Муниципальное бюджетное общеобразовательное учреждение
городского округа «Город Архангельск»
«Средняя школа № 37 имени Николая Степановича Мусинского»

ПРИКАЗ

31 августа 2026 г. № 330

**Об обеспечении информационной безопасности
и защите информационных ресурсов
от несанкционированного доступа**

В целях исполнения требований 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», обеспечения конфиденциальности, целостности и доступности информационных ресурсов школы, а также предотвращения случаев несанкционированного доступа (НСД) к информации,

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. «Положение об обеспечении информационной безопасности и защите от несанкционированного доступа к информационным ресурсам МБОУ СШ № 37 (Приложение № 1).

1.2. Правила использования информационно-коммуникационной сети Интернет и информационных ресурсов

2. Назначить ответственным за организационно-техническое обеспечение защиты информации, администрирование средств защиты информации и предотвращение несанкционированного доступа Архипову С.В., учителя.

3. Архипову С.В.:

3.1. В срок до 30.09.2026

провести аудит текущих средств защиты информации (антивирусная защита, настройки прав доступа в локальной сети, парольная политика).

3.2. Обеспечить разграничение прав доступа работников и обучающихся к информационным ресурсам образовательного учреждения в соответствии с их служебными обязанностями (принцип минимальных привилегий).

3.3. Обеспечить регулярное резервное копирование критически важных данных.

3.4. Вести журнал учета инцидентов информационной безопасности и немедленно информировать директора о фактах несанкционированного доступа или сбоях в работе средств защиты.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор С.В. Козяр

Приложение №1
к приказу от 31.08.2026 № 330

ПОЛОЖЕНИЕ
об обеспечении информационной безопасности и защите от несанкционированного доступа к информации в муниципальном бюджетном общеобразовательном учреждении городского округа «Город Архангельск» «Средняя школа № 37 имени Николая Степановича Мусинского»

1. Общие положения

1.1. Настоящее Положение (далее – Положение) определяет систему правовых, организационных и технических мер, направленных на обеспечение информационной безопасности (ИБ), защиту от несанкционированного доступа (НСД) к информационным ресурсам, а также защиту обучающихся от информации, причиняющей вред их здоровью и развитию, в муниципальном бюджетном общеобразовательном учреждении городского округа «Город Архангельск» «Средняя школа № 37 имени Николая Степановича Мусинского» (далее – МБОУ СШ № 37 , образовательное учреждение)

1.2. Положение разработано в соответствии с:

Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

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

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

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

Указом Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

Иными нормативными правовыми актами Российской Федерации и Уставом МБОУ СШ № 37.

2. Цели и задачи обеспечения информационной безопасности

2.1. Главной целью является создание защищенной информационной среды, обеспечивающей конфиденциальность, целостность и доступность информационных ресурсов МБОУ СШ № 37.

2.2. Основными задачами являются:

предотвращение несанкционированного доступа (НСД), утечки, хищения, искажения или уничтожения информации;

защита персональных данных обучающихся, их родителей (законных представителей) и работников образовательного учреждения;

защита обучающихся от доступа к информации, причиняющей вред их здоровью и (или) развитию, а также не совместимой с задачами образования;

обеспечение правовой и технической защиты интеллектуальной собственности образовательного учреждения;

формирование культуры информационной безопасности у работников и обучающихся.

3. Объекты информационной безопасности

К объектам защиты в МБОУ СШ № 37 относятся:

информационные ресурсы (базы данных, реестры, электронные журналы и дневники, документация на бумажных и электронных носителях);

персональные данные субъектов;

средства вычислительной техники (персональные компьютеры, серверы, ноутбуки, планшеты);

телекоммуникационное оборудование и каналы связи (локальная вычислительная сеть, сеть Интернет);

системное и прикладное программное обеспечение;

официальный сайт МБОУ СШ № 37 и страницы в социальных сетях.

4. Организационные меры защиты информации

4.1. Приказом директора МБОУ СШ № 37 назначается лицо, ответственное за обеспечение информационной безопасности (далее – Ответственный), в функции которого входит:

контроль за соблюдением режима ИБ и правил работы с персональными данными;

организация контентной фильтрации и антивирусной защиты;

проведение инструктажей работников по правилам ИБ;

мониторинг угроз и реагирование на инциденты.

4.2. Доступ работников к информационным ресурсам предоставляется на основе принципа «разграничения прав доступа» (минимально необходимые привилегии для выполнения должностных обязанностей).

4.3. Запрещается передача учетных записей (логинов и паролей) третьим лицам, включая коллег и обучающихся.

5. Технические меры защиты от несанкционированного доступа

5.1. В МБОУ СШ № 37 в обязательном порядке применяются следующие технические средства:

Антивирусная защита: на всех рабочих станциях и серверах установлено лицензионное антивирусное программное обеспечение (ПО) с автоматическим обновлением баз не реже одного раза в сутки.

Контентная фильтрация: используются программно-аппаратные средства для блокировки доступа к сайтам, содержащим запрещенную информацию (экстремизм, порнография, пропаганда наркотиков, азартные игры и т.д.), в соответствии с требованиями Минкомсвязи России.

Парольная защита: доступ к операционным системам, учетным записям и специализированному ПО защищен паролями. Пароли должны регулярно меняться (не реже 1 раза в 3 месяца) и соответствовать требованиям сложности.

Резервное копирование: критически важные данные (базы данных электронного журнала, финансовые документы) регулярно резервируются на защищенные внешние носители или в облачные хранилища, соответствующие требованиям 152-ФЗ.

