ПРИНЯТО
Общим собранием работников школы
Протокол № 1
от «27» 03 2020 г
председатель Общего собрания
работников школы
С.Ф.Рафикова

УТВЕРЖДАЮ
Директор МБОУ «Старо-
Уруссинская СОШ»
З.М.Фаздуллина
Введено в действие приказом
№ 41 от «27» 03 2020г

ПОЛОЖЕНИЕ
об Администраторе информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Старо-Уруссинская средняя общеобразовательная школа» Ютазинского муниципального района Республики Татарстан

1. Общие положения

1.1 Настоящее положение разработано на основе "Политики информационной безопасности.

1.2. Положение определяет основные задачи, функции, обязанности, права и ответственность Администратора информационной безопасности автоматизированной системы (далее – администратор ИБ).

1.3. Администратор ИБ назначается приказом и является лицом, выполняющим функции по защите информации обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в пределах зоны своей ответственности.

1.4. В своей деятельности Администратор ИБ руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты информации и контролирует их выполнение пользователями локальной вычислительной сети (далее – ЛВС), систем управления базами данных (далее – СУБД) и пользователями автоматизированного рабочего места (далее – АРМ).

2. Задачи и функции Администратора ИБ

2.1Основными задачами Администратора ИБ являются:

- контроль эффективности защиты информации.
- сопровождение СЗИ от несанкционированного доступа (*далее* – **НСД**) и основных технических средств и систем (*далее* – **ОТСС**);
- контроль разграничения доступа;

2.2 Для выполнения поставленных задач на Администратора ИБ возлагаются следующие *функции:*

2.2.1 Контроль соответствия действий пользователей АРМ требованиям «Политики информационной безопасности» на всех стадиях жизненного цикла АРМ.

2.2.2Участие на стадии проектирования (внедрения) АРМ в разработке технологии обработки информации ограниченного доступа (*далее* – **информации**) по вопросам:

- организации порядка учета, хранения и обращения с документами и носителями информации;
- определения степени секретности отдельных документов, носителей и массивов информации;
- подготовки инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей АРМ по вопросам защиты информации, а также ответственных по защите информации в процессе автоматизированной обработки информации.

2.2.3Сопровождение СЗИ от НСД к ней, в том числе средств криптографической защиты информации, на стадии эксплуатации АРМ, включая ведение служебной информации СЗИ от НСД (управление ключевой системой, сопровождение правил разграничения доступа), оперативный контроль за функционированием СЗИ от НСД.

2.2.4Контроль соответствия общесистемной программной среды стандарту (контроль целостности программного обеспечения) и проверка включаемых в АРМ новых программных средств.

2.2.5.Оперативный контроль за ходом технологического процесса обработки информации.

2.2.6Методическое руководство работой пользователей АРМ в вопросах обеспечения информационной безопасности.

3. Задачи и функции Администратора ИБ

3.1 Для реализации поставленных задач и возложенных функций Администратор ИБ ОБЯЗАН:

3.1.1 Сопровождать СЗИ от НСД и ОТСС:

3.1.1.1 Вести учет и знать перечень установленных в подразделениях ОТСС, СЗИ от НСД и перечень задач, решаемых с их использованием.

3.1.1.2 Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на рабочих станциях (*далее* – **РС**) специальных программных и программно-аппаратных СЗИ от НСД.

3.1.1.3 Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств, защищенных РС и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств АРМ.

3.1.1.4 Периодически проверять состояние используемых СЗИ от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

3.1.1.5 Контролировать комплектность средств вычислительной техники (далее – СВТ) и изменения аппаратно-программной конфигурации.

3.1.1.6 Периодически – не реже 1 раза в год - контролировать целостность печатей (пломб, наклеек) на устройствах, защищенных РС, где таковые печати (пломбы, наклейки) имеются.

3.1.1.7 Проводить периодический инструктаж пользователей АРМ по правилам работы с используемыми СЗИ.

3.1.2 Организовывать разграничения доступа:

3.1.2.1 Знать перечень защищаемых информационных ресурсов и участвовать в разработке системы их защиты.

3.1.2.2 Осуществлять учет и периодический контроль состава и полномочий пользователей различных РС АРМ.

