ПРИНЯТО
Протокол заседания педагогического совета от 28.08.2020 №1

УТВЕРЖДАЮ:
приказом директора от 29.08.2020 г. № 86
Директор _____ Р.М.Магомедов

Положение об организации работ по обеспечению безопасности информации в Муниципальном бюджетном общеобразовательном учреждении «Могилёвская средняя общеобразовательная школа им.Н.У.Азизова»

1. Общие положения

Настоящее Положение определяет основные мероприятия и порядок проведения работ по обеспечению безопасности информации (ОБИ) в МБОУ Могилёвская СОШ им.Н.У.Азизова (далее – Организация).

Настоящие Положение разработано на основании требований законодательства РФ в области информационной безопасности, нормативных и методических документов уполномоченных органов (ФСТЭК России, ФСБ России), а также правовых актов автономного округа, действующих на момент разработки документа.

В настоящем Положении используются термины и определения, установленные законодательством Российской Федерации, национальными стандартами вобласти защиты информации.

В организации обрабатывается общедоступная информация и информация ограниченного доступа, не составляющая государственную тайну, в том числе служебная информация (документы с пометкой «ДСП») и персональные данные (ПДн).

Автоматизированная обработка информации осуществляется с использованием средств вычислительной техники (СВТ) и различных информационных систем (ИС) на автоматизированных рабочих местах (АРМ пользователей) и серверах организации.

Организация, как обладатель информации ограниченного доступа, обязана принимать меры по защите информации и ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Требования к ОБИ формируются на основании установленных классов защищённости ИС (уровня защищенности ПДн) и перечня актуальных угроз безопасностиинформации.

Требования ОБИ реализуются комплексом организационных и техническихмер, средств и механизмов защиты информации, определенных в документации системы защиты информации (СЗИ).

Настоящие Положение обязательно для исполнения всеми государственными гражданскими служащими и иными работниками организации (далее – работники).

2. Порядок организации работ по обеспечению безопасности информации

С целью организации работ по защите информации приказом назначается должностное лицо, ответственное за защиту информации.

Функции, решаемые задачи и обязанности ответственного за защиту информации определены в инструкции лица, ответственного за

защиту информации.

Непосредственное выполнение работ по реализации требований и мер безопасности информации в организации осуществляет администратор безопасности (АБИ), назначаемый приказом руководителя организации. Функции, решаемые задачи и обязанности АБИ определены инструкцией.

Реализация требований ОБИ осуществляется всеми работниками организации (администраторами, пользователями, эксплуатационным персоналом).

Обязанности и ответственность пользователей по ОБИ при ее обработкеопределены в Инструкции пользователя.

Работы по ОБИ в организации осуществляются согласно Плану проведениямероприятий ОБИ организации.

Все работы ОБИ подлежат учету в Журнале учета мероприятий по ОБИ.

3. Технологический процесс обработки информации

Технические средства и системы обработки информации (ТС), места их размещения, программное обеспечение, используемое для обработки информации, а также используемые средства защиты информации и их характеристики подлежат учёту в Техническом паспорте объекта информатизации (ОИ). Ответственность за ведение Технического паспорта ОИ и актуализацию сведений в нём возлагается на АБИ.

Все ТС организации размещены в пределах контролируемой зоны (КЗ). Режим обработки информации многопользовательский с разграничение прав доступа.

Обработка информации в организации осуществляется в соответствии с Положением о порядке работы с информационными ресурсами.

Работа с информационными ресурсами организация осуществляется в соответствии с правами разграничения доступа. Правила разграничения доступа назначаются администраторами. Доступ к информационным ресурсам осуществляется при помощи учётных записей пользователей.

Обработка информации предусматривает следующие действия с данными: сбор, накопление , хранение, использование, уточнение, передача, удаление (уничтожение). Новые данные вводятся вручную, посредством клавиатурного ввода, а также путём считывания в электронном виде.

