ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ
АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА МАКЕЕВКА
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ШКОЛА № 58 ГОРОДА МАКЕЕВКИ»
286121, ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА, Г.О. МАКЕЕВКА, Г. МАКЕЕВКА,
УЛ. ЧИГИРИНСКАЯ, Д. 7
e-mail: makschool58@mail.ru Идентификационный код 9311014130
тел. +7 949 393-35-31

исх. от 01.09.2025 № 197
на № _____ от _____

УТВЕРЖДАЮ
Директор ГБОУ «Средняя школа № 58
городского округа Макеевка»
_____ /Ю.В.Кротова./
«01» _____ 20___ г.
Приказ № 197 от 01.09.2025г.

ПОЛОЖЕНИЕ

об информационной безопасности

ГБОУ «Средняя школа № 58 городского округа Макеевка»

1. Общие положения

1.1. Настоящее Положение регулирует отношения в сфере обеспечения информационной безопасности в Государственном бюджетном общеобразовательном учреждении «Средняя школа № 58 городского округа Макеевка» (далее – Учреждение).

1.2. Положение обязательно для исполнения всеми работниками Учреждения, обучающимися, их законными представителями, а также иными лицами, имеющими доступ к информационным ресурсам, сетям и средствам информатизации Учреждения.

1.3. Информационная безопасность Учреждения понимается как состояние защищённости информационных ресурсов, систем обработки данных, персональных сведений и информационно-телекоммуникационной инфраструктуры от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, распространения, а также от иных противоправных воздействий.

1.4. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации и вступает в силу с даты его утверждения директором Учреждения.

2. Нормативно-правовая база

Обеспечение информационной безопасности в Учреждении осуществляется на основании:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

- Постановлений Правительства РФ, приказов Минпросвещения России, методических рекомендаций Рособрнадзора и Роскомнадзора;

- Локальных нормативных актов Учреждения.

3. Цели и задачи

3.1. **Цель**: создание и поддержание безопасной информационной среды, обеспечивающей бесперебойное функционирование образовательного процесса, защиту персональных данных и предотвращение негативного информационного воздействия на обучающихся.

3.2. **Задачи**:

- Обеспечение конфиденциальности, целостности и доступности информационных ресурсов Учреждения;

- Организация контроля за использованием информационно-телекоммуникационной сети «Интернет»;

- Защита персональных данных работников, обучающихся и их законных представителей;

- Формирование у участников образовательных отношений навыков безопасного поведения в цифровой среде;

- Своевременное выявление, регистрация и устранение инцидентов информационной безопасности.

4. Организация системы информационной безопасности

4.1. Общее руководство системой информационной безопасности осуществляет директор Учреждения.

4.2. Непосредственную организацию и контроль за выполнением требований настоящего Положения возлагает на заместителя директора по учебно-воспитательной/информационно-технической работе.

4.3. Техническое обеспечение и администрирование средств защиты возлагается на системного администратора (или уполномоченного специалиста).

4.4. В Учреждении может создаваться Комиссия по информационной безопасности (по приказу директора), в состав которой входят представители администрации, педагогического коллектива, системный администратор, педагог-психолог, представитель родительского комитета.

4.5. Ответственность за соблюдение требований информационной безопасности в структурных подразделениях несут руководители подразделений (заведующие кабинетами, руководители кружков, классные руководители).

5. Основные мероприятия по обеспечению информационной безопасности

5.1. **Технические меры:**

- Установка и регулярное обновление лицензионного антивирусного программного обеспечения на всех рабочих станциях и серверах;

- Настройка средств фильтрации интернет-трафика для ограничения доступа к информации, запрещённой законодательством РФ и не соответствующей возрасту обучающихся;

- Разграничение прав доступа к информационным системам, учётным записям и базам данных;

- Регулярное резервное копирование критически важных данных;

- Использование защищённых каналов связи при передаче персональных данных.

