УТВЕРЖДАЮ
Директор МАОУ «СОШ №135»
Знаемова Е.А.

_____

«__09__» ___января___ 20_20_ г.

ПОЛИТИКА
информационной безопасности
Муниципального автономного общеобразовательного учреждения
«Средняя общеобразовательная школа №135» города Барнаула

ВЫПОЛНИЛ
техник-программист

_____ В.А. Трофимов

«__09__» ___января___ 20_20_ г.

Барнаул, 2020

1. Вводные положения

1.1. Общие положения

Политика информационной безопасности (далее – Политика) Муниципального автономного общеобразовательного учреждения «Средняя общеобразовательная школа №135» города Барнаула (далее – Школа) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми Школа руководствуется в своей деятельности.

Настоящая Политика разработана в соответствии с федеральными законами от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Общее руководство за обеспечением информационной безопасности осуществляется директором Школы.

Ответственность за организацию мероприятий по обеспечению информационной безопасности и контроль за соблюдением требований информационной безопасности несет администратор информационной безопасности. Ответственность за функционирование информационных систем Школы несет администратор информационных систем.

Должностные обязанности администратора информационной безопасности и системного администратора закрепляются в соответствующих инструкциях.

Настоящая Политика распространяется на всех сотрудников и должностных лиц Школы и обязательна для исполнения.

Сотрудники Школы обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов Школы по вопросам обеспечения информационной безопасности.

Положения Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.2. Цели и задачи обеспечения информационной безопасности.

Основными целями Политики являются защита информации Школы от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Уставе Школы.

Политика направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации, и обеспечение нормального функционирования технологических процессов.

Задачами настоящей Политики являются:

- описание организации системы управления информационной безопасностью;
- определение порядка сопровождения информационных систем Школы;
- определение политики реализации антивирусной защиты, учетных записей, предоставления доступа к информационным ресурсам, использования паролей, защиты автоматизированных рабочих мест.

1.3. Период действия и порядок внесения изменений:

Политика признается утратившей силу на основании приказа директора Школы.

Изменения в Политику вносятся приказом директора Школы.

Инициаторами внесения изменений в политику информационной безопасности являются:

- директор Школы;
- руководители структурных подразделений Школы;
- администратор информационной безопасности.

Плановая актуализация настоящей Политики производится ежегодно и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация Политики информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Школы;
- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб Школе;
- при изменении политики Российской Федерации в области информационной безопасности, указов и законов Российской Федерации в области защиты информации.

Ответственным за актуализацию Политики информационной безопасности (плановую и внеплановую) является администратор информационной безопасности.

Контроль за исполнением требований настоящей Политики и поддержанием ее в актуальном состоянии возлагается на администратора информационной безопасности.

2. Основные положения

2.1. Назначение Политики

Политика – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Школе.

Политика относятся к административным мерам обеспечения информационной безопасности и определяет стратегию Школы в области информационной безопасности.

Политика регламентирует эффективную работу средств защиты информации, охватывает все особенности процесса обработки информации, определяя поведение информационных систем и их пользователей в различных ситуациях.

Политика реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политику, утверждаются директором Школы.

2.2. Основные принципы обеспечения информационной безопасности.

Основными принципами обеспечения информационной безопасности являются:

1) Законность (осуществление защитных мероприятий и разработки системы информационной безопасности органов власти и учреждений в соответствии с законодательством в области защиты информации);

2) Системность (учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности);

3) Комплексность (согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов);

4) Непрерывность (постоянная работа и организационная поддержка мер и средств защиты для эффективного обеспечения информационной безопасности);

5) Своевременность (постановка задач по комплексной защите информации и реализация мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности);

6) Преемственность и непрерывность совершенствования (совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и систем их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите);

7) Разумная достаточность (выбор достаточного уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми);

8) Персональная ответственность (ответственность за обеспечение информационной безопасности для каждого работника органа власти и учреждения в пределах его полномочий);

9) Минимизация полномочий (предоставление пользователям минимальных прав в соответствии с должностными регламентами, должностными инструкциями работников органов власти и учреждений);

10) Исключение конфликта интересов (четкое разделение обязанностей работников органов власти и учреждений и исключение ситуаций, когда сфера ответственности допускает конфликт интересов);
11) Взаимодействие и сотрудничество (работники органов власти и учреждений должны осознано соблюдать установленные правила и оказывать содействие деятельности подразделений (ответственных лиц) за обеспечение информационной безопасности);
12) Гибкость системы защиты (способность реагировать на изменения внешней среды и условий осуществления органами власти и учреждениями своих функций);
13) Простота применения средств защиты (не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при работе пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций);
14) Обоснованность и техническая реализуемость (реализация на современном уровне развития науки и техники, обоснованность с точки зрения достижения заданного уровня безопасности информации, а также соответствие установленным нормам и требованиям по безопасности информации);
15) Специализация и профессионализм (реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными работниками);
16) Обязательность контроля (обязанность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств).

