

УТВЕРЖДЕНО
приказом директора
ГБОУ СО «Школа города Лесного»
от 30.08. 2024 г. № 284

Политика
информационной безопасности
государственного бюджетного общеобразовательного учреждения
Свердловской области «Школа города Лесного, реализующая
адаптированные основные общеобразовательные программы»

Определения и термины

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе, их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1. Общие положения

1.1. Политика информационной безопасности (далее – Политика ИБ) государственного бюджетного общеобразовательного учреждения Свердловской области «Школа города Лесного, реализующая адаптированные основные общеобразовательные программы» (далее – школа) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области ИБ, которыми руководствуются работники ГБОУ СО «Школа города Лесного» при осуществлении своей деятельности.

1.2. Основной целью Политики ИБ ГБОУ СО «Школа города Лесного» является защита информации при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

1.3. Политика ИБ разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №687 от 15 сентября 2008 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18 декабря 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 31 августа 2013 г. № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования», а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4. Выполнение требований Политики ИБ является обязательным для всех работников школы.

2. Цель и задачи политики информационной безопасности

2.1. Основными целями политики ИБ являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам школы;
- защита целостности информации с целью поддержания возможности школы по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами школы;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в управлении лицеем;
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
- предотвращение и/или снижение ущерба от инцидентов ИБ.

2.2. Основными задачами политики ИБ являются:

- разработка требований по обеспечению ИБ;
- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
- разработка нормативных документов для обеспечения ИБ школы;
- выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ школы;
- организация антивирусной защиты информационных ресурсов школы;
- защита информации школы от НСД и утечки по техническим каналам связи;
- организация периодической проверки соблюдения ИБ с последующим представлением отчета по результатам указанной проверки директору школы.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ ГБОУ СО «Школа города Лесного» направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников школы, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал школы. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3. Стратегия обеспечения ИБ ГБОУ СО «Школа города Лесного» заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников школы.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения ИБ являются:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов ГБОУ СО «Школа города Лесного»;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ школы, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками школы за обеспечение ИБ исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5. Объекты защиты

5.1. Объектами защиты с точки зрения ИБ в ГБОУ СО «Школа города Лесного» являются:

- информационный процесс профессиональной деятельности;
- информационные активы школы.

5.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности ГБОУ «Школа города Лесного»;

— персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

— другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности

6.1. В отношении всех собственных информационных активов ГБОУ СО «Школа города Лесного», активов, находящихся под контролем школы, а также активов, используемых для получения доступа к инфраструктуре школы, должна быть определена ответственность соответствующего сотрудника школы.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами школы должна доводиться до сведения директора ГБОУ СО «Школа города Лесного».

6.2. Все работы в пределах ГБОУ СО «Школа города Лесного» должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в управлении школы.

6.3. Внос в здание и помещения школы личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы ГБОУ СО «Школа города Лесного» производится только при согласовании с заместителем директора по АХЧ.

6.4. Данные (конфиденциальные или строго конфиденциальные), составляющие тайну школы и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.5. Заместитель директора по АХЧ должен периодически пересматривать права доступа сотрудников и других пользователей к соответствующим информационным ресурсам.

6.6. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

6.7. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.8. В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

6.9. Каждый сотрудник обязан немедленно уведомить заместителя директора по АХЧ обо всех случаях предоставления доступа третьим лицам к информационным ресурсам. Доступ третьих лиц к информационным системам школы должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам школы должен быть четко определен, контролируем и защищен.

6.10. Сотрудникам, использующим в работе портативные компьютеры ГБОУ СО «Школа города Лесного», может быть предоставлен удаленный доступ к сетевым ресурсам школы.

6.11. Сотрудникам, работающим за пределами школы с использованием компьютера, не принадлежащего управлению школы, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6.12. Сотрудники, имеющие право удаленного доступа к информационным ресурсам ГБОУ СО «Школа города Лесного», должны соблюдать требование, исключающее одновременное подключение их компьютера к сети школы и к каким-либо другим сетям, не принадлежащим школе.

