РАССМОТРЕНО И РЕКОМЕНДОВАННО К УТВЕРЖДЕНИЮ:
на заседании педагогическом совете
протокол № 6
от «11» ноября 2019г.

___г.

УТВЕРЖДАЮ:
Директор МАОУ «СОШ № 5»
_____В.Н. Новиков
Приказ № 457 «11» ноября 2019г.

Положение
по обеспечению информационной безопасности учреждения Муниципального образовательного учреждения «СОШ №5»

1. Общие положение.

1.1 Настоящее положение разработано в соответствии с Федеральным законом РФ "О персональных данных" от 27 июля 2006 г. № 152-ФЗ (ред. от 29.07.2017 № 223-ФЗ), Постановлением Правительства РФ от 07.10.2017 г. N 1235 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации, и формы паспорта безопасности этих объектов (территорий)", Постановлением Правительства Российской Федерации от 02.08.2019 №1006 «Об утверждении требований к антитеррористической защищенности объектов (территории) Министерства просвещения Российской Федерации и объектов (территории), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»., приказами Управления образования, МАОУ «СОШ № 5» и регламентирует порядок организации и осуществления контрольно-пропускного режима в учреждении.

1.2. Информационная безопасность является одним из составных элементов комплексной безопасности: под информационной безопасностью школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидации.

2. Физические меры защиты основаны на применении разного рода механических, электро или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

2.1 Мероприятия по физической защите объектов и средств информатизации учреждения

2.2 Обеспечение физической безопасности всей информационно-телекоммуникационной системы Учреждения и отдельных ее элементов.

2.3 Физическая защита направлена на обеспечение безопасности:

- периметра информационной системы (защита контролируемой зоны);
- периметра отдельных объектов системы (выделенных территорий, зданий, помещений);
- носителей информации, оборудования и каналов передачи данных, хранящих, обрабатывающих и передающих информацию в открытом виде (магнитных и бумажных носителей информации, экранов мониторов, серверов и рабочих станций, открытых каналов связи и т.п.);
- ключевых элементов криптографических и парольных систем;

2.4 Основными направлениями физической защиты Учреждения являются:

- контроль физического доступа к оборудованию, на контролируемую территорию и в помещения;
- обеспечение безопасности кабельной системы;
- обеспечение безопасности при утилизации отработавшего оборудования и носителей информации;
- обеспечение безопасности рабочих мест
- контроль физического доступа к оборудованию, на контролируемую территорию и в помещения

3. Для разграничения доступа в помещения, где располагается серверное оборудование и другие критически важные объекты ИТКС Учреждения, целесообразно использовать системы физической защиты. Необходимо соблюдать следующие правила доступа в помещения:

3.1. Во всех подразделениях Учреждения необходимо исключить несанкционированное нахождение посторонних лиц, дата и время их входа и выхода должны регистрироваться в журнал.

3.2. Необходимо немедленно изъять права доступа в защищенные области (территорию, помещения) у увольняющихся сотрудников. (пропуск, ключи)

4. Для предотвращения утечки информации и противодействия потенциальным нарушителям необходимо соблюдать следующие правила:

4.1 Эксплуатация автоматизированных рабочих мест (далее - АРМ) и серверов должна осуществляться в помещениях, оборудованных надежными замками, средствами сигнализации, исключающими возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающими физическую сохранность находящихся в помещении защищаемых ресурсов (АРМ, документов, реквизитов доступа и т.п.).

4.2 Размещение и установка АРМ и серверов должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней доступ.

4.3 В помещениях во время обработки и отображения на АРМ информации ограниченного распространения должен присутствовать только персонал, допущенный к работе с данной информацией.

Запрещается прием посетителей в помещениях, когда осуществляется обработка защищаемой информации.

4.4 Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами. Помещения должны быть обеспечены средствами уничтожения документов.

4.5 Вспомогательное оборудование (например, копировальные аппараты, факс-машины) должно быть размещено таким образом, чтобы уменьшить риск НСД (несанкционированного доступа) к защищенным областям или компрометации конфиденциальной информации.

4.6 Запрещается предоставлять конфиденциальную информацию посторонним лицам о происходящем в защищенных областях (территории, помещениях).

4.7 В нерабочее время защищенные области (территория, помещения) должны быть физически недоступны (закрыты на замки) и периодически проверяться сторожем (охрана).

4.8 Персоналу, осуществляющему техническое обслуживание серверов, должен быть предоставлен доступ в защищенные области (территорию, помещения) только в случае необходимости и после получения разрешения. По необходимости доступ такого персонала (особенно к конфиденциальным данным) следует ограничить, а их действия следует отслеживать.

4.9 Запрещается использование фотографической, звукозаписывающей и видео аппаратуры в защищенных областях, за исключением санкционированных случаев. (с разрешение Управления образования, директора школы)

4.10 По окончании рабочего дня помещения с установленными защищенными АРМ (автоматизированного рабочего место) должен сдаваться ключ охраннику (сторожу).

5. Обеспечение безопасности кабельной системы ИТКС учреждения.

5.1. Защита кабельной системы ИТКС направлена на снижение вероятности несанкционированного доступа к информации путем гальванического подключения к информационным кабелям или снятия информации через побочные электромагнитные излучения и наводки на другие кабели, а также на обеспечение защиты кабельного оборудования от электромагнитных помех.