Пользователи имеют право постоянного хранения файлов с данными на:

- жёстком диске АРМ пользователя;
- учтённом съёмном носителе информации (USB-накопители, оптические диски, гибкие магнитные диски).

Доступ к жесткому диску АРМ пользователя разрешен только АБИ. Учтенные съёмные носители информации выдаются пользователю под роспись.

Доступ к АРМ пользователей производится по идентификатору (логину) и паролю в соответствии с требованиями парольных политик организации.

На АРМ пользователей устанавливается лицензионное либо свободно распространяемое общесистемное ПО, согласованное к использованию Департаментом информационных технологий и связи автономного округа.

Обработка информации на АРМ пользователей осуществляется с

использованием специализированного прикладного ПО и web-браузера.

Пользователи имеют доступ к ресурсам сети «Интернет» со своих АРМ.

В качестве вспомогательного средства для разработки документов на АРМ пользователей установлен программный пакет семейства Microsoft Office.

Копии установленного на АРМ пользователей ПО хранятся у АБИ.

Обработка служебной информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (документов с пометкой «для служебного пользования») производится только на учтённых съёмных машинных носителях информации (МНИ). Порядок и условия обработки служебной информации ограниченного доступа на АРМ пользователей определены в инструкции пользователю.

4. Система защиты информации

Перечень объектов доступа

Объектами доступа являются:

- ТС, включая средства отображения информации;
- помещения, в которых размещены ТС;
- носители информации, включая съёмные носители информации и жёсткие магнитные диски (далее – ЖМД);
- базы данные (далее – БД) и каталоги файлов на съёмных носителях информации и ЖМД;
- общесистемное и специальное ПО, предназначенное для обработки информации и разработки документов;
- программные средства, осуществляющие функции по защите информации, а также функции контроля безопасности;
- каналы информационного обмена и телекоммуникации.

Перечень субъектов доступа

Субъектами доступа к защищаемой информации на ОИ являются:

- администратор безопасности информации;
- системный администратор;
- пользователи, работающие на АРМ;
- процессы, выполняемые от имени АБИ, системного администратора и пользователей при обработке информации и настройке средств защиты информации.

Штатные средства доступа к информации

В качестве штатных средств доступа на ОИ предусмотрены:

- стандартные средства ОС Windows;
- программные из пакета MS Office;
- система управления базами данных (далее – СУБД) «Lotus Notes»;
- web-браузер;
- программы из пакета антивируса;
- средства настройки и контроля функций СЗИ.

Объекты защиты организации:

- ТС (в т.ч. СВТ, машинные носители информации (МНИ), средства и системы связи передачи данных);
- информация, хранящаяся и обрабатываемая на ТС;
- общесистемное, прикладное, специальное ПО;
- средства защиты информации.

Требования к средствам защиты информации

Все используемые программные и аппаратные СЗИ имеют действующие сертификаты на соответствие требованиям по безопасности информации, установленные Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю России.

Класс защищённости применяемых средств защиты информации должен соответствовать классу защищенности средств и систем обработки информации.

При обмене информацией между организацией и внешними по отношению к ней информационными системами, а также при передаче данных по кабельным системам, расположенным в пределах КЗ и не защищённым от НСД к информации организационно-техническими мерами, для обеспечения конфиденциальности информации требуется применение СЗКИ.

Установку и настройку СЗИ разрешается проводить только АБИ.

Эксплуатация СЗИ должна осуществляться в строгом соответствии с правилами, установленными в Инструкции по эксплуатации СЗИ.

Порядок учёта, хранения и использования СКЗИ, криптографических ключей (ключей электронной подписи, ключей шифрования), а также порядок изготовления, смены, уничтожения и действия при компрометации криптографических ключей определён в Инструкции по работе с СКЗИ.

Правила разграничения доступа

средствами СЗИ реализованы правила разграничения доступа, при которых каждый пользователь имеет доступ к:

- средствам ОС, обеспечивающим запуск и функционирование АРМ;
- средствам разработки документов;
- средствам антивирусного контроля;
- прикладному ПО;
- персональному каталогу на ЖМД, предназначенному для хранения информации;
- внешним накопителям данных, предназначенных для хранения информации;
- устройствам и средствам их программной поддержки, необходимым для работы с документами.

