Правительство Санкт-Петербурга Комитет по образованию
Администрация Красногвардейского района Санкт-Петербурга
Государственное бюджетное общеобразовательное учреждение средняя общеобразовательная школа № 490 с углубленным изучением иностранных языков Красногвардейского района Санкт-Петербурга

П Р И К А З

02 сентября 2024 года **№ 80-о**

«Об утверждении организационных документов по защите информации, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»

В соответствии со статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», подпунктами «б» и «д» пункта 1 постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении 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», подпунктом «б» пункта 13 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации
от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», пунктами 16.3 и 18.1 раздела 2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17,

ПРИКАЗЫВАЮ:

1. Утвердить следующие организационные документы по защите информации, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»:

1.1. Перечень сотрудников, допущенных к информации ограниченного доступа, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная

автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», согласно Приложению № 2 к настоящему приказу;

1.2. Инструкцию по порядку учета, хранения и уничтожения носителей информации ограниченного доступа, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», согласно Приложения № 1 к настоящему приказу;

1.3. Инструкцию о порядке резервирования и восстановления работоспособности технических (аппаратных) средств и программного обеспечения, баз данных и средств защиты информации в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» согласно Приложению № 3 к настоящему приказу;

1.4. Инструкцию по обеспечению защиты информации, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», согласно Приложению № 4 к настоящему приказу;

1.5. Регламент администрирования учетных записей пользователей государственной информационной системы Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» согласно Приложению № 5 к настоящему приказу;

1.6. Правила доступа к персональным данным, обрабатываемым в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», согласно Приложению № 6 к настоящему приказу;

1.7. Перечень лиц, имеющих право доступа к персональным данным, обрабатываемым в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», для выполнения ими служебных (трудовых) обязанностей, согласно Приложению № 2 к настоящему приказу.

2. Контроль за исполнением приказа оставляю за собой

Директор школы Н.Б. Александрова

Приложение № 1
к приказу от 02.09.2024 года № 80-о

ИНСТРУКЦИЯ
по порядку учета, хранения и уничтожения носителей информации ограниченного доступа, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»

1. Общие положения

Настоящая Инструкция устанавливает порядок использования носителей информации ограниченного доступа, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» (далее – КАИС КРО).

2. Порядок использования носителей информации ограниченного доступа

Под использованием носителей информации ограниченного доступа в Государственном бюджетном общеобразовательном учреждении средней общеобразовательной школе № 490 с углубленным изучением иностранного языка Красногвардейского района Санкт-Петербурга понимается их подключение к инфраструктуре КАИС КРО с целью обработки, приема или передачи информации.

В КАИС КРО допускается использование только учтенных машинных носителей информации ограниченного доступа, которые подвергаются регулярной ревизии и контролю. Учет машинных носителей информации ограниченного доступа, используемых в КАИС КРО, ведется в соответствующем журнале учета носителей информации ограниченного доступа, типовая форма которого приведена в приложении к настоящей Инструкции.

К носителям информации ограниченного доступа предъявляются те же требования по информационной безопасности, что и для стационарных автоматизированных рабочих мест (целесообразность дополнительных мер обеспечения информационной безопасности определяются администраторами безопасности КАИС КРО).

3. Порядок учета, хранения и обращения с носителями информации ограниченного доступа и их утилизации

Каждый носитель информации ограниченного доступа с записанной на нем информацией должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу носителей информации ограниченного доступа осуществляет администратор безопасности КАИС КРО. Факт выдачи носителя информации фиксируется в журнале учета носителей информации ограниченного доступа.

Сотрудники Учреждения могут получать машинный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ сотрудник сдает носитель информации ограниченного доступа для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

При использовании сотрудниками Учреждения носителей информации ограниченного доступа необходимо:

руководствоваться требованиями настоящей инструкции по порядку учета, хранения и уничтожения носителей информации ограниченного доступа, содержащейся в КАИС КРО;

использовать носители информации ограниченного доступа исключительно для выполнения своих служебных обязанностей;

ставить в известность администратора безопасности КАИС КРО о любых фактах нарушения требований настоящей инструкции по порядку учета, хранения и уничтожения носителей информации ограниченного доступа, содержащейся в КАИС КРО;

бережно относиться к носителям информации ограниченного доступа;

обеспечивать физическую безопасность носителей информации ограниченного доступа всеми разумными способами, в том числе хранением носителя в сейфе;

извещать администратора безопасности КАИС КРО о фактах утраты (кражи) носителей информации ограниченного доступа.