- кабели электропитания и сетевые кабели для передачи данных необходимо защищать от вскрытия для целей перехвата информации и повреждения. Для уменьшения такого риска в помещениях организации предлагается реализовать следующие защитные меры:

- кабели электропитания и линии связи, идущие к информационным системам, должны быть проведены под землей (по возможности) или защищены надлежащим образом с помощью других средств.

- необходимо принять меры по защите сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, например, воспользовавшись экранами или проложив эти линии так, чтобы они не проходили через общедоступные места.

- с целью снижения влияния электромагнитных помех, силовые и коммуникационные кабели должны быть разнесены в пространстве.

6. Для исключительно уязвимых или критически важных систем следует принять дополнительные меры, таких, как:

- шифрование данных;
- установка бронированных экранов и использование запираемых помещений;
- использование других маршрутов или сред передачи данных.

7. Оборудование, подлежащее выводу из эксплуатации, и использованные носители информации могут содержать остаточную информацию ограниченного доступа. Регламентация порядка и процедур их утилизации позволяет перекрыть каналы несанкционированного доступа к этой информации:

- устройства хранения информации, содержащие ценную информацию, при выведении из эксплуатации должны быть физически уничтожены, либо должно быть проведено гарантированное стирание с них остаточной информации;
- все оборудование, включая носители информации, перед передачей другому владельцу или списанием должно быть проверено на отсутствие важной информации или лицензионного программного обеспечения;
- дальнейшая судьба поврежденных устройств хранения, содержащих важную информацию, (уничтожение или ремонт) определяется на основе заключения экспертной комиссии.

8. Безопасность рабочих мест сотрудников Учреждения предусматривает:

Рабочие места сотрудников Учреждения - наиболее многочисленная категория объектов ИТКС, через которые возможен несанкционированный доступ к информации.

- документы на всех видах носителей и технические средства обработки информации, должны храниться (размещаться) в помещениях, исключающих несанкционированный доступ к ним;
- персональные компьютеры, терминалы и принтеры должны защищаться блокираторами клавиатуры, паролями или другими методами на время отсутствия пользователя;
- должны быть приняты надежные меры, исключающие несанкционированное использование копировальной техники;

- распечатки, содержащие информацию ограниченного доступа должны изыматься из печатающего устройства немедленно, необходимо устанавливать печатающие устройства для печати конфиденциальных документов в помещениях, где работают сотрудники, ответственные за их учет, хранение и выдачу исполнителям.

9. Информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера:

9.1 информацию, защита которой предусмотрена законодательными актами РФ. в т. ч. персональные данные:

9.2 средства и системы информатизации. программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

10. Система информационной безопасности (далее - СИБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата):

- целостность (точность и полноту информации и компьютерных программ);

- доступность (возможность получения пользователями информации в пределах их компетенции).

10.1 Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе:

- организационная зашита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба:

- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

10.2 Правовые нормы обеспечения информационной безопасности

- школа имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

- школа обязана обеспечить сохранность конфиденциальной информации.

Администрация школы: назначает ответственного за обеспечение информационной безопасности; издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

- имеет право включать требования по защите информации в договоры по всем видам деятельности;

- разрабатывает перечень сведений конфиденциального характера; имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

10.3 Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора школы о назначении ответственного за обеспечение информационной безопасности;

- должностные обязанности ответственного за обеспечение информационной безопасности; перечень защищаемых информационных ресурсов и баз данных;

- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников школы и др.

10.4 Порядок допуска сотрудников школы к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера; · контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

11. Мероприятия по обеспечению информационной безопасности для обеспечения информационной безопасности в школе требуется проведение следующих первоочередных мероприятий:

· инструктаж работника специалистом по информационной безопасности;

· защита интеллектуальной собственности школы;

· защита компьютеров, локальных сетей и сети подключения к системе Интернета;

· организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся школы;

· учет всех носителей конфиденциальной информации.

12. Организация работы с информационными ресурсами и технологиями

12.1 Система организации делопроизводства:

- учет всей документации школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

- особый режим уничтожения документов.

12.2 В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

- все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

- документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

- выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.

- передача документов исполнителю производится только через ответственного за организацию делопроизводства.

- запрещается выносить документы с грифом "Для служебного пользования" за пределы школы.

- при смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

-для организации делопроизводства приказом директора школы назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы.

Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

13. Обеспечение безопасности на Школьном сайте учреждения

13.1 Школьный сайт относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам,

осуществляющим обработку персональных данных. 14.2 Школьный сайт обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения. Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой в Школьном сайте.

13.2 Участники образовательного процесса, имеющие доступ к Школьному сайту, не имеют права передавать персональные логины и пароли для входа на Школьный сайт другим лицам. Передача персонального логина и пароля для входа в Школьный сайт другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.

13.3 Участники образовательного процесса, имеющие доступ к Школьному сайту, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).

13.4 Участники образовательного процесса, имеющие доступ к Школьному сайт, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не более чем одного рабочего дня со дня получения информации о таком нарушении руководителя ОО, службу технической поддержки Школьного сайта.

13.5 При проведении работ по обеспечению безопасности информации на Школьном сайте участники образовательного процесса, имеющие доступ к Школьному сайту, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.