Приложение № 5
к приказу от 21.05.2013 № 121
(в редакции от 01.10.2018 г.)

Порядок доступа работников и иных лиц
в помещения МАОУ Лицея № 6 «Перспектива», в которых размещена информационная система и коммуникационное оборудование, а также хранятся носители конфиденциальной информации

Настоящий порядок разработан в соответствии с Федеральными законами от 27.07.2006 г. № 152-ФЗ «О персональных данных», от 27.06.2007 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлениями Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», с учётом Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами (утв. постановлением Правительства РФ от 21.03.2012 № 211), Положения о порядке обращения с конфиденциальной информацией, её накопления и обработки в информационных системах администрации города Красноярска (утв. распоряжением администрации г. Красноярска от 01.02.2007 г. № 14-р).

1. В помещениях, в которых размещены информационные системы МАОУ Лицея № 6 «Перспектива» (далее – Оператор) и коммуникационное оборудование, а также хранятся носители конфиденциальной информации (далее – режимные помещения) допускаются: руководитель Оператора, лицо, назначенное ответственным за организацию работ по защите конфиденциальной информации (за обеспечение безопасности персональных данных) и лица, имеющие прямое отношение к обработке соответствующей конфиденциальной информации.

2. Лица, по роду своей деятельности не являющиеся персоналом, допущенным к работе в конкретных режимных помещениях, допускаются в указанные помещения с санкции руководителя оператора.

3. Режимные помещения не допускается оставлять без контроля. В рабочее время контроль каждого режимного помещения осуществляется лицами, обрабатывающими конфиденциальную информацию в режимном помещении. В нерабочее время контроль целостности режимных помещений осуществляется дежурным персоналом.

4. Двери режимных помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода сотрудников, посетителей. Ключи от входных дверей режимных помещений нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учёта хранилищ. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище.

5. По окончании рабочего дня каждое режимное помещение и установленные в нём хранилища должны быть закрыты и опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации.

6. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до замены замка или изменения секрета замка устанавливает руководитель Оператора или лицо, назначенное ответственным за организацию работ по защите конфиденциальной информации (за обеспечение безопасности персональных данных).

7. В обычных условиях режимные помещения, находящиеся в них хранилища могут быть вскрыты исполнителями, занимающимися обработкой конфиденциальной информации в режимном помещении, лицом, назначенным ответственным за организацию работ по защите конфиденциальной информации (за обеспечение безопасности персональных данных) или руководителем Оператора. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения и (или) хранилища посторонних лиц, о случившемся должно быть немедленно сообщено лицу, назначенному ответственным за организацию работ по защите конфиденциальной информации (за обеспечение безопасности персональных данных) или руководителю оператора. Лицо, назначенное ответственным за организацию работ по защите конфиденциальной информации (за обеспечение безопасности персональных данных), должно оценить возможность компрометации документов, содержащих сведения конфиденциального характера, составить акт и, при необходимости, - организовать принятие мер к локализации последствий компрометации персональных данных.

8. Техническое обслуживание средств автоматизированной обработки персональных данных осуществляется в отсутствие лиц, не имеющих доступа к обработке соответствующих персональных данных.

Директор МАОУ Лицея № 6 «Перспектива»
А.В. Лапков