При использовании носителей информации ограниченного доступа запрещено:

использовать носители информации ограниченного доступа в личных целях;

передавать носители информации ограниченного доступа другим лицам (за исключением администратора безопасности КАИС КРО);

хранить носители информации ограниченного доступа вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

выносить носители информации ограниченного доступа из служебных помещений для работы с ними на дому, либо в других помещениях (местах).

Любое использование неучтенных носителей информации ограниченного доступа в КАИС КРО (обработка, прием, передача информации), инициированное сотрудником Учреждения, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором безопасности КАИС КРО). Администратор безопасности КАИС КРО имеет право блокировать или ограничивать использование носителей информации ограниченного доступа, используемых в КАИС КРО.

Информация об использовании сотрудником Учреждения носителей информации ограниченного доступа протоколируется и, при необходимости, может быть предоставлена лицу, ответственному за организацию обработки персональных данных в КАИС КРО.

В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации ограниченного доступа инициируется служебная проверка, проводимая комиссией, состав которой утвержден *(указывается должность)*.

По факту выясненных обстоятельств составляется акт проверки инцидента и передается (указывается должность) для принятия мер согласно действующему законодательству Российской Федерации.

Информация, хранящаяся на носителях информации ограниченного доступа, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения. На носители информации ограниченного доступа записывается только предназначенная пользователям информация. Отправка информации третьей стороне на носителях информации ограниченного доступа осуществляется в порядке, установленном соответствующим регламентом взаимодействия.

В случае утраты, уничтожения носителей информации ограниченного доступа необходимо поставить в известность руководителя соответствующего структурного подразделения. Соответствующие отметки вносятся в журналы учета носителей информации ограниченного доступа.

Носители информации ограниченного доступа, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение носителей информации ограниченного доступа осуществляется уполномоченной комиссией. По результатам уничтожения носителей информации ограниченного доступа составляется акт об уничтожении носителей информации ограниченного доступа.

В случае увольнения сотрудника предоставленные ему носители информации ограниченного доступа изымаются.

4. Ответственность

Сотрудники Учреждения, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 3
к приказу от 02.09.2024 года №80-о

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических (аппаратных) средств и программного обеспечения, баз данных и средств защиты информации в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»

1. Назначение и область действия

Настоящая Инструкция определяет:

меры защиты от утери информации;

действия по восстановлению информации в случае ее утери;

ответственность должностных лиц, связанных с резервным копированием и восстановлением информации.

Под резервным копированием информации понимается создание избыточных копий информации в электронном виде для быстрого восстановления работоспособности в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» (далее – КАИС КРО) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

Действие настоящей Инструкции распространяется на всех сотрудников Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы № 490 с углубленным изучением иностранного языка Красногвардейского района Санкт-Петербурга (далее – Учреждение), имеющих доступ к ресурсам КАИС КРО, а также на основные технические средства, программное обеспечение и средства защиты информации КАИС КРО.

Сотрудниками Учреждения, ответственными за реагирование на сбои, которые могут привести к потере информации, назначаются:

сотрудники, непосредственно обрабатывающие информацию, содержащуюся в КАИС КРО;

администратор безопасности КАИС КРО.

2. Общие требования к резервному копированию

В настоящей Инструкции описываются следующие организационно-технические мероприятия:

резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);

контроль резервного копирования;

хранение резервных копий;

полное или частичное восстановление данных.

Копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию.

Техническое обеспечение систем резервного копирования должно:

являться комплексом взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающихся на единой технологической платформе;

иметь возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации.

Программное обеспечение систем резервного копирования должно иметь лицензию и сертификат соответствия по безопасности информации, а также обеспечивать простоту процесса инсталляции, конфигурирования и сопровождения.

Сопровождение системы резервного копирования возлагается на *администратора безопасности*, который обязан следить за работоспособностью программных и аппаратных средств, осуществляющих резервное копирование в соответствии с их инструкциями по эксплуатации.

Предварительный учет машинных носителей с резервными копиями производится в отдельном журнале учета машинных носителей для резервного копирования, который находится у администратора безопасности. Все машинные носители с резервными копиями маркируются, на них указывается предназначение носителя.

В случае неотделимости носителей резервируемой информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

Хранение отдельных машинных носителей с резервными копиями организуется в отдельном помещении, физический доступ к которому строго ограничен. Контроль за физическим доступом возлагается на администратора безопасности.

Доступ к машинным носителям с резервными копиями имеют только (*указываются должности или наименование подразделений)*, которые несут персональную ответственность за сохранность резервных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

Машинные носители с резервными копиями изымаются для работы только работником, непосредственно осуществляющим резервное копирование, под подпись в журнале учета машинных носителей с резервными копиями. Передача машинных носителей с резервными копиями без документального оформления не допускается.