Доступ к средствам настройки и изменения полномочий доступа в СЗИ имеет только АБИ. Операции доступа к объектам доступа документируются средствами регистрации и учёта.

5. Средства защиты информации

Для защиты информации от несанкционированного доступа и воздействия вредоносных программ, на всех ТС организации применяются сертифицированные средства защиты информации от несанкционированного доступа (СЗИ от НСД) и средства антивирусной защиты (САВЗ).

Для защиты информации передаваемой по незащищенным каналам связи за пределы КЗ (во внешние системы) применяются средства криптографической защиты информации (СКЗИ). В установленных случаях могут использоваться средства электронной подписи.

СКЗИ и их носители подлежат учету в Журнале по экземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. При этом программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

В локальной вычислительной сети (ЛВС) организации для обеспечениябезопасности периметра ЛВС применяются сертифицированные

средства межсетевогоэкранирования и обнаружения вторжений.

Для контроля защищенности ЛВС используется сетевой сканер безопасности.

Контроль настройки и работы используемых в организации средств защиты информации осуществляет АБИ.

6. Реализация мер защиты

Идентификация и аутентификация субъектов доступа и объектов доступа

Применяемые на ОИ меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Идентификация и проверка подлинности субъектов доступа при входе в систему осуществляется СЗИ от НСД с использованием персональных идентификаторов, а также по имени (логину) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

СЗИ от НСД не позволяет использовать для входа в систему незарегистрированные идентификаторы.

Правила и требования к парольной защите определены в Инструкции по организации парольной защиты.

Программы, тома, каталоги, файлы, записи, поля записей, терминалы, компьютеры (АРМ), узлы сети, каналы связи, внешние устройства, подключённые к АРМ, идентифицируются по именам при обращении к ним при помощи средств ОС и СЗИ. Правильность предоставления доступа в соответствии с установленными правами субъектов по отношению к конкретным объектам (каталогам, устройствам) обеспечивается СЗИ и используемыми на ОИ сетевыми политиками безопасности.

Управление доступом субъектов доступа к объектам доступа

Применяемые меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных на ОИ правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.

Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей на ОИ и выдача (замена) пользовательских персональных идентификаторов для СЗИ от НСД, осуществляется АБИ и системным администратором в соответствии с правилами и процедурами, определёнными в Инструкции по управлению доступом к техническим средствам и информационным ресурсам.

На ОИ реализован дискреционный метод разграничения доступа. В системе задействована функция блокирования органов управления АРМ при временном оставлении рабочего места. При использовании незарегистрированного пароля, либо пароля, зарегистрированного не для текущего пользователя, разблокировка системы невозможна. В системе применяется ограничение неуспешных попыток входа в систему. При превышении установленного количества неуспешных попыток входа система блокируется.

Ограничения программной среды

Цель принятия мер по ограничению программной среды – обеспечение установки и (или) запуска только разрешённого к использованию в

организации программного обеспечения и исключения возможности установки и (или) запуска запрещённого к использованию на ОИ программного обеспечения.

Контроль установки (инсталляции) разрешённого к использованию ПО и (или) его компонентов осуществляется АБИ и системным администратором на основе журналов регистрации событий ОС и средств антивирусного контроля. АРМ.

Пользователи АРМ не имеют права самостоятельно устанавливать ПО.

Установка ПО на АРМ пользователей производится в соответствии с требованиями и правилами, установленными в Инструкции по модификации технических и программных средств.

Защита машинных носителей информации

Защита машинных носителей информации (средства обработки (хранения) информации, съёмные машинные носители информации) обеспечивается организационно-режимными мероприятиями. Цель принятия мер по защите МНИ – исключение возможности несанкционированного доступа к МНИ и хранящейся на них информации, а также несанкционированное использование съёмных МНИ.

