

**ГОСУДАРСТВЕННОЕ  
АВТОНОМНОЕ НЕТИПОВОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
«РЕГИОНАЛЬНЫЙ ЦЕНТР ВЫЯВЛЕНИЯ,  
ПОДДЕРЖКИ И РАЗВИТИЯ СПОСОБНОСТЕЙ И  
ТАЛАНТОВ У ДЕТЕЙ И МОЛОДЕЖИ»**

241035, г. Брянск, ул. Протасова, стр.1Б

тел.: +74832772302

e-mail: [smartkidscenter032@ya.ru](mailto:smartkidscenter032@ya.ru)

сайт: <https://talant32.ru/>

ИНН/КПП 3257070301/325701001



**УТВЕРЖДАЮ**

Директор ГАНОУ «РЦПД»

Е.В. Воробьев

2026 г.

**Инструкция № АТ-14-2026  
по информационной безопасности**

**Общие положения.**

1. Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных системах МАУ ДО «Детский технопарк «Кванториум»
2. Работники МАУ ДО «Детский технопарк «Кванториум».» обязаны:
3. Знать и соблюдать требования настоящей Инструкции и других документов по информационной безопасности при работе с ПК, имеющими доступ к информационным ресурсам локальной сети МАУ ДО «Детский технопарк «Кванториум» и сети «Интернет»;
4. Знать и уметь правильно использовать то аппаратно - программное обеспечение, которое установлено на его ПК, а также строго выполнять правила работы со средствами защиты информации, установленными на них;
5. Хранить в тайне свой пароль (пароли);
6. Выполнять следующие требования по антивирусному контролю:
  - Антивирусный контроль всех дисков и файлов ПК должен проводиться ежедневно в начале работы при их загрузке в автоматическом режиме;
  - Обновление антивирусных баз должно проводиться в соответствии с периодичностью, указанной в руководствах по применению конкретных антивирусных средств.
  - В процессе работы обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (flesh-дисках, CD-, DVD- и т.п.). Разархивирование и контроль входящей информации должен проводиться непосредственно после ее приема. Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный носитель);
  - Устанавливаемое (изменяемое) на ПК программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на ПК лицом, установившим (изменившим) программное обеспечение, в присутствии пользователя ПК должна быть выполнена антивирусная проверка;
  - При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках

и т.п.) работник ГАНОУ «РЦПД» должен провести внеочередной антивирусный контроль своего ПК;

7. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов инженера по защите информации, владельца зараженных файлов;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, немедленно приостановить работу и сообщить о данном факте ответственному по защите информации;
- по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

8. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним ПК.

9. Хранить значение своих паролей на бумажном или другом носителе информации.

#### **Работникам ГАНОУ «РЦПД» категорически запрещается:**

- использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами ПК;
- осуществлять обработку конфиденциальной информации (персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц;
- осуществлять обработку конфиденциальной информации (персональных данных) при подключенном ПК к сети Интернет;
- записывать и хранить конфиденциальную информацию (персональные данные) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются;
- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию;
- предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом;
- 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 немедленно ставить в известность ответственного по защите информации.

#### **Права работников, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет».**

Работники ГАНОУ «РЦПД» пользователи ПК имеют право:

- Давать ответственному по защите информации предложения по совершенствованию мер информационной безопасности в учреждении;
- Обращаться к инженеру по защите информации для оказания необходимой технической и методологической помощи в своей работе.

Ответственный по защите информации имеет право:

- Требовать от работников - пользователей ПК соблюдения установленных технологий обработки информации и выполнения инструкций и других документов по обеспечению безопасности и защите информации;
- Обращаться к руководителю с требованием прекращения работы сотрудников - пользователей ПК при несоблюдении ими установленных технологий обработки информации или невыполнении требований по обеспечению информационной безопасности;
- Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств.

**Ответственность.**

Работники учреждения, пользователи ПК, имеющие доступ к информационным ресурсам локальной сети ГАНОУ «РЦПД» и сети «Интернет», несут персональную ответственность за обеспечение информационной безопасности при их использовании, и соблюдение требований настоящей Инструкции.

Ответственный за антитеррористическую безопасность:

Заместитель директора



В.В. Алехин