Уничтожение отделяемых машинных носителей с резервными копиями производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

3. Периодичность резервного копирования общего программного обеспечения

Резервное копирование общего программного обеспечения производится в соответствии со следующим графиком:

ежедневно производится резервное копирование конфигурационных файлов общего программного обеспечения;

еженедельно производится резервное копирование конфигурационных файлов общего программного обеспечения.

4. Периодичность резервного копирования специального программного обеспечения

Резервное копирование специального программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

5. Периодичность резервного копирования баз данных

Полное резервное копирование баз данных производится ежедневно.

Не реже 1 раза в неделю выполняется проверка наличия файлов последних (на момент проверки) резервных копий, а также содержимого соответствующих журнальных файлов выполнения процедуры резервного копирования.

В случае необнаружения файлов последних (на момент проверки) резервных копий или содержимого соответствующих журнальных файлов выполнения процедуры резервного копирования осуществляется полное резервное копирование баз данных.

В случае отсутствия требуемого пространства хранения резервных копий, выявленного в результате проверки наличия файлов последних резервных копий или журнальных файлов

выполнения процедуры резервного копирования и невозможности выделения пространства для хранения резервных копий выполнятся:

очистка созданных дополнительных резервных копий;

очистка временных объектов, образовавшихся в результате сопровождения КАИС КРО;

настройка свободного, нераспределенного пространства, имеющегося на устройстве хранения резервных копий объекта КАИС КРО.

6. Восстановление информации из резервных копий

В случае необходимости восстановление данных из резервных копий производится администратором безопасности КАИС КРО.

Восстановление данных из резервных копий производится в случае ее исчезновения или нарушения вследствие несанкционированного доступа в КАИС КРО, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного и специализированного программного обеспечения производится с резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей информации. При этом используется последняя копия информации.

При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

7. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в КАИС КРО возлагается на администратора безопасности КАИС КРО.

В случае обнаружения попыток несанкционированного доступа к носителям резервной информации, а также иных нарушений информационной безопасности, произошедших в процессе резервного копирования, необходимо сообщить *(указывается должность или наименование подразделения)* служебной запиской в течение рабочего дня после обнаружения указанного события.

Приложение № 4
к приказу от 02.09.2024 № 80-о

ИНСТРУКЦИЯ
по обеспечению защиты информации, содержащейся в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»

Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность пользователя, администратора безопасности и системного администратора в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» (далее – КАИС КРО), а также их права и ответственность.

Средства защиты информации от несанкционированного доступа предназначены для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил и обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации.

1. Обязанности пользователя КАИС КРО

Пользователь КАИС КРО обязан:

использовать КАИС КРО для выполнения служебных задач;

работать в КАИС КРО строго в соответствии с должностной инструкцией;

использовать для доступа к КАИС КРО собственную уникальную учетную запись (логин и пароль/персональный идентификатор);

хранить в тайне данные учетной записи для доступа к КАИС КРО, не оставлять без присмотра персональный идентификатор;

не допускать при работе с КАИС КРО просмотр посторонними лицами информации ограниченного доступа, отображаемой на дисплее автоматизированного рабочего места;

блокировать экран дисплея автоматизированного рабочего места парольной заставкой при оставлении рабочего места;

соблюдать правила работы со средствами защиты информации в соответствии с эксплуатационной документацией и установленным режимом разграничения доступа к программным и техническим средствам КАИС КРО;

хранить в тайне пароли доступа к КАИС КРО;

немедленно информировать администратора безопасности КАИС КРО в случае обнаружения попыток несанкционированного доступа к КАИС КРО;

немедленно информировать сотрудников, осуществляющих системное администрирование, или сообщать администратору безопасности КАИС КРО при появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении автоматизированного рабочего места или возникновении неисправностей (сбоев) в работе сервисов КАИС КРО.

2. Обязанности и функции администратора безопасности КАИС КРО

Администратор безопасности КАИС КРО обязан:

докладывать по подчиненности о выявленных нарушениях и несанкционированных действиях пользователей и персонала, принимать необходимые меры по устранению нарушений;

совместно со специалистами (указываются должности или наименование подразделения) принимать меры по восстановлению работоспособности средств защиты информации от несанкционированного доступа;

проводить инструктаж по правилам работы с используемыми средствами защиты информации от несанкционированного доступа.

Основными функциями администратора безопасности КАИС КРО являются:

поддержание функционирования средств защиты информации от несанкционированного доступа, в пределах возложенных обязанностей;

обучение персонала и пользователей вычислительной техники правилам работы со средствами защиты информации от несанкционированного доступа;

формирование и распределение списка ролей пользователей, определяемых эксплуатационной документацией на средства защиты информации от несанкционированного доступа;

участие в проведении служебных проверок фактов нарушения или угрозы нарушения безопасности информации;

текущий контроль соблюдения требований инструкций по эксплуатации средств защиты информации от несанкционированного доступа.