При передаче МНИ межу пользователями или в сторонние организации для ремонта или утилизации производится уничтожение (стирание) информации, а также контроль уничтожения (стирания).

Порядок учёта, хранения и использования съёмных МНИ (ГМД, USB-накопители и т.д.) определён в Инструкции по порядку учёта, хранения и обращения со съёмными носителями информации.

Регистрация событий безопасности

Принимаемые меры по регистрации событий безопасности позволяют обеспечить сбор, запись, хранение и защиту информации о событиях безопасности, а также возможности просмотра и анализа информации о таких событиях.

Регистрация событий безопасности обеспечивается сертифицированными средствами защиты информации АРМ и серверов.

Регистрация, учёт и порядок реагирования на события безопасности регламентируются Положением о порядке выявления и реагирования на инциденты информационной безопасности.

Антивирусная защита

Целью принятия мер по антивирусной защите является обеспечение обнаружения компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации СЗИ, а также реагирование на обнаружение этих программ и информации.

САВЗ установлены на всех АРМ и серверах, обрабатывающих информацию.

Применение САВЗ решает следующие задачи:

- автоматическое сканирование АРМ на наличие вирусных программ;
- автоматическое блокирование обнаруженных вирусных программ путём их удаления из программных модулей или уничтожения;
- проведение регулярного сканирования АРМ на наличие вирусов;
- реализация механизма обновления базы данных признаков вредоносных компьютерных программ (вирусов);

– ведение журналов событий безопасности.

Все используемые в организации МНИ подвергаются обязательному контролю на наличие компьютерных вирусов при помощи антивирусной программы. ЖМД находится под контролем антивирусной программы постоянно. При обнаружении вирусного кода он удаляется из программы. АБИ и (или) системным администратором периодически проводится антивирусный контролю ЖМД по расширенному алгоритму.

Обновление БД антивирусного средства производится по мере выпуска данных обновлений производителем.

Правила и требования, регламентирующие антивирусную политику определены в Инструкции по организации антивирусной защиты.

Контроль (анализ) защищённости информации

Мероприятия, проводимые в целях контроля и анализа защищённости информации, включают в себя:

– контроль состава ТС, ПО и СЗИ;
– выявление, анализ и устранение уязвимостей ПО и СЗИ;
– контроль установки обновлений ПО, включая ПО СЗИ;
– контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;
– контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации полномочий пользователей и правил разграничения доступа пользователей в системе.

Используемые средства регистрации и учёта событий безопасности СЗИ позволяют АБИ контролировать неизменность конфигурации серверов, АРМ, файлов и реестров используемого ПО.

АБИ проводит периодическое обслуживание и тестирование функций СЗИ.

Порядок выполнения работ по выявлению, анализу и устранению уязвимостей ПО и СЗИ определён в Положении по организации контроля (анализа) защищённости.

Обеспечение целостности программного обеспечения и информации

Контроль целостности ПО (в т.ч. ПО СЗИ), установленного на АРМ пользователей и серверах, осуществляется средствами сертифицированных СЗИ и функциональными возможностями ОС АРМ и серверов.

В целях обеспечения возможности восстановления ПО, в случае возникновения нештатных ситуаций, организовано хранение:

– дистрибутивов используемого системного и прикладного ПО;
– дистрибутивов с ПО для СЗИ;
– файлов, содержащих конфигурации и настройки СЗИ.

Для обеспечения возможности восстановления информации, содержащейся в файлах, папках и БД, выполняется периодическое резервное копирование критически важных информационных ресурсов на внешние системы хранения данных.

Обеспечение доступности информации

Доступность информации обеспечивается:

– использованием отказоустойчивых ТС;
– выявлением, анализом и устранением уязвимостей ПО;
– резервированием ТС, ПО и каналов передачи информации;
– периодическим резервным копированием информации.