6.13. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети школы, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

6.14. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

6.15. Рекомендованные правила:

— сотрудникам ГБОУ СО «Школа города Лесного» разрешается использовать сеть Интернет только в служебных целях;

— запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

— работа сотрудников ГБОУ СО «Школа города Лесного» с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации школы в сеть Интернет;

— сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем управлению школы;

— сотрудники ГБОУ СО «Школа города Лесного» перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

— запрещен доступ в Интернет через сеть ГБОУ СО «Школа города Лесного» для всех лиц, не являющихся сотрудниками школы, включая членов семьи сотрудников школы.

6.16. Заместитель директора по АХЧ имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.17. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация.

6.18. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит ответственное лицо по обслуживанию компьютерной техники из штатных работников по должности «электроник», назначенных приказом директора школы.

6.19. Компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются «компьютерное оборудование». Компьютерное оборудование является собственностью ГБОУ СО «Школа города Лесного» и предназначено для использования исключительно в производственных целях.

6.20. Каждый сотрудник, получивший в пользование компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.21. Компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться к ответственному лицу по обслуживанию компьютерной техники из штатных работников по должности «электроник». Данные не должны быть скомпрометированы в случае халатности или небрежности, приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.22. Программное обеспечение, установленное на предоставленном в пользование компьютерном оборудовании, является собственностью ГБОУ ОУ «Школа города Лесного» и должно использоваться исключительно в производственных целях.

6.23. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелегальное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности.

6.24. На всех компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений

6.25. Сотрудники школы не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.26. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию по электронной почте без использования систем шифрования. Строго конфиденциальная информация ни при каких обстоятельствах не подлежит пересылке третьим лицам по электронной почте.

6.27. Сотрудники ГБОУ СО «Школа города Лесного» для обмена документами должны использовать только свой официальный адрес электронной почты.

6.28. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

6.29. В целях предотвращения ошибок пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать заместителя директора по АХЧ. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.30. Не допускается при использовании электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.31. Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

6.32. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях ИБ, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.33. В случае кражи переносного компьютера следует незамедлительно сообщить заместителю директора по АХЧ.

6.34. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать заместителя директора по АХЧ и ответственного электроника по обслуживанию компьютерной техники;
- не пользоваться зараженным компьютером;
- не использовать компьютер до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование.

6.35. Сотрудникам ГБОУ ОУ «Школа города Лесного» запрещается:

- нарушать ИБ;
- сканировать порты или систему безопасности;
- контролировать работу сети (если имеется) с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя конечного устройства;
- передавать информацию о сотрудниках, обучающихся или списки сотрудников, обучающихся школы посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.36. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.37. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6.38. Сотрудники ГБОУ СО «Школа города Лесного» имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них и к которым они имеют санкционированный доступ.

6.39. Заявки на проведение технического обслуживания компьютеров должны направляться электронике по обслуживанию компьютерной техники по согласованию с заместителем директора по АХЧ.

6.40. Операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы.

7. Управление информационной безопасностью

7.1. Управление ИБ ГБОУ СО «Школа города Лесного» включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов ГБОУ СО «Школа города Лесного» по обеспечению ИБ;
- обеспечение бесперебойного функционирования комплекса средств ИБ;
- осуществление контроля (мониторинга) функционирования системы ИБ;
- оценку рисков, связанных с нарушениями ИБ.

8. Реализация политики информационной безопасности

8.1. Реализация Политики ИБ ГБОУ СО «Школа города Лесного» осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении школы.

9. Порядок внесения изменений и дополнений в Политику информационной безопасности

Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10. Контроль соблюдения политики информационной безопасности

10.1. Текущий контроль соблюдения выполнения требований Политики информационной безопасности ГБОУ СО «Школа города Лесного» возлагается на сотрудника, назначенного приказом директора школы.

10.2. Директор ГБОУ СО «Школа города Лесного» на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль соблюдения ее требований.

