ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 4D97FC523D7EB9EBE20748A81E6A7384
Владелец: Резникова Ольга Михайловна
Действителен: с 07.05.2024 до 31.07.2025

Муниципальное автономное общеобразовательное учреждение «Средняя школа №43» Петропавловск - Камчатского городского округа

Утверждаю»
Директор МАОУ «СШ № 43»
_____ О.М. Резникова

«____» _____ 2024г.

Положение о политике информационной безопасности МАОУ «СШ № 43»

1. Общие положения

1.1. Настоящая Политика информационной безопасности разработана в соответствии с положениями:

- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящая Политика информационной безопасности представляет собой совокупность положений, правил и требований, определяющих структуру, необходимый уровень и способы защиты информации, принимаемой, передаваемой, обрабатываемой и хранимой информационной системой МАОУ «СШ № 43» (далее - информационная система).

Информационная система - это система, построенная на базе компьютерной техники, предназначенная для хранения, поиска, обработки и передачи значительных объёмов информации, имеющая определённую практическую сферу применения.

1.3. Защите подлежит вся информация, принимаемая, передаваемая, обрабатываемая и хранимая информационной системой, в том числе содержащая:

- сведения, составляющие служебную и коммерческую тайну, доступ к которым ограничен МАОУ «СШ № 43», как собственником информации, в соответствии с положениями предоставленными Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- персональные данные, доступ к которым ограничен в соответствии с положениями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- открытые сведения, в части обеспечения доступности и целостности информации.

1.4. Основными целями Политики информационной безопасности МАОУ «СШ № 43»

являются:

- обеспечение управления и поддержки высшим руководством МАОУ «СШ № 43» информационной безопасности в соответствии с требованиями образовательной среды Российской Федерации, соответствующими законами и нормами;
- защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба;
- обеспечение целостности и конфиденциальности информации;
- обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности.

1.5. Основными задачами Политики информационной безопасности МАОУ «СШ № 43» являются:

- доступность обрабатываемой информации;
- защита информации от несанкционированного доступа к ней посторонних лиц, от утечки по техническим каналам, от специальных воздействий на информацию в целях её блокирования, уничтожения, искажения;
- контроль целостности и аутентичности (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи МАОУ «СШ № 43»;
- обеспечение конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи МАОУ «СШ № 43»;
- оценка рисков информационной безопасности.

2. Субъекты правоотношений, связанных с использованием информационной системы и обеспечением безопасности информации

2.1. К субъектам правоотношений, связанных с использованием информационной системы и обеспечением безопасности информации относятся:

- МАОУ «СШ № 43», как обладатель информации;
- работники МАОУ «СШ № 43», как пользователи информационной системой в соответствии с возложенными на них трудовыми обязанностями;
- иные пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в информационной системе.

2.2. Доступ к информационной системе имеют следующие работники:

ведущий инженер программист.

Уровень доступа к информационной системе определяется для каждого работника индивидуально с соблюдением следующих требований:

- каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;
- конфиденциальная и открытая информация МАОУ «СШ № 43» размещается на разных серверах;
- непосредственный руководитель работника имеет право на просмотр информации, используемой работником.

Работники МАОУ «СШ № 43», как пользователи информационной системой в соответствии с возложенными на них трудовыми обязанностями, обязаны соблюдать данные требования политики информационной безопасности.

Все работники должны быть ознакомлены персонально под роспись с организационно-распорядительными документами по защите информации, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению безопасности информации.

Каждый работник при приеме на работу подписывает обязательство о соблюдении требований работы с информационной системой.

Все работники, допущенные к работе с информационной системой несут персональную ответственность за нарушение правил использования, передачи, хранения информации, в том

числе конфиденциальной информации.

2.3. Доступ к информационной системе имеют следующие пользователи: ведущий инженер программист.

В процессе использования информационной системы пользователи обязаны соблюдать данные требования политики информационной безопасности.

Для пользователей разрабатываются инструкции о порядке использования информационной системы, включающие требования по обеспечению безопасности информации.

До предоставления доступа к информационной системе пользователи должны быть ознакомлены с перечнем конфиденциальной информации и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки такой информации.

Пользователи, допущенные к работе с информационной системой, несут ответственность за нарушение правил использования, передачи, хранения информации, в том числе конфиденциальной информации.

