Государственное бюджетное учреждение дополнительного профессионального образования Воронежской области «Институт развития образования имени Н. Ф. Бунакова»

СОГЛАСОВАНО

Директор Центра цифровой трансформации образования ГБУ ДПО ВО «ВИРО им. Н.Ф. Бунакова»

_____Д. Г. Плотников

м.п.

«__» _____ 2020 г.

УТВЕРЖДАЮ

Ректор
ГБУ ДПО
«ВИРО им. Н. Ф. Бунакова»

_____А. Ю. Митрофанов

м.п.

«__» _____ 2020 г.

ПРАВИЛА

доступа в помещения, в которых
расположены информационные системы
и/или хранятся материальные носители информации
ограниченного доступа (в т.ч. персональных данных)

Воронеж, 2020

1 Общие положения

1.1 Настоящие Правила доступа в помещения, в которых расположены информационные системы и/или хранятся материальные носители информации ограниченного доступа (в т.ч. персональных данных), в рабочее и нерабочее время, а также в нештатных ситуациях, Государственного бюджетного учреждения дополнительного профессионального образования Воронежской области «Институт развития образования имени Н. Ф. Бунакова» (далее – Оператор, Правила) разработаны в соответствии с требованиями:

– пункта 1 б Постановления Правительства от 21.03.2012 г. № 211;

– пункта 15 Постановления Правительства от 15.09.2008 № 687;

– пункта 6.б Приказа ФСБ России от 10 07.2014 г. № 378;

– меры ЗТС.3 Приказа ФСТЭК России от 11.02.2013 г. № 17.

1.2 Настоящие Правила вступают в силу с момента их утверждения руководителем Оператора и действуют бессрочно, до их замены новыми Правилами или их отмены на основании приказа руководителя Оператора.

1.3 Все работники Оператора должны быть ознакомлены с настоящими Правилами под подпись.

1.4 Каждый работник, допущенный в помещения, в которых ведется обработка информации ограниченного доступа, несет персональную ответственность за соблюдение данных Правил.

2 Правила доступа в Помещения

2.1 Правила определяют порядок доступа и правила охраны (обеспечения безопасности) помещений, в которых осуществляется обработка и/или информации ограниченного доступа (далее – Помещения).

2.2 Целью организации режима обеспечения безопасности Помещений является обеспечение безопасности информации ограниченного доступа, сохранности носителей информации ограниченного доступа и средств защиты информации.

2.3 ***Перечень Помещений*** утверждается руководством Оператора.

2.4 Доступ в Помещения должен быть предоставлен только работникам, указанным в ***Перечне лиц, имеющих право доступа в помещения в рабочее и нерабочее время***.

2.5 Нахождение в Помещениях лиц, не входящих в указанный выше перечень, допускается только в сопровождении работника, допущенного к работе в таких Помещениях.

2.6 Для всех Помещений организуется режим обеспечения безопасности, который должен включать в себя минимум следующие мероприятия:

– расположение в Помещении средств вычислительной техники, предназначенных для визуализации обрабатываемой информации (телевизоров, мониторов, экранов мобильных устройств и пр.), исключающее возможность просмотра лицами, находящимися в данном Помещении (рядом со входом в данное Помещение, или рядом с окном Помещения в случае расположения Помещений на первых этажах зданий) и не допущенными к обработке информации ограниченного доступа;

– запирание Помещений на ключ по окончании рабочего дня, а также в рабочее время в случае отсутствия в Помещении других сотрудников, допущенных в данное Помещение;

– закрытие шкафов и сейфов, предназначенных для хранения носителей информации ограниченного доступа, на ключ по окончании рабочего дня, а также в рабочее время в случае отсутствия в Помещении других сотрудников, допущенных в данное Помещение;

– сдачу Помещения под охрану по окончании рабочего дня.

2.7 Доступ работников в Помещения в нерабочее время должен осуществляться только с письменного разрешения Ответственного за защиту информации.

2.8 В конце рабочего дня все материальные носители информации ограниченного доступа должны быть помещены в шкафы и сейфы, предназначенные для их хранения.

В случае отсутствия в помещении шкафов и сейфов, все носители информации ограниченного доступа должны быть сданы Ответственному за защиту информации.

В случае, если материальный носитель содержит информацию ограