСТРУКЦИЯ

администратора безопасности информации, обрабатываемой в государственных информационных системах

1. Общие положения

Настоящая инструкция администратора безопасности информации, обрабатываемой в государственных информационных системах (далее - Инструкция) определяет функции, права и обязанности администратора (администраторов) безопасности информации, обрабатываемой в государственных информационных системах (далее – ГИС), а также устанавливает требования и рекомендации к администрированию средств защиты информации, задействованных в подсистеме обеспечения информационной безопасности.

Администратор (администраторы) безопасности назначается в целях осуществления функций по обеспечению контроля над исполняемыми процессами и мерами информационной безопасности, обозначенными федеральным законодательством Российской Федерации, а также организационно распорядительными и методическими документами федеральных органов исполнительной власти Российской Федерации, на которых возложены функции по осуществлению реализации государственной политики, организации межведомственной координации и взаимодействия, специальных и контрольных функций в области государственной безопасности по вопросам обеспечения защиты информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации.

В своей деятельности администратор безопасности руководствуется следующими нормативными правовыми актами и организационно распорядительными документами:

1) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

3) Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014);

4) Методические рекомендации Управления ФСТЭК России по Северо-Западному федеральному округу по совершенствованию системы защиты информации в органах государственной власти, органах местного самоуправления и подведомственных им организациях, находящихся в пределах Северо-Западного федерального округа на 2018 год (с приложениями).

2. Должностные обязанности

Администратор безопасности, в рамках вверенных ему полномочий, обязан:

соблюдать требования настоящей Инструкции, а также иных инструкций и регламентов, утвержденных в организации в части его касающейся;

знать информационные технологии, а также основные процессы и этапы обработки информации в ГИС организации;

поддерживать в актуальном состоянии организационно-распорядительные документы, регламентирующие правила обработки информации в ГИС, а также проводить ознакомление сотрудников организации с данными документами;

обеспечивать постоянный контроль над исполнением мер федерального законодательства и изданных в соответствии с ним подзаконных актов в области защиты информации, обрабатываемой в ГИС;

принимать участие в мероприятиях, направленных на повышение эффективности принятых мер по защите информации;

незамедлительно уведомлять руководителя организации или лицо его замещающее обо всех нарушениях функционирования ГИС;

незамедлительно сообщать руководителю организации или лицу его замещающему об утрате носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других

фактах, которые могут привести к нарушению состояния безопасности ГИС организации.

Администратору безопасности запрещается:

разглашать защищаемую информацию, в том числе информацию о составе и особенностях функционирования средств защиты информации, доверенную или ставшую ему известной вследствие исполнения должностных обязанностей;

не сообщать устно или письменно, не передавать третьим лицам (с использованием информационных технологий или без) и не раскрывать публично защищаемую информацию (в том числе ее опубликование или размещение в открытых источниках, интернет ресурсах, социальных сетях, системах мгновенного обмена электронными сообщениями и т.п.) без соответствующего разрешения (распоряжения) руководителя организации или лица его замещающего;

использовать, прямо или косвенно, защищаемую информацию для осуществления деятельности, не связанной с выполнением возложенных на него должностных обязанностей;

фиксировать учетные данные пользователя: пароли, идентификаторы, ключи и др., ставшие ему известными в рамках исполнения служебных обязанностей.

При необходимости покинуть автоматизированное рабочее место (АРМ) администратор безопасности обязан принять меры по обеспечению контроля за его функционированием во время своего отсутствия, а именно, осуществить блокировку доступа к операционной системе АРМ. В случае отсутствия иных лиц, имеющих право самостоятельного доступа в помещение с размещенным АРМ, администратор безопасности обязан закрыть окна и двери, опечатать помещение.

3. Права

Администратор безопасности имеет право:

требовать отключения от сети и отстранения от работы в ГИС пользователей, предпринявших попытки несанкционированного доступа (в том числе успешные) к защищаемым ресурсам организации или компонентам подсистемы обеспечения информационной безопасности ГИС, или нарушивших другие требования информационной безопасности вплоть до выяснения всех обстоятельств данного инцидента;

участвовать в любых проверках работоспособности компонентов подсистемы обеспечения информационной безопасности (в рамках вверенных ему обязанностей);

вносить предложения по совершенствованию подсистемы обеспечения информационной безопасности, доводить данные сведения до руководителя организации или лица его замещающего;

проходить курсы повышения квалификации в области защиты информации, обрабатываемой в ГИС.