



Государственное бюджетное общеобразовательное учреждение начальная общеобразовательная
ШКОЛА № 300
Центрального района Санкт-Петербурга,
191002, г. Санкт-Петербург, Большая Московская улица, д.10/1-3
Тел.: (812) 713-2582, факс: (812) 713-2582, e-mail: sch300.cent@obr.gov.spb.ru, сайт: <http://shkola300.spb.ru>

ПРИНЯТО

Общим собранием
работников
ГБОУ школы № 300
Центрального района
Санкт-Петербурга
Протокол № 1
от «28» августа 2019 г.

УТВЕРЖДАЮ

Директор школы
_____ Ю.Б. Ильина
30 августа 2019 г.

Введено в действие приказом № 114
от 30.08.2019 года

ПОЛОЖЕНИЕ
о разрешительной системе доступа сотрудников к защищаемым
информационным ресурсам

Санкт-Петербург
2019

Сфера действий настоящего Положения

Настоящее Положение устанавливает правила предоставления и разграничения доступа сотрудников к защищаемым информационным ресурсам ГБОУ школы № 300 Центрального района Санкт-Петербурга (далее – школа), не содержащим сведений, составляющих государственную тайну.

Положение предназначено лиц, ответственных за подключение сотрудников к информационным системам Комитета, других лиц, участвующих в процедурах предоставления и прекращения доступа сотрудников к информационным ресурсам.

Положение распространяется на информационные ресурсы, накапливаемые и обрабатываемые в электронном виде на персональных компьютерах сотрудников, в вычислительной сети исполнительных органов государственной власти Санкт-Петербурга, в базах данных информационных систем, а также на отчуждаемых (съемных) электронных носителях информации.

Положение не распространяется на информационные ресурсы на бумажных носителях, кино- и фотоматериалы.

Основные понятия, используемые в Положении

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные ресурсы - документы, массивы документов, накапливаемые и обрабатываемые в централизованных системах хранения данных школы.

Общедоступные информационные ресурсы - информационные ресурсы, содержащие информацию, доступ к которой не ограничен. Общедоступными информационными ресурсами могут пользоваться все сотрудники Комитета по их усмотрению.

Защищаемые информационные ресурсы - объекты файловых систем, содержащие информацию, нарушение целостности, доступности и (или) конфиденциальности которой может нанести ущерб.

Ответственный за информационный ресурс - лицо, которому предоставлено право разрешать или ограничивать доступ к информационному ресурсу.

Перечень защищаемых информационных ресурсов, с указанием лиц ответственных за них, утверждается руководителем. Перечень пересматривается при изменении состава ресурсов и условий их обработки, а также при инвентаризации информационных ресурсов.

Предоставление доступа сотрудникам к защищаемым информационным ресурсам, не содержащим персональных данных

Правом предоставления доступа к защищаемым информационным ресурсам, не содержащим персональных данных, обладает ответственный за

информационные ресурсы - начальник структурного подразделения, где создается и поддерживается в актуальном состоянии информационный ресурс.

Допуск сотрудника к защищаемым информационным ресурсам или изменение прав доступа осуществляется на основании служебной записки на имя руководителя с приложением заявки.

Ответственный проверяет обоснованность поступившей служебной записки, принимает решение о предоставлении доступа пользователя к информационному ресурсу и накладывает соответствующую резолюцию в служебной записке и заявке. В случае положительного решения, информационный ресурс будет предоставлен сотруднику в объеме указанном в заявке на подключение.

Ответственный оценивает техническую возможность предоставления доступа к запрашиваемому информационному ресурсу и в случае наличия технической возможности дает указание службе технической поддержки по настройке доступа к информационному ресурсу (при необходимости на создание учетной записи или на внесение изменений в существующую учетную запись).

Сотрудники службы технической поддержки выполняют работы по предоставлению доступа пользователя к защищаемому информационному ресурсу, инструктируют пользователя об особенностях работы с вновь установленными прикладными программами, а также (при необходимости) сообщают пользователю регистрационное имя и пароль способом, исключающим возможность ознакомления с этими данными посторонних лиц.

Предоставление доступа сотрудникам к защищаемым информационным ресурсам, содержащим персональные данные

Перечень информационных систем, в которых разрешено обрабатывать персональные данные, и список лиц ответственных за каждый информационный ресурс, содержащий персональные данные, утверждаются приказом директора.

Сотрудники, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного директором.

Состав персональных данных, права при обработке персональных данных (чтение, запись, удаление и т.д.), необходимые сотруднику для выполнения служебных обязанностей определяются ответственным.

В служебной записке обосновывается необходимость допуска сотрудника к персональным данным, состав персональных данных, необходимые права по обработке персональных данных, срок, на который предоставляется допуск сотрудника к обработке персональных данных.

Ответственный проверяет обоснованность поступившей служебной записки, накладывает соответствующую резолюцию и, в случае

положительного решения, информационный ресурс будет предоставлен сотруднику в объеме указанном в заявке на подключение.

Ответственный дает указания сотрудникам службы технической поддержки по настройке доступа сотрудника к обработке персональных данных с соответствующими правами (при необходимости на создание учетной записи или на внесение изменений в существующую учетную запись).

Порядок прекращения доступа сотрудника к защищаемым информационным ресурсам

Прекращение прав доступа сотрудника к защищаемым информационным ресурсам, содержащим персональные данные, а также не содержащим персональные данные, осуществляется на основании служебной записки.

При увольнении сотрудника прекращается действие прав, уволенного сотрудника, по доступу к информационным ресурсам и удаление учетных записей сотрудника.

В случае нарушения сотрудником требований, установленных правил безопасности персональных данных в школе, права доступа сотрудника к защищаемым информационным ресурсам временно приостанавливаются по решению директора. Восстановление или прекращение прав доступа сотрудника к защищаемым информационным ресурсам в этом случае осуществляется после проведения служебного расследования.

Порядок изменения прав доступа сотрудника к защищаемым информационным ресурсам

Порядок изменения прав доступа сотрудника к защищаемым информационным ресурсам в сторону их расширения аналогичен порядку их предоставления.

Порядок изменения прав доступа сотрудника к защищаемым информационным ресурсам в сторону их уменьшения аналогичен порядку их прекращения.

Ответственность

Начальник структурного подразделения несет ответственность за обоснованность запроса на предоставление доступа сотруднику к защищаемым информационным ресурсам и контроль выполнения сотрудником установленных требований безопасности информации.

Руководитель несет ответственность за принятие обоснованного решения по предоставлению прав доступа сотруднику к защищаемым информационным ресурсам.

Инженер-программист несет ответственность за правильность настроек программных и технических средств разграничения доступа к защищаемым информационным ресурсам в соответствии с правами, необходимыми сотрудникам для выполнения функциональных обязанностей.

Сотрудники, допущенные к защищаемым информационным ресурсам, несут ответственность за нарушение конфиденциальности информации, доступ к которой ограничен федеральным законом или обладателем информации, в соответствии с действующим законодательством.