УТВЕРЖДЕНО
директором Центра «Поиск»
О. А. Томилиной
приказ № 514
от «28» декабря 2024 г.

И Н С Т Р У К Ц И Я

по обеспечению защиты информации при взаимодействии пользователей Центра «Поиск» с информационными сетями общего пользования

1. Общие положения

1.1. Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ "О персональных данных".

1.2. Инструкция по обеспечению защиты информации, содержащейся в информационных ресурсах Государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск»), при взаимодействии пользователей с информационными сетями общего пользования (далее – Инструкция) определяет условия и порядок подключения рабочих станций Центра «Поиск» к информационным сетям общего пользования (далее – Сетям), а также мероприятия по обеспечению безопасности информации, содержащейся в информационных ресурсах Центра «Поиск», при подключении и взаимодействии пользователей с этими сетями.

1.3. Положения Инструкции определены исходя из следующих основных угроз безопасности информации, возникающих при взаимодействии с информационными сетями общего пользования:

– несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних локальных вычислительных сетях (серверах,

рабочих станциях) или на автономных рабочих станциях, как из Сетей, так и из внутренних локальных вычислительных сетей (далее – ЛВС);

- несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, серверу, Web/Proxy серверу), соединяющему внутренние ЛВС Центра «Поиск» с Сетями;
- несанкционированного доступа к данным, передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;
- заражения программного обеспечения компьютерными "вирусами" из Сети как посредством приема "зараженных" файлов, так и посредством E-mail;
- внедрения программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;
- несанкционированной передачи защищаемой информации из ЛВС в Сеть.

1.4. Непосредственную ответственность за надлежащее выполнение Инструкции всеми сотрудниками Центра «Поиск» несет директор Центра.

1.5. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Поиск» и не исключает обязательного выполнения их требований.

1.6. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Условия подключения абонентов к Сети

2.1. К Сети подключаются все рабочие станции Центра «Поиск».

2.2. Подключение к Сети рабочей станции, осуществляющей обработку информации с открытым доступом, может осуществляться без оборудования средствами защиты информации от НСД.

2.3. Подключение к Сети рабочих станций, на которых обрабатывается информация, не разрешенная к открытому опубликованию, осуществляется только после установки на них средств защиты информации от НСД.

3. Порядок подключения и взаимодействия пользователей с Сетью

3.1. Подключение рабочей станции к Сети должно осуществляться в установленном порядке через провайдера Сети.

3.2. Подключение локальной вычислительной сети Центра «Поиск» к Сети должно осуществляться через средства разграничения доступа в виде межсетевых экранов. Не допускается подключение ЛВС к Сети в обход межсетевых экранов (далее – МЭ).

3.3. Доступ к МЭ, к средствам его конфигурирования может осуществляться только администратором информационной безопасности.

3.4. На технических средствах рабочих станций должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения рабочей станции к Сети.

3.5. Установку программного обеспечения, обеспечивающего функционирование рабочей станции, могут выполнять только уполномоченные специалисты Центра «Поиск» или специалисты сторонних организаций под контролем администратора информационной безопасности.

3.6. Пользователи рабочих станций не имеют права производить самостоятельную установку и модификацию программного обеспечения, однако могут обращаться к администратору информационной безопасности для проведения его экспертизы на предмет улучшения характеристик, наличия "вирусов", замаскированных возможностей выполнения непредусмотренных действий.

3.7. Ответственность за установку на рабочей станции программ, не включенных в состав рекомендованного к использованию программного обеспечения, целиком ложится на пользователя.

3.8. При обнаружении фактов использования произвольных программ, не включенных в состав рекомендованного к использованию на рабочей станции программного обеспечения, администратор информационной безопасности обязан отключить рабочую станцию от Сети и ЛВС и поставить об этом в известность директора Центра «Поиск».

3.9. Средства защиты информации, устанавливаемые на автономные АРМ, рабочие станции и серверы внутренней ЛВС при обработке на них защищаемой информации, должны осуществлять идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю.

3.10. Модификация конфигурации программного обеспечения рабочей станции должна быть доступна только со стороны администратора информационной безопасности.

3.11. Средства регистрации и регистрируемые данные должны быть недоступны для пользователя.

3.12. Web-серверы, почтовые серверы должны размещаться в отдельном защищаемом помещении, доступ в которое имеет ограниченный круг лиц, определенный приказом директора Центра «Поиск».

3.13. При предоставлении пользователям прикладных сервисов следует исходить из принципа минимальной достаточности.

3.14. Эффективно использовать имеющиеся в маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа.

3.15. Абоненты Сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;
- знать правила работы со средствами защиты информации, установленными на рабочих станциях;
- уметь пользоваться средствами антивирусной защиты.

3.16. При работе в Сети пользователю категорически запрещается:

- изменять состав и конфигурацию программных и технических средств рабочей станции;

– производить отправку защищаемых данных без соответствующего разрешения.

3.17. Ведение учета пользователей, подключенных к Сети, осуществляется администратором информационной безопасности Центра «Поиск».

3.18. Администратор информационной безопасности обязан контролировать использование ресурсов Сети сотрудниками Центра «Поиск» и вносить предложения об изменении списка доступных ресурсов.

3.19. Доступ к ресурсам Сети может быть блокирован администратором информационной безопасности без предварительного уведомления, при возникновении нештатных ситуаций, либо в иных случаях, предусмотренных организационными документами.

3.20. Контроль за выполнением мероприятий по обеспечению безопасности информации на рабочих станциях возлагается на администратора информационной безопасности.

4. Работа с корпоративной электронной почтой

4.1. Корпоративная электронная почта является собственностью компании и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

4.2. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

4.3. Доступ к серверу электронной почты может быть блокирован администратором информационной безопасности без предварительного уведомления, при возникновении нештатных ситуаций, либо в иных случаях предусмотренных организационными документами.

4.4. При работе с корпоративной системой электронной почты запрещается:

– использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с администратором информационной безопасности;

– публиковать свой адрес, либо адреса других сотрудников компании в открытом доступе без предварительного согласования с администратором информационной безопасности;

– открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами;

– осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с администрацией Центра «Поиск»;

– рассылать материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, программы для осуществления несанкционированного доступа;

– рассылать серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Сети, а также ссылки на вышеуказанную информацию;

– распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

– распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством;

– распространять информацию ограниченного доступа;

– предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.