РАССМОТРЕНО И
РЕКОМЕНДОВАНО
к утверждению на заседании
педагогического совета
протокол № 7 от 29.03.2021

УТВЕРЖДАЮ
Директор МАОУ СОШ №8
_____ Т.В. Кузнецова
приказ № 102/1 от 29.03.2021

ПОЛОЖЕНИЕ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМНО – ТЕХНИЧЕСКОЙ ИНФРАСТРУКТУРЕ, ИНФОРМАЦИОННЫХ СИСТЕМАХ И РЕСУРСАХ

1. Общие положения

1. Положение по обеспечению информационной безопасности в системно – технической инфраструктуре, информационных системах и ресурсах Муниципального автономного общеобразовательного учреждения средняя общеобразовательная школа № 8 (далее – Положение) является локальным нормативным актом Муниципального автономного общеобразовательного учреждения средняя общеобразовательная школа № 8 (далее - Учреждение), устанавливающим требования к соблюдению информационной безопасности в целях сохранения информации Учреждения, а также сохранения в работоспособном состоянии системно – технической инфраструктуры, информационных систем и ресурсов Учреждения.

2. Положение разработано на основе следующих нормативных документов и локальных нормативных актов:

- Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействию терроризму»;
- Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»;
- Постановлением Правительства от 02.08.2019 г. № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»;
- Устава Учреждения.

3. Действия настоящего Положения распространяется на всех сотрудников Учреждения.

4. Настоящее Положение принимается педагогическим советом и утверждается приказом директора школы.

2. Требования по обеспечению информационной безопасности

1. Каждый сотрудник Учреждения в своей деятельности должен руководствоваться принципами неукоснительного соблюдения режима

информационной безопасности и предпринимать все необходимые действия для защиты информации от кражи, утери, несанкционированного изменения, а также обеспечивать сохранность оборудования и персональных данных, хранящихся в Учреждении, в соответствии с настоящими Требованиями и требованиями законодательства.

2. В отношении информационных систем сотрудникам запрещено осуществлять самовольно, без согласования с директором школы следующие действия:

2.1. изменять (сокращать, увеличивать) объем оперативной памяти, объем выделенных дисковых и процессорных ресурсов;

2.2. изменять схемы и технические параметры резервного копирования данных, операционных систем, программного обеспечения;

2.3. изменять версии системного и прикладного программного обеспечения серверов, включая обновления (установка сервис – паков), системой управления базой данных;

2.4. устанавливать информационные системы и любое программное обеспечение в нарушение утвержденных правил;

2.5. предоставлять самостоятельный доступ третьим лицам к информационным системам и к данным, содержащихся в них. Исключением является случаи обслуживания внешних организаций по договорам технического обслуживания;

2.6. перегружать и отключать серверы и информационные системы, находящихся на этапах эксплуатации;

2.7. вносить изменения в функционал информационных систем и модулей на сервере;

2.8. работать на серверах информационных систем под обезличенными учетными записями;

2.9. передавать третьим лицам информацию об аппаратно – программной инфраструктуре, структуре баз данных и содержимом баз данных информационных систем;

2.10. подключать новых пользователей к серверу, либо изменять права доступа пользователей на сервере;

2.11. изменять учетную информацию (логин, пароль) пользователей информационных систем;

2.12. предоставлять неограниченный доступ к серверам и персональным компьютерам из внешних сетей;

2.13. предоставлять конфиденциальную информацию коллегам вне возложенных на них функций, а также лицам, не являющимися сотрудниками Учреждения;

2.14. размещать информацию о пароле учетной записи в местах, позволяющих несанкционированно воспользоваться паролем без применения специальных технических знаний;

2.15. хранить пароли в незащищенном виде: в электронной почте, в файлах, на бумажных носителях в неохраняемых помещениях;

2.16. оставлять информационные системы включенными или в режиме «сон» в нерабочее время, выходные и праздничные дни;

2.17. использовать оборудование, подключенное к сети Учреждения, без установленных средств антивирусной защиты;

2.18. использовать личное ИТ-оборудование для обработки служебной информации и подключения к сети Учреждения, включая бытовую технику, не являющееся оборудованием, принадлежащим Учреждению;

2.19. использовать интернет в неслужебных целях (запрещено неслужебное использование торрент-ресурсов, скачивание фильмов, музыки, фотографий и любого другого медиа-контента);

2.20. предоставлять внешний доступ к ресурсам Учреждения, в том числе применять средства удаленного доступа (TeamViewer, AmmyAdmin и подобные средства удаленного доступа);

2.21. подключать третьих лиц к wi-fi сети Учреждения под своим аккаунтом, а также выдавать обезличенные учетные записи для доступа в интернет;

2.22. менять или удалять уникальные идентификаторы оборудования (инвентарные номера, шильды с заводскими номерами и/или артикулами).

3. Ответственность

1. Сотрудники Учреждения несут ответственность за несоблюдение настоящего Положения в соответствии с действующим законодательством.