5.2. **Организационные меры:**

- Ведение журнала учёта инцидентов информационной безопасности;

- Проведение вводного и периодического инструктажа работников по вопросам ИБ;

- Запрет на использование личных носителей информации и нелицензионного ПО в служебных целях без согласования с администрацией;

- Обеспечение физической сохранности серверного оборудования и коммутационных узлов.

5.3. **Воспитательно-просветительские меры:**

- Включение тем цифровой грамотности и безопасности в уроки информатики, классные часы, внеурочную деятельность;

- Проведение мероприятий для родителей по профилактике киберугроз;

- Размещение памяток и правил безопасного поведения в сети на официальном сайте и информационных стендах Учреждения.

6. Права и обязанности субъектов

6.1. **Работники Учреждения обязаны:**

- Соблюдать требования настоящего Положения и локальных актов;

- Не передавать учётные данные третьим лицам;

- Незамедлительно сообщать об обнаруженных уязвимостях, подозрительных файлах или инцидентах системному администратору или заместителю директора;

- Использовать информационные ресурсы исключительно в служебных и образовательных целях.

6.2. **Обучающиеся обязаны:**

- Использовать компьютерную технику и сеть Интернет только в учебных целях и под контролем педагога;

- Не посещать ресурсы, содержащие запрещённую, экстремистскую, порнографическую информацию или информацию, пропагандирующую насилие и вредные привычки;

- Уважать авторские права и не распространять персональные данные других лиц без согласия.

6.3. **Администрация Учреждения вправе:**

- Ограничивать или временно блокировать доступ к информационным ресурсам в случае нарушения правил ИБ;

- Проводить проверки соблюдения требований информационной безопасности;

- Вносить изменения в технические и организационные меры защиты в соответствии с изменениями законодательства и угроз.

7. Порядок реагирования на инциденты информационной безопасности

7.1. Инцидентом ИБ считается любое событие, повлёкшее или могущее повлечь нарушение конфиденциальности, целостности или доступности информации (утечка данных, заражение вредоносным ПО, несанкционированный доступ, публикация противоправного контента с IP-адресов Учреждения и т.п.).

7.2. При выявлении инцидента лицо, обнаружившее его, обязано:

- Немедленно прекратить работу с затронутым ресурсом;

- Сообщить системному администратору и заместителю директора;

- Сохранить доказательства (скриншоты, логи, вредоносные файлы) без самостоятельного удаления или модификации.

7.3. Системный администратор проводит локализацию инцидента, восстанавливает работоспособность систем, фиксирует событие в журнале и готовит акт.

7.4. При необходимости Учреждение информирует уполномоченные органы (Роскомнадзор, правоохранительные органы, Министерство образования ДНР/РФ) в порядке, установленном законодательством.

7.5. По результатам расследования разрабатываются мероприятия по недопущению повторения инцидента.

8. Контроль и ответственность

8.1. Контроль за исполнением настоящего Положения возлагается на заместителя директора и Комиссию по информационной безопасности.

8.2. Проверки соблюдения требований ИБ проводятся не реже одного раза в учебный год, а также при изменении нормативной базы или возникновении системных инцидентов.

8.3. За нарушение требований настоящего Положения работники несут дисциплинарную, материальную, административную или уголовную ответственность в соответствии с законодательством РФ. Обучающиеся и их законные представители несут ответственность в порядке, предусмотренном законодательством об образовании и защите прав несовершеннолетних.

9. Заключительные положения

9.1. Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует до принятия нового документа.

9.2. Изменения и дополнения вносятся приказом директора Учреждения по предложению заместителя директора, системного администратора или Комиссии по информационной безопасности.

9.3. Текст Положения размещается на официальном сайте Учреждения в разделе «Документы» и доводится до сведения работников и обучающихся под подпись.

9.4. Контроль за применением Положения осуществляет директор Учреждения.

Разработал:

Заместитель директора по УВР/ИТ

ГБОУ «Средняя школа № 58

городского округа Макеевка»

_____ /Ф.И.О./

«___» _____ 20____ г.

---

*Примечание для внутреннего использования.