ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 544
С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ АНГЛИЙСКОГО ЯЗЫКА
МОСКОВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

УЧТЕНО
мнение Совета родителей
протокол от 08.11.2022 № 2

ПРИНЯТО
решением Общего собрания работников ГБОУ школы № 544 с углубленным изучением английского языка Московского района Санкт-Петербурга протокол от 01.11.2022 № 2

УТВЕРЖДЕНО
приказом Директора ГБОУ школы № 544 с углубленным изучением английского языка Московского района Санкт-Петербурга
08.11.2022 № 175/1
_____ И.В. Васинович

DN: OU=Директор, O=ГБОУ школа 544 с углубленным изучением английского языка, CN=Васинович Ирина Викторовна, E=school544msk@obr.gov.spb.ru
Дата: 2022.11.08 15:08:16 +03'00'

ИНСТРУКЦИЯ
пользователя автоматизированной системы обработки конфиденциальной информации и персональных данных ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга

Санкт- Петербург
2022

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана для обеспечения защиты конфиденциальной информации, в том числе персональных данных, в автоматизированных системах, используемых в ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.2. Наиболее вероятными каналами утечки информации для автоматизированных систем (далее – АС) являются:

- несанкционированный доступ к информации, обрабатываемой в автоматизированной системе;
- хищение технических средств, с хранящейся в них информацией, или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

1.3. Работа с конфиденциальной информацией, персональными данными, а также со служебными документами ограниченного распространения (далее – информация ограниченного распространения), строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен
- отвечать и распоряжаться конкретный сотрудник, выдача документов осуществляется под роспись;
- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. ОБЯЗАННОСТИ РАБОТНИКОВ ГБОУ ШКОЛА №544 С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ АНГЛИЙСКОГО ЯЗЫКА МОСКОВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА, ИМЕЮЩИХ ДОСТУП К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2.1. Работники, получившие доступ к конфиденциальной информации, обязаны хранить в тайне данные сведения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки информации немедленно информировать руководителя структурного подразделения ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга, специалиста по защите информации.

Конфиденциальная информация не подлежит разглашению. Прекращение доступа к такой информации не освобождает сотрудника (работника) от взятых им обязательств по неразглашению сведений ограниченного распространения.

В случае оставления занимаемой должности сотрудник (работник) обязан вернуть все документы и материалы, относящиеся к деятельности ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга. В том числе отчеты, инструкции, переписку, списки сотрудников (работников), компьютерные

программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности администрации, полученные в течение срока работы.

2.2. Сотрудники (работники) при работе с конфиденциальной информацией обязаны:
- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;
- выполнять требования специалиста по защите информации, касающиеся обеспечения информационной безопасности;
- знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;
- хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты, установленной на АС;
- использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, карты памяти, компакт диски и т.д.);
- контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления в службу технической поддержки и специалисту по защите информации, ответственному за антивирусную защиту автоматизированной системы;
- немедленно ставить в известность директора ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга;
- в случае утери носителя с конфиденциальной информацией или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах;
- ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к защищенной АС;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АС.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя илинеустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, нскорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

2.3. Ставить в известность сотрудников (работников) ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга при:
- необходимости обновления антивирусных баз;
- обновлении программного обеспечения;
- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации АС;
- необходимости вскрытия системных блоков персональных компьютероввходящих в состав АС;
- резервном копировании информации.

2.4. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Вынос ПЭВМ, на которой проводилась обработка конфиденциальной информации, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с директором ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-

поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы.

ПЭВМ, используемые для работы с конфиденциальной информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации сотрудниками.

2.5. Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно конфиденциальную информацию;
- использовать конфиденциальную информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами, содержащими конфиденциальную информацию на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;
- накапливать ненужную для работы конфиденциальную информацию, при работе с персональными данными, соблюдать сроки ее хранения;
- передавать или принимать без расписки документы, содержащие конфиденциальную информацию и персональные данные;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие конфиденциальную информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами;
- использовать компоненты программного и аппаратного обеспечения АС подразделения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (картах памяти и т.п.);
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность специалистов ГБОУ школа №544 с углубленным изучением английского языка Московского района Санкт-Петербурга.

3. ОТВЕТСТВЕННОСТЬ

3.1. Сотрудник (работник) несет ответственность за соблюдение требований настоящей инструкции, а также других документов в области защиты информации.

3.2. За разглашение конфиденциальной информации, персональных данных, а также служебной тайны, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, сотрудники могут быть привлечены к дисциплинарной или иной, предусмотренной действующим законодательством ответственности.