3. Обязанности системного администратора КАИС КРО

Системный администратор КАИС КРО обязан:

обеспечивать функционирование и поддержание работоспособности программных и аппаратных средств КАИС КРО;

определять права и правила разграничения доступа пользователей в КАИС КРО;

осуществлять установку и настройку специального программного обеспечения КАИС КРО;

сообщать администратору безопасности КАИС КРО и непосредственному руководителю о выявленных нарушениях и несанкционированных действиях пользователей и принимать необходимые меры по устранению нарушений;

совместно с администратором безопасности КАИС КРО и специалистами *(указываются должности или наименование подразделения)* принимать меры по восстановлению работоспособности средств защиты информации от несанкционированного доступа;

участвовать в проведении служебных проверок фактов нарушения или угроз нарушения безопасности информации;

осуществлять контроль соблюдения пользователями требований эксплуатационной документации на программные и аппаратные средства КАИС КРО.

4. Права пользователя КАИС КРО

Пользователь КАИС КРО имеет право:

обращаться к администратору безопасности КАИС КРО по вопросам эксплуатации средств защиты информации КАИС КРО;

обращаться к системному администратору КАИС КРО по вопросам функционирования системного и прикладного программного обеспечения КАИС КРО;

обращаться к системному администратору КАИС КРО по вопросам дополнительного оснащения автоматизированных рабочих мест техническими и программными средствами в случае служебной необходимости.

5. Ответственность пользователя КАИС КРО

Пользователь КАИС КРО несет ответственность:

за обеспечение безопасности информации, содержащейся в КАИС КРО, при ее обработке в КАИС КРО;

за нарушение работоспособности или вывод из строя средств защиты информации автоматизированного рабочего места;

за преднамеренные действия, повлекшие модификацию или уничтожение информации ограниченного доступа в КАИС КРО, и несанкционированный доступ к информации ограниченного доступа в КАИС КРО;

за разглашение информации ограниченного доступа.

За нарушение настоящей Инструкции к пользователю могут применяться меры дисциплинарного воздействия.

6. Ответственность администратора безопасности КАИС КРО

На администратора безопасности КАИС КРО возлагается персональная ответственность за качество проводимых им работ по эксплуатации средств защиты информации от несанкционированного доступа в соответствии с функциональными обязанностями, определенными инструкцией администратора безопасности КАИС КРО.

За нарушение требований настоящей Инструкции администратор безопасности КАИС КРО несет ответственность в соответствии с действующим законодательством Российской Федерации.

7. Ответственность системного администратора КАИС КРО

На системного администратора КАИС КРО возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в КАИС КРО в соответствии с функциональными обязанностями, определенными инструкцией системного администратора КАИС КРО.

За нарушение требований настоящей Инструкции системный администратор КАИС КРО несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 5
к приказу от 02.09.2024 № 80-о

РЕГЛАМЕНТ
администрирования учетных записей пользователей государственной информационной системы Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»

1. Общие положения

Настоящий Регламент определяет вопросы регистрации и изменения учетных записей пользователей в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» (далее – КАИС КРО).

Управление учетными записями пользователей КАИС КРО возлагается на системного администратора и администратора безопасности.

2. Правила присвоения учетных записей пользователям

В КАИС КРО существует два вида учетных записей:

учетная запись администратора, позволяющая управлять учетными записями пользователей и осуществлять настройку правил разграничения доступа;

учетная запись пользователя, предназначенная для авторизации пользователя в КАИС КРО.

С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю КАИС КРО должна быть сопоставлена учетная запись и пароль, под которыми он будет однозначно идентифицироваться в КАИС КРО. Использование несколькими сотрудниками при работе одной и той же учетной записи запрещается.

Любые действия с учетными записями пользователей сотрудниками, не уполномоченными на проведение подобных действий, запрещаются и идентифицируются как факт несанкционированного доступа.

3. Порядок создания и изменения учетных записей пользователей

Основанием для создания и изменения учетной записи пользователя является письменная заявка администратора безопасности на имя *руководителя Учреждения*, с указанием сотрудника(-ов), которому(-ым) требуется создать (изменить) учетную запись. Заявка согласуется с администратором безопасности КАИС КРО и передается системному администратору КАИС КРО. Системный администратор КАИС КРО рассматривает предоставленную заявку и совершает необходимые операции по созданию (изменению) учетной записи пользователя(-ей), присвоению ему начального значения пароля и необходимых прав доступа к КАИС КРО.

