		Приложение УТВЕРЖДЕН приказом МАОУ СОШ № 15 г. Тюмени от 05.07.2024 № 557

Порядок
действий работников
по информационной безопасности, обеспечивающий защиту от несанкционированного доступа к информационным ресурсам объектов (территорий) наименование учреждения

1. Общие положения

1.1. Настоящий Порядок определяет мероприятия и порядок действий работников по информационной безопасности, обеспечивающий защиту от несанкционированного доступа к информационным ресурсам объектов (территорий) МАОУ СОШ № 15 г. Тюмени (далее – Учреждение).

1.2. Настоящий Порядок разработан в соответствии с Постановлением Правительства РФ от 02.08.2019 № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)».

1.3. К информационным ресурсам Учреждения относятся сайт Учреждения в информационно-телекоммуникационной сети «Интернет», информационные системы и программы для электронных вычислительных машин, используемые в своей деятельности Учреждением.

1.4. Безопасность информационных ресурсов обеспечивается с помощью системы защиты данных, нейтрализующей актуальные угрозы.

2. Организация доступа к информационным ресурсам

2.1. Допуск для работы информационным ресурсам предоставляется работникам Учреждения, доступ которых необходим для выполнения ими служебных (трудовых) обязанностей согласно предоставленным им полномочиям в соответствии с трудовым договором, должностной инструкцией, локальными нормативными актами работодателя и действующим законодательством (далее – пользователь).

2.2. Пользователь информационного ресурса имеет право решать поставленные задачи только в соответствии с полномочиями доступа к ресурсу.

2.3. Пользователь несет ответственность за правильность подключения к

информационному ресурсу и за все действия при работе в информационном ресурсе.

2.4. Вход пользователя в информационный ресурс в зависимости от вида такого ресурса в целях обеспечения информационной безопасности может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

Обеспечение информационной безопасности использования иных информационных ресурсов, которые в силу своей конфигурации не имеют электронного идентификатора или персонального пароля, осуществляется путем установки таких информационных ресурсов только на автоматизированных рабочих местах работников (далее – АРМ), которым предоставлен соответствующий доступ к таким информационным ресурсам. Непосредственный доступ работника к АРМ обеспечивается по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Работа в информационном ресурсе допускается исключительно для выполнения своих служебных обязанностей.

Передача данных информационных ресурсов информации третьим лицам или использование их в личных целях запрещается.

2.6. При работе с информационным ресурсом пользователь каждый раз перед началом работы обязан проверить отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств. В случае обнаружения вирусов либо вредоносных программ пользователь информационной системы обязан немедленно прекратить их использование и действовать в соответствии с требованиями, установленными в Учреждении.

2.7. В случае утраты или уничтожения данных информационного ресурса либо разглашении содержащихся в нем сведений, об этом немедленно ставится в известность администратор информационной безопасности.

3. Обязанности пользователей информационных ресурсов

3.1. Сотрудник, осуществляющий исполнение своих служебных обязанностей в информационных ресурсах, обязан:

1) строго соблюдать установленные правила обеспечения безопасности информации в информационных ресурсах;

2) знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

3) хранить в тайне свой пароль (пароли);

4) хранить свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

5) выполнять установленный в Учреждении порядок организации антивирусной защиты;

6) немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (токена, смарт-карты, ключа авторизации) или при подозрении компрометации паролей, а также

при обнаружении:

нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих компонентах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к АРМ;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ информационного ресурса;

отклонений в нормальной работе информационных ресурсов;

некорректного функционирования установленных на АРМ технических средств защиты;

непредусмотренных отводов кабелей и подключенных устройств.

3.2. Пользователю категорически запрещается:

1) использовать информационные ресурсы в неслужебных целях;

2) самовольно вносить какие-либо изменения в конфигурацию информационных ресурсов;

3) осуществлять работу информационных ресурсов в присутствии посторонних (не допущенных к данной работе) лиц;

4) оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

5) умышленно использовать недокументированные свойства и ошибки в информационном ресурсе или в настройках ресурса, которые могут привести к возникновению кризисной ситуации;

6) предоставлять возможность доступа к информационному ресурсу так, чтобы существовала возможность визуального считывания информации.

3.3. Лица, виновные в нарушении требований настоящего Порядка и иных документов, регламентирующих вопросы защиты данных информационных ресурсов, несут ответственность в соответствии с действующим законодательством Российской Федерации

Лист ознакомления с приказом от _____ № _____:

ФИО	Должность	Дата	Подпись