3. Требования к организации защиты информации, содержащейся в информационной системе

3.1. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

3.2. Для обеспечения защиты информации, содержащейся в информационной системе, МАОУ «СШ № 43» назначается должностное лицо, ответственные за защиту информации: ведущий инженер программист.

3.3. Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы МАОУ «СШ № 43»] в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

3.4. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

3.5. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

- неправомерного блокирования информации (обеспечение доступности информации).

3.6. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;

- разработка системы защиты информации информационной системы;

- внедрение системы защиты информации информационной системы;

- аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

3.7. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется МАОУ «СШ № 43» с учётом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

- принятие решения о необходимости защиты информации, содержащейся в информационной системе;

- классификацию информационной системы по требованиям защиты информации (далее - классификация информационной системы);

- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

- определение требований к системе защиты информации информационной системы.

3.8. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

- анализ целей создания информационной системы и задач, решаемых этой информационной системой;

- определение информации, подлежащей обработке в информационной системе;

- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

- принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, МАОУ «СШ № 43» и уполномоченных лиц.

3.9. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс - третий, самый высокий - первый. Класс защищенности информационной системы определяется в соответствии с приложением № 1 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17.

Класс защищённости определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу

защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (далее - ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются актом классификации.

Класс защищенности информационной системы, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, не должен быть выше класса защищенности информационно-телекоммуникационной инфраструктуры центра обработки данных.

3.10. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, (далее - банк данных угроз безопасности информации ФСТЭК России), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

При определении угроз безопасности информации в информационной системе, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, должны учитываться угрозы безопасности информации, актуальные для информационно-телекоммуникационной инфраструктуры центра обработки данных.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом

Президента Российской Федерации от 16 августа 2004 г. № 1085.

3.11. Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

- цель и задачи обеспечения защиты информации в информационной системе;
- класс защищённости информационной системы;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;
- перечень объектов защиты информационной системы;
- требования к мерам и средствам защиты информации, применяемым в информационной системе;
- стадии (этапы работ) создания системы защиты информационной системы;
- требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
- функции МАОУ «СШ № 43» по обеспечению защиты информации в информационной системе;
- требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);
- требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

3.12. При определении требований к системе защиты информации информационной системы учитываются положения настоящей Политики информационной безопасности.

4. Требования к мерам защиты информации, содержащейся в информационной системе

4.1. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении № 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных

информационных системах, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17.

4.2. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать 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).

4.3. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

4.4. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

4.5. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

4.6. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

4.7. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.8. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

4.9. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

4.10. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

4.11. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

4.12. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам),

системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

4.13. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

4.14. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

4.15. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

- определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации, приведенными в приложении N 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17;

- адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

- уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, приведенных в приложении N 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

- дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Для выбора мер защиты информации для соответствующего класса защищенности информационной системы применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

4.16. В информационной системе соответствующего класса защищенности в рамках ее системы защиты информации должны быть реализованы меры защиты информации, выбранные в соответствии с пунктом 9.15 настоящей Политики информационной безопасности и обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации.

При этом в информационной системе должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

4.17. В случае если меры защиты информации, реализованные в информационно-телекоммуникационной инфраструктуре центра обработки данных, обеспечивают блокирование угроз безопасности информации, актуальных для функционирующей на его базе информационной системы, принятие дополнительных мер защиты информации в данной информационной системе не требуется. При этом полномочия в части защиты информации должны быть распределены между оператором информационной системы и оператором информационно-телекоммуникационной инфраструктуры центра обработки данных.

4.18. При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

4.19. Меры защиты информации выбираются и реализуются в информационной системе в рамках ее системы защиты информации с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации и облачных вычислений.

4.20. Потенциал нарушителей определяется в ходе оценки их возможностей, проводимой при определении угроз безопасности информации в соответствии с пунктом 3.11 настоящей Политики информационной безопасности.

МАОУ «СШ № 43»может быть принято решение о применении в информационной системе соответствующего класса защищенности мер защиты информации, обеспечивающих защиту от угроз безопасности информации, реализуемых нарушителями с более высоким потенциалом.

4.21. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При этом:

в информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

В информационных системах 1 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В информационных системах 2 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В информационных системах 3 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

Классы защиты и уровни доверия определяются в соответствии с нормативными правовыми актами ФСТЭК России, изданными в соответствии с подпунктом 13.1. пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В информационных системах применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических

условиях (заданиях по безопасности). При этом функции безопасности таких средств должны обеспечивать выполнение настоящих Требований.