5.2. Физическая защита: серверное и сетевое оборудование размещается в специально отведенном, запираемом помещении, доступ в которое имеют только уполномоченные лица.

5.3. Запрещается самовольная установка работниками или обучающимися любого программного обеспечения на компьютеры образовательного учреждения без согласования с Ответственным за ИБ.

6. Порядок использования сети Интернет

6.1. Доступ к сети Интернет предоставляется исключительно в образовательных и служебных целях.

6.2. Работникам и обучающимся запрещается:

посещать ресурсы с информацией, запрещенной законодательством РФ или не соответствующей возрасту обучающегося;

скачивать и запускать исполняемые файлы из ненадежных источников;

разглашать в сети Интернет конфиденциальную информацию об образовательном учреждении, работниках и обучающихся;

осуществлять действия, направленные на нарушение работоспособности сетевой инфраструктуры образовательного учреждения (хакерские атаки, спам и т.п.).

6.3. При обнаружении ресурса, содержащего запрещенную информацию или угрозу ИБ, пользователь обязан немедленно прекратить работу с данным ресурсом и сообщить об этом Ответственному за ИБ или администрации МБОУ СШ № 37.

6.4 Ответственное лицо проводит локализацию инцидента, расследование и составляет Акт об инциденте информационной безопасности.

7. Ответственность

7.1. Работники МБОУ СШ № 37, виновные в нарушении требований настоящего Положения, разглашении конфиденциальной информации или допуске несанкционированного доступа к информационным ресурсам, несут дисциплинарную, материальную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

7.2. Обучающиеся, нарушившие правила использования информационных ресурсов образовательного учреждения, привлекаются к дисциплинарной ответственности в соответствии с Уставом МБОУ СШ № 37, а их родители (законные представители) информируются о факте нарушения.

8. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента его утверждения приказом директора МБОУ СШ № 37

8.2. Изменения и дополнения в Положение вносятся приказом директора МБОУ СШ № 2в случае изменения действующего законодательства РФ или локальных потребностей организации.

8.3. Настоящее Положение размещается на официальном сайте МБОУ СШ № 37 в разделе «Документы» и на информационных стендах для ознакомления всех участников образовательного процесса.

Приложение №2
к приказу от 31.08.2026 № 330

Правила использования информационно-коммуникационной сети Интернет и информационных ресурсов

1. Правила работы с паролями

Управление доступом является основой информационной безопасности школы. К работе с паролями предъявляются следующие требования:

Персонализация: Учетные записи создаются персонально для каждого сотрудника. Использование общих (групповых) учетных записей не допускается

Сложность и актуальность: Пароли должны соответствовать требованиям сложности (сочетание заглавных и строчных букв, цифр и спецсимволов) и регулярно меняться в соответствии с установленным регламентом

Конфиденциальность: Категорически запрещается передача паролей третьим лицам, а также их хранение в открытом виде (на бумажных стикерах, в незащищенных текстовых файлах)

Многофакторная аутентификация: Для административных учетных записей и аккаунтов с доступом к базам персональных данных рекомендуется или обязывается использование двухфакторной аутентификации

2. Запреты на установку нелицензионного ПО

Образовательные организации обязаны строго соблюдать законодательство об интеллектуальной собственности:

Запрет на самостоятельную установку: Пользователям (как сотрудникам, так и обучающимся) категорически запрещается самостоятельно устанавливать любое программное обеспечение на школьные компьютеры без согласования с системным администратором или ответственным за информационную безопасность

Только легальное ПО: На компьютерах школы допускается использование только лицензионного программного обеспечения или свободного ПО (open-source), включенного в утвержденный администрацией перечень

Ответственность: Использование нелицензионного программного обеспечения влечет за собой серьезные риски, включая административные штрафы и уголовную ответственность для руководства образовательной организации

3. Правила использования электронной почты

Электронная почта является официальным каналом связи и требует строгого регламента:

Служебные адреса: Для административной и образовательной переписки должны использоваться только официальные адреса электронной почты школы

Запрет на использование личных ящиков: Запрещается использовать личные почтовые ящики и личные облачные аккаунты для хранения или пересылки служебных документов, особенно содержащих персональные данные обучающихся, родителей и сотрудников

Антивирусная проверка: Все передаваемые и получаемые файлы должны проверяться средствами антивирусной защиты. Запрещается открывать вложения от неизвестных отправителей без предварительной проверки

Запрещенные действия: Запрещается осуществлять массовые рассылки (спам), пересылать информацию конфиденциального характера, материалы, нарушающие авторские права, а также сообщения неэтичного или противоправного содержания

4. Правила использования съемных носителей

Съемные носители (USB-флешки, внешние жесткие диски, карты памяти) являются частым вектором распространения вредоносного ПО и утечки данных:

Служебная необходимость: Использование съемных носителей допускается только при наличии обоснованной служебной необходимости и в пределах полномочий пользователя

Запрет на личные носители: Запрещается использование личных (неучтенных) съемных носителей для обработки, хранения или переноса служебной информации и персональных данных

Обязательная проверка: Перед подключением к школьной сети любой съемный носитель должен быть обязательно проверен актуальными средствами антивирусной защиты

Технические ограничения: На всех рабочих станциях школы должна быть отключена функция автозапуска (autorun) с внешних носителей

Ограничение на копирование: Копирование персональных данных и информации ограниченного доступа на съемные носители допускается только при наличии документированного основания и в соответствии с установленным порядком передачи