ПРИЛОЖЕНИЕ № 15
К ПРИЗАЗУ МАОУ «СОШ № 2»
«ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ»
ОТ 03.10.2023 № 390

ПРАВИЛА ДОСТУПА В ПОМЕЩЕНИЯ С УСТАНОВЛЕННЫМИ СРЕДСТВАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

Настоящий документ описывает правила доступа в помещения, в которых установлены средства информационной защиты информации (далее - ИСПДн).

Настоящий документ разработан в целях выполнения требований Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

2. Требования к помещениям, где установлены СКЗИ.

ИСПДн необходимо устанавливать в помещения с капитальными стенами, прочными металлическими или деревянными дверями. Входные двери оборудуются двумя замками (внутренним и автоматическим) и охранной сигнализацией.

Окна этих помещений на первом этаже, а также на других, расположенных возле пожарных лестниц, балконов и других сооружений, откуда возможно бесконтрольное проникновение посторонних лиц, должны иметь заделанные в стены металлические решетки (или должны быть установлены датчики сигнализации на открытие окон).

По окончанию рабочего дня входные двери запираются. Ключи от рабочих комнат, опечатанных печатями ответственных лиц, сдаются в опечатанном виде дежурному охраннику, под роспись в журнале приема-сдачи помещений под охрану, с указанием времени сдачи и отметкой о включении сигнализации.

При размещении ИСПДн необходимо выполнять следующие требования:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными ИСПДн, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на ИСПДн, технические средства, на которых эксплуатируется ИСПДн и защищаемую информацию;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.
- оснащение помещений, где установлены ИСПДн входными дверьми с замками, для обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

3. Порядок доступа в помещения, где установлены ИСПДн.

Вход в помещение, где установлены и хранятся ИСПДн, разрешен сотрудникам, служебные обязанности которых предусматривают допуск к работе с данными ИСПДн.

Доступ других лиц в данные помещения в случае служебной необходимости возможен только с разрешения руководителя.

Все помещения, где установлены и хранятся ИСПДн, должны быть оборудованы в противопожарном отношении.

Уборка, ремонт и другие работы в помещениях, где установлены и хранятся ИСПДн, производится только в присутствии работников данного отдела.

В случае срабатывания охранно-пожарной сигнализации в помещении, где ИСПДн, дежурный обязан:

– вызвать ответственного сотрудника за помещение, где сработала сигнализация, и сообщить о срабатывании охранно-пожарной сигнализации ответственному за обеспечение безопасности персональных данных в организации;

– проверить целостность замков и печати на входной двери помещения и отсутствие запаха дыма;

– наружным осмотром здания убедиться в целостности стекол на окнах помещения.

При ложном срабатывании охранно-пожарной сигнализации (отсутствии следов проникновения в охраняемое помещение и признаков пожара), дежурный ожидает прибытия ответственного сотрудника за данное помещение для проверки и переустановки сигнализации.

При обнаружении следов вскрытия помещения дежурный обязан:

– вызвать наряд полиции по телефону **02**;

– сообщить руководителю, ответственному за обеспечение безопасности персональных данных в организации о случившемся и далее действовать по их указаниям;

– до прибытия работников полиции обеспечить охрану места происшествия.

В случае других нештатных ситуаций (пожара, аварий отопления, водоснабжения и т.п.) дежурный действует в соответствии с «Инструкцией по обеспечению безопасности обработки персональных данных, при возникновении нештатных ситуаций в организации».