4. Порядок блокировки и уничтожения учетных записей пользователей

При прекращении срока действия полномочий пользователя, а также на период временного отсутствия пользователя учетная запись должна блокироваться.

Основанием для блокировки и уничтожения учетной записи пользователя является письменная заявка (*указываются должности*) на имя *(указывается фамилия, имя, отчество, должность)*. Заявка согласуется с администратором безопасности КАИС КРО и передается системному администратору КАИС КРО. Системный администратор КАИС КРО рассматривает предоставленную заявку и совершает необходимые операции по блокировке и уничтожению учетной записи пользователя КАИС КРО.

5. Ответственность пользователей

В целях предотвращения несанкционированного доступа к информации в КАИС КРО определяется ответственность пользователей КАИС КРО по соблюдению правил использования учетных записей пользователей КАИС КРО.

Пользователям КАИС КРО запрещается работать под чужими учетными записями.

Пользователи КАИС КРО обязаны хранить в тайне учетную запись и пароль для доступа к КАИС КРО.

Приложение № 6
к приказу от 02.09.2024 № 80-о

ПРАВИЛА
доступа к персональным данным, обрабатываемым в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга»

1. Общие положения

Настоящие Правила определяют порядок доступа к персональным данным, обрабатываемым в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга» (далее – КАИС КРО), лиц, имеющих право доступа к этим персональным данным.

Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Безопасность персональных данных при их обработке в КАИС КРО обеспечивается с помощью подсистемы «Система защиты информации» КАИС КРО.

2. Организация доступа к персональным данным

Организация доступа к персональным данным, обрабатываемым в КАИС КРО, лиц, имеющих право доступа к персональным данным для выполнения ими служебных (трудовых) обязанностей, должностным лицом, ответственным за организацию обработки персональных данных в КАИС КРО.

На основании Перечня лиц, имеющих право доступа к персональным данным, обрабатываемым в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», для выполнения ими служебных (трудовых) обязанностей, должностное лицо, ответственное за организацию обработки персональных данных в КАИС КРО, разграничивает доступ к персональным данным.

Перечень лиц, имеющих право доступа к персональным данным, обрабатываемым в КАИС КРО, для выполнения ими служебных (трудовых) обязанностей, составляется как на электронном, так и на бумажном носителях.

Должностное лицо, ответственное за организацию обработки персональных данных в КАИС КРО, на основании Перечня лиц, имеющих право доступа к персональным данным, обрабатываемым в государственной информационной системе Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга», предоставляет пользователям доступ к персональным данным, проверяет на его автоматизированном рабочем месте заданные возможности доступа.

3. Обязанности лиц, имеющих право доступа к персональным данным, обрабатываемым в КАИС КРО

Лица, имеющие доступ к персональным данным КАИС КРО, обязаны:
не сообщать персональные данные лицам, не имеющим права доступа к ней;
обеспечивать сохранность материалов с персональными данными;

не делать неучтенных копий на бумажных и электронных носителях;

не оставлять включенным автоматизированное рабочее место с предоставленными правами доступа после окончания работы (в перерывах), не оставлять материалы с персональным данными на рабочих столах;

при работе с документами, содержащими персональные данные, исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;

не вносить изменения в настройку средств защиты информации;

немедленно сообщать непосредственному руководителю об утрате, утечке или искажении персональных данных, об обнаружении неучтенных материалов с указанной информацией;

не допускать действий, способных повлечь утечку персональных данных;

предъявлять для проверки лицам, наделенным необходимыми полномочиями в соответствии с законодательством Российской Федерации, числящиеся и имеющиеся в наличии документы, касающиеся персональных данных, только по согласованию с руководителем Учреждения.

4. Порядок доступа должностных лиц органов государственной власти, должностных лиц и субъектов персональных данных к персональным данным

Право доступа к персональным данным имеют должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, которым доступ к такой информации предусмотрен федеральными законами.

Право доступа к персональным данным имеют должностные лица, которым доступ к такой информации предусмотрен федеральными законами и (или) приказами Учреждения.

Доступ к персональным данным субъектов персональных данных осуществляется на основании направленного запроса.

5. Заключительные положения

При работе с документами, связанными с предоставлением персональных данных, должен обеспечиваться режим ограниченного доступа к соответствующим документам.

Лица, допущенные к персональным данным, должны ознакомиться с настоящими Правилами под подпись.

Лица, виновные в нарушении требований настоящих Правил и иных документов, регламентирующих вопросы защиты персональных данных, несут ответственность в соответствии с действующим законодательством Российской Федерации.