МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ГИМНАЗИЯ № 2»
(МБОУ «ГИМНАЗИЯ № 2»)
«2 №-а ГИМНАЗИЯ» МУНИЦИПАЛЬНӦЙ ВЕЛӦДАН СЬӦМКУД УЧРЕЖДЕНИЕ

УТВЕРЖДАЮ
Директор МБОУ «Гимназия № 2»
_____ Н.В. Яловая
приказ МБОУ «Гимназия № 2»
от 30.12.2015 № 458

ИНСТРУКЦИЯ
администратора информационной системы персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор автоматизированной системы (далее – Администратор) назначается приказом директора.

1.2. Администратор подчиняется директору.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, Положением об обработке персональных данных, руководящими и нормативными документами ФСТЭК и ФСБ России и документами организации, регламентирующими обработку и защиту конфиденциальной информации.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке конфиденциальной информации.

1.5. Администратор несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн в соответствии с действующим законодательством Российской Федерации и локальными нормативными актами.

1.6. Методическое руководство работой Администратора осуществляет лицо, ответственное за организацию обработки персональных данных.

2. ОСНОВНЫЕ ПОНЯТИЯ

Для целей Инструкции используются следующие:

2.1. персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.2. оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

2.3. обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

2.4. автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

2.5. распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.6. предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

2.7. блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.8. уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

2.9. обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

2.10. информационная система персональных данных (далее - ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

2.11. конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытия третьим лицам и распространения без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

2.12. документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

2.13. средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

2.14. информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

2.15. контролируемая зона - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посетителей, а также транспортных, технических и иных материальных средств.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА

Администратор обязан:

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн: программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО); аппаратных средств; аппаратных и программных средств защиты.

3.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

3.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа.

3.5. Вести учет пользователей ИСПДн.

3.6. Вести электронный журнал учета запросов пользователей ИСПДн на получение конфиденциальной информации.

3.7. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

3.8. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

3.9. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.10. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

3.11. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователем ИСПДн.

3.12. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

3.13. Информировать ответственного за организацию обработки персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

3.14. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

3.15. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

3.16. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

3.17. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

4. Парольная политика

4.1. Общие требования к паролям:

4.1.1. минимальное требование: буквенно-цифровой пароль. желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # $ % ^ & * ( ) _ - + = | \ ? / . , : ; '] [{ } < > . и т.п.);

4.1.2. минимальная длина пароля: не менее 6 (шести) символов;

4.1.3. максимальный срок действия пароля: 90 суток;

4.1.4. запрет использования трех ранее использовавшихся паролей;

4.1.5. пароль пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о пользователе, доступную другим лицам;

4.1.6. запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

4.1.7. запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например: 1234567, qwerty и т.п.).

4.2. Обязанности ответственного по парольной защите:

4.2.1. осуществлять внеплановую смену пароля по распоряжению начальника отдела асу (в соответствии с заявкой на сброс пароля);

4.2.2. осуществлять внеплановую смену пароля при экстренном случае согласно пункту

4.2.3. обеспечить проверку паролей на соответствие требованиям п. 2.1.;

4.2.4. обеспечить принудительную смену первоначального значения пароля при первом входе в систему;

4.2.5. обеспечить запрос на смену паролей перед истечением срока действия;

4.2.6. обеспечить автоматическую блокировку учётной записи при истечении срока действия пароля;

4.2.7. обеспечить автоматическую блокировку учётной записи на 30 минут после неверных попыток введения пароля (не менее 5 попыток);

4.2.8. уведомлять пользователя в произвольной форме о выполнении задания по направленной заявке на сброс пароля (с ознакомлением с начальным значением пароля);

4.2.9. не разглашать данные учетных записей пользователей.

4.3. Существующие автоматизированные системы при наличии в них штатных средств настройки политики паролей приводятся в соответствии с настоящими требованиями.

4.4. Внеплановая смена пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую должность внутри Гимназии и т.п.) должна производиться ответственным за парольную защиту после окончания последнего рабочего дня сотрудника (перед увольнением, переходом на новую должность).

4.5. При увольнении, переходе на новую должность сотрудника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

4.6. Для создания значений паролей могут применяться специальные программные средства (генераторы паролей). Программы для осуществления таких операций выбираются ответственным по парольной защите.

5. АНТИВИРУСНАЯ ЗАЩИТА

5.1. К использованию в Гимназии допускаются только лицензионные антивирусные средства.

5.2. Программное обеспечение антивирусные средства выбирается с учетом:

5.2.1. возможности централизованного дистанционного управления;

5.2.2. цены, качества поиска, обнаружения, лечения, локализации ВП, а также влияния на производительность компьютера и иных средств вычислительной техники, на которых будет установлены антивирусные средства.

5.3. Ответственный за антивирусную защиту организует и обеспечивает установку и настройку антивирусных средств на серверах, рабочих станциях в соответствии с документацией поставщика антивирусных средств.

5.4. Своевременное обновление баз данных сигнатур антивирусных средств является неотъемлемой частью обеспечения эффективной защиты информации от вирусных программ.

5.5. Обновление баз данных сигнатур антивирусных средств должно производиться не реже 1 раза в день (или по мере выпуска (опубликования) указанных баз данных сигнатур).

5.6. Обязательному контролю на наличие вирусов подлежат все компоненты автоматизированной системы, связанные с обработкой и хранением информации: файловые серверы, серверы баз данных, серверы приложений, серверы резервного копирования, серверы электронной почты, серверы терминалов, рабочие станции, рабочие станции мобильных пользователей; сменные носители информации (магнитные и оптические диски, флеш-накопители и т.п.).

5.7. Обязательному контролю подлежит любая информация (файлы любых форматов), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных и оптических дисках, флеш-накопителях и т.п.).

5.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов, программных закладок.

5.9. Настройка антивирусных средств должна обеспечивать автоматический контроль защиты от вирусов при каждой перезагрузке компьютера.

5.10. Плановое профилактическое сканирование на наличие вирусов всех дисков и файлов рабочих станций и серверов должно производиться в автоматическом режиме (не менее одного раза в неделю). Для этого ответственным за антивирусную защиту настраиваются средства планирования запуска задач.

5.11. Плановое профилактическое антивирусное сканирование серверов рекомендуется проводить в часы минимальной их загрузки (в ночное время), рабочих станций – в обеденное время.

5.12. Обязанности ответственного за антивирусную защиту:

5.12.1. осуществляет управление конфигурацией и логической структурой всего программного обеспечения антивирусных средств;

5.12.2. осуществляет распространение обновлений антивирусных баз сигнатур антивирусных средств на серверах и рабочих станциях в автоматическом режиме;

5.12.3. если обновления баз данных сигнатур антивирусных средств невозможно распространять в автоматическом режиме, то обновления устанавливаются в ручном режиме не реже одного раза в неделю;

5.12.4. ограничивает доступ пользователей к установленным на рабочей станции антивирусным средствам;

5.12.5. планирует мероприятия по защите от вредоносных программ;

5.12.6. обеспечивает настройку антивирусных средств на автоматическое обновление и периодическую плановую проверку на вирусы.

6. ОТВЕТСТВЕННОСТЬ

6.1. Администратор несет персональную ответственность за свои действия или бездействие, которые повлекут за собой разглашение конфиденциальной информации, а также за нарушение нормального функционирования информационных систем или ее отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными актами Гимназии.