На основе мониторинга и анализа сообщений в электронных журналах учёта событий средств защиты информации проводится периодическая проверка работоспособности серверного и телекоммуникационного оборудования, каналов связи, средств обработки и защиты информации (в т.ч. направлением текстовых сообщений и принятием «ответов», визуального контроля, контроля трафика, контроля «поведения» системы и иными методами).

В целях восстановления доступности информационных ресурсов после аппаратных или программных сбоев организовано периодическое резервное копирование информации на систему хранения данных.

Контроль за выполнением резервного копирования возложен на АБИ и системного администратора. Восстановление системы и информации осуществляется АБИ и системным администратором.

Реализация мер, направленных на поддержание непрерывности работы средств и систем обработки информации осуществляется в соответствии с Порядком резервирования и восстановления работоспособности ТС, ПО и СЗИ.

Защита технических средств

Помещения, в которых размещены средства и системы обработки информации (ТС), расположены в пределах КЗ. Доступ в помещения имеет ограниченный круг лиц. Реализуемые в организации меры по защите ТС направлены на исключение НСД:

- к стационарным ТС, обрабатывающим информацию;
- к средствам, обеспечивающим функционирование ОИ;
- в помещения, в которых постоянно расположены ТС.

Порядок доступа в помещения организации осуществляется в соответствии с Инструкцией по управлению доступом к техническим средствам, информационным ресурсам и помещениям.

Защита средств и систем связи и передачи данных

Для обеспечения безопасного межсетевого взаимодействия используются сертифицированные средства межсетевого экранирования (СМЭ). СМЭ выполняют фильтрацию входящего и исходящего трафика на различных уровнях стека протоколов, регистрацию и учёт событий системы, а также обеспечивает установление защищённых (шифрованных) соединений между узлами, принадлежащими разным организациям и (или) разным информационным системам.

Для обеспечения защиты информации при передаче по незащищённым каналам связи применяются сертифицированные СКЗИ.

Порядок и правила, определяющие действия пользователей при использовании ресурсов и сервисов сети Интернет, установлены в Инструкции по обеспечению безопасности при работе в сети Интернет.

Эксплуатация СКЗИ осуществляется в соответствии с Инструкцией по эксплуатации средств криптографической защиты информации.

Управление конфигурацией систем обработки и защиты информации

Управление конфигурацией ОИ, а также СЗИ, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений обеспечивается АРМ и системным администратором.

7. Информирование по вопросам обеспечения безопасности информации

Ознакомление работников организации с правилами работы с информацией осуществляется:

- путем проведения руководителями структурных подразделений организации первичных инструктажей с вновь принятыми работником по соблюдению установленных правил обработки и защиты информации;
- путем проведения обучения работников (пользователей средств вычислительной техники) администратором безопасности правилам работы с используемыми средствами защиты информации;
- путем самостоятельного изучения работником документов, регламентирующих вопросы ОБИ в организации.

Допуск работников к информационным ресурсам организации осуществляется только после прохождения первичного инструктажа и ознакомления с документами организации по вопросам обеспечения ИБ.

При проведении первичного инструктажа нового пользователя должны быть разъяснены:

- права и обязанности пользователя при работе с информационными ресурсами организации;
- действия, которые запрещены в отношении информации, составляющей информационные ресурсы организации
- порядок и условия работы с информацией ограниченного доступа;
- возможные последствия и ответственность в случае нарушения правил работы с информационными ресурсами организации (информацией ограниченного доступа).

8. Контроль принятых мер по обеспечению безопасности информации

Организация контроля выполнения мероприятий информационной безопасности возлагается на ответственного за ОБИ в организации.

Руководители структурных подразделений организации осуществляют повседневный контроль выполнения требований по ОБИ в своих подразделениях.

АБИ организации осуществляет текущий контроль выполнения требований по ОБИ в рамках выполнения своих обязанностей.

Мероприятия по контролю ОБИ в организации проводятся в соответствии с Планом внутренних проверок состояния защиты информации.

Контроль эффективности принятых мер защиты информации должен осуществляться в соответствии с Положением по организации контроля эффективности защиты информации.