2.3. Ответственность за реализацию Политики информационной безопасности.

Ответственность за реализацию политики возлагается:
- в части разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты, доведения правил Политики до сотрудников Школы – на администратора информационной безопасности;
- в части исполнения правил политики – на каждого сотрудника Школы, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей Политики.

2.4. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе.

Организация обучения сотрудников Школы в области информационной безопасности возлагается на администратора информационной безопасности.

Обучение проводится согласно плану, утвержденному директором Школы.

Подписи сотрудников об ознакомлении с Политикой заносятся в «Журнал проведения инструктажа по информационной безопасности».

Допуск персонала к работе с защищаемыми информационными ресурсами Школы осуществляется только после его ознакомления с настоящей Политикой, а также иными инструкциями пользователей отдельных информационных систем.

Согласие на соблюдение правил и требований настоящей Политики подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с конфиденциальной информацией Школы осуществляется только после ознакомления с «Порядком организации работы с материальными носителями защищаемых информационных ресурсов» и «Порядком организации работы с электронными носителями конфиденциальной информации».

Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками Школы, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

2.5. Защищаемые информационные ресурсы Школы.

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых информационных ресурсов».

3. Политики информационной безопасности.

3.1. Политика предоставления доступа к информационному ресурсу.

3.1.1. Назначение.

Настоящая политика определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам Школы.

3.1.2. Положение политики.

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим приказом директора Школы.

3.2. Политика учетных записей.

3.2.1. Назначение.

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов Школы.

3.2.2. Положение политики.

Регистрационные учетные записи подразделяются на:

- пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Школы;
- системные – используемые для нужд операционной системы;
- служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Школы назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую

пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

3.3. Политика использования паролей.

3.3.1. Назначение.

Настоящая Политика определяет основные правила парольной защиты в Школе.

3.3.2. Положения политики.

Положения политики закрепляются в «Порядке организации парольной защиты в информационных системах Школы».

3.4. Политика реализации антивирусной защиты.

3.4.1. Назначение.

Настоящая политика определяет основные правила для реализации антивирусной защиты в Школе.

3.4.2. Положения политики.

Положения политики закрепляются в «Порядке проведения антивирусного контроля».

3.5. Политика защиты автоматизированного рабочего места.

3.5.1. Назначение

Настоящая политика определяет основные правила и требования по защите информации Школы от неавторизованного доступа, утраты или модификации.

3.5.2. Положения политики.

Положения данной политики определяются в соответствии с используемым техническим решением.

4. Профилактика нарушений политик информационной безопасности.

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в Школе и проведение разъяснительной работы по информационной безопасности среди пользователей.

4.1. Ликвидация последствий нарушения политик информационной безопасности.

Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации, своевременно обнаруживает нарушения информационной безопасности, факты осуществления несанкционированного доступа к защищаемым информационным ресурсам и предпринимает меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления несанкционированного доступа к защищаемым информационным ресурсам, необходимо уведомить администратора информационной безопасности и администратора информационной системы, и далее следовать их указаниям.

Действия администратора информационной безопасности и администратора информационной системы при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- регламентом пользователя;
- политикой информационной безопасности;
- регламентом администратора информационной безопасности;
- регламентом системного администратора.

После устранения инцидента составляется акт о факте нарушения и принятых мерах по восстановлению работоспособности информационной системы, а также регистрируется факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

4.2. Ответственность за нарушение Политики.

Сотрудники Школы в рамках своих служебных обязанностей и полномочий несут ответственность за выполнение правил Политики.

На основании статьи 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования Политики, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Школе в результате нарушения ими правил Политики информационной безопасности (статья 238 Трудового кодекса Российской Федерации).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации компьютерной техники, следствием которых явилось нарушение работы компьютерной техники, уничтожение, блокирование или модификация защищаемой информации, сотрудники Школы несут

ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.