3.1.2.3 Контролировать и требовать соблюдение установленных правил по организации парольной защиты в АС.

3.1.2.4 Осуществлять оперативный контроль работы пользователей, защищенных РС, анализировать содержимое журналов событий операционных систем (*далее* - **ОС**) и СЗИ от НСД этих РС, адекватно реагировать на возникающие нештатные ситуации.

3.1.2.5 Принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и РС АРМ. Контролировать соблюдение сотрудниками подразделений автоматизации утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств РС и серверов.

3.1.2.6 Контролировать выполнение требований по обеспечению безопасности информации при организации технического обслуживания РС и отправке их в ремонт (контролировать стирание информации на магнитных носителях).

3.1.2.7 Организовывать учет, хранение, прием и выдачу персональных идентификаторов, осуществлять контроль правильности их использования.

3.1.2.8 Осуществлять периодический контроль порядка учета, создания, хранения и использования резервных и архивных копий массивов данных.

3.1.2.9 По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ от НСД, установленных на РС АРМ.

3.1.2.10 Требовать от пользователей стирания остаточной информации на несъёмных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки РС.

3.1.2.11 Контролировать обеспечение защиты конфиденциальной информации при взаимодействии абонентов с информационными сетями общего пользования.

3.1.3 Контролировать эффективность защиты информации:

3.1.3.1 Проводить работу по выявлению возможности вмешательства в процесс функционирования АРМ и осуществления НСД к информации и техническим средствам РС.

3.1.3.2 Докладывать руководству о выявленных угрозах безопасности информации, обрабатываемой в АРМ, об имевших место попытках НСД к информации и техническим средствам РС.

3.1.3.3 Проводить занятия с администраторами и пользователями АРМ по правилам работы на РС, оснащенных СЗИ НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности защиты информации.

3.1.3.4 Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в АРМ.

3.2 Администратору ИБ ЗАПРЕЩАЕТСЯ:

3.2.1 Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ее модификации, копирования, уничтожения, блокирования доступа к информации;

3.2.2 Использовать в своих и в чьих-либо личных интересах ресурсы АРМ, предоставлять такую возможность другим;

3.2.3 Выключать СЗИ от НСД без санкции руководства;

3.2.4 Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки, другую информацию о структуре, составе, программном и техническом обеспечении и особенностях функционирования и защиты АРМ;

3.2.5 Производить в рабочее время без санкции руководства и предупреждения пользователей действия, приводящие к сбою, остановке, замедлению работы АРМ, блокированию доступа, потере информации;
3.2.6 Нарушать правила эксплуатации оборудования АРМ;

4. Права и ответственность Администратора ИБ

4.1. Администратор ИБ имеет право:
4.1.1. Анализировать права доступа к ресурсам на серверах АРМ и РС пользователей.
4.1.2. Требовать от пользователей АРМ выполнения инструкций по обеспечению безопасности и защите информации в АРМ
4.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов АРМ.
4.1.4. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим докладом руководству.
4.1.5. Производить анализ защищенности АРМ путем применения специального ПО, осуществления попыток взлома системы защиты АРМ. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным согласованием с начальником управления автоматизации.
4.1.6. Вносить свои предложения по совершенствованию мер защиты в АРМ.

4.2. Администратор ИБ несет ответственность за:
4.2.1. Реализацию принятой политики информационной безопасности;
4.2.2. Программно-технические и криптографические СЗИ, а также за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

Список сокращений

АРМ – автоматизированное рабочее место .
ИБ – информационная безопасность.
Информация – в документе: информация, подлежащая защите, представленная в виде электронных документов или иных совокупностей данных, хранящаяся на электронных носителях и/или циркулирующая в сетях передачи данных организации.
ЛВС – локальная вычислительная сеть.
НСД – несанкционированный доступ к информации.
ОС – операционная система.
ОТСС – основные технические средства и системы.
РС – рабочая станция, компьютер.
СВТ – средство вычислительной техники.
СЗИ – средства защиты информации.
СУБД – система управления базами данных.

Пронумеровано и прошнуровано
5 (пять) листов
Директор МБОУ «Старо-Уруссинская СОШ» З.М.Фаздуллина