4.22. При проектировании вновь создаваемых или модернизируемых информационных систем, имеющих доступ к информационно-телекоммуникационной сети "Интернет", должны выбираться маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности).

5. Требования к программно-техническим средствам информационной системы

Программно-технические средства информационной системы должны:

- располагаться на территории Российской Федерации;
- соответствовать требованиям, предусмотренным постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;
- быть сертифицированными Федеральной службой безопасности Российской Федерации и (или) Федеральной службой по техническому и экспортному контролю в отношении входящих в их состав средств защиты информации, включающих программно-аппаратные средства, средства антивирусной и криптографической защиты информации и средства защиты информации от несанкционированного доступа, уничтожения, модификации и блокирования доступа к ней, а также от иных неправомерных действий в отношении такой информации (в том числе сведения, составляющие врачебную тайну);
- обеспечивать хранение документации МАОУ «СШ № 43» в форме электронных документов, предусматривая резервное копирование документации в форме электронных документов и метаданных, восстановление документации в форме электронных документов и метаданных из резервных копий;
- обеспечивать протоколирование и сохранение сведений о предоставлении доступа и о других операциях с документами и метаданными в автоматизированном режиме, а также автоматизированное ведение электронных журналов учета точного времени и фактов размещения, изменения и удаления информации, содержания вносимых изменений;
- функционировать в бесперебойном круглосуточном режиме, за исключением установленных периодов проведения работ по обслуживанию информационных систем и устранению неисправностей в работе, суммарная длительность которых не должна превышать 4 часов в месяц (за исключением перерывов, связанных с обстоятельствами непреодолимой силы);
- обеспечивать информационное взаимодействие информационных систем между собой путем обмена информационными сообщениями посредством формирования, отправки, получения, обработки запросов и ответов, форматы которых разрабатываются операторами информационных систем.

6. Обеспечение информационной безопасности персональных данных

6.1. Защита, хранение, обработка и передача персональных данных работников и пользователей информационной системой регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлением Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

6.2. Персональные данные работника - информация, необходимая МАОУ «СШ № 43»в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные пользователей информационной системой - информация, необходимая МАОУ «СШ № 43» в связи с кадровой документацией.

6.3. К персональным данным работника относятся:

- фамилия, имя, отчество;
- пол;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- сведения об образовании, в том числе данные об организациях, осуществляющих образовательную деятельность по реализации профессиональных образовательных программ, о документах об образовании и (или) о квалификации, о договоре о целевом обучении, а также данные о сертификате специалиста или о прохождении аккредитации специалиста;
- занимаемая должность в МАОУ «СШ № 43»;
- иные сведения, необходимые МАОУ «СШ № 43»в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

6.4. Все персональные сведения о работниках и пользователях МАОУ «СШ № 43» может получить только от них самих. В случаях когда МАОУ «СШ № 43» получает необходимые персональные данные работников и пользователей только у третьего лица, МАОУ «СШ № 43»уведомляет об этом работников и пользователей и получает от них письменное согласие.

6.5. МАОУ «СШ № 43» сообщает работникам и пользователям о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работников и пользователей дать письменное согласие на их получение.

6.6. Персональные данные работников и пользователей являются конфиденциальной информацией и не могут быть использованы МАОУ «СШ № 43»или любым иным лицом в личных целях.

6.7. При определении объема и содержания персональных данных работников и пользователей МАОУ «СШ № 43»руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

6.8. Работники и пользователи не должны отказываться от своих прав на сохранение и защиту тайны.

6.9. МАОУ «СШ № 43» обрабатывает в информационных системах с использованием средств автоматизации следующие категории персональных данных работника, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных.

6.10. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

7. Заключительные положения

7.1. Политика информационной безопасности утверждается руководителем МАОУ «СШ № 43» и доводится до сведения всех работников МАОУ «СШ № 43»и соответствующих сторонних организаций.

7.2. Основные положения и требования настоящей Политики информационной безопасности распространяются на все структурные МАОУ «СШ № 43».

7.3. Настоящая Политика информационной безопасности вступает в силу с момента ее утверждения.

С Политикой информационной безопасности ознакомлены:

N п/п	Ф. И. О. работника	Дата	Подпись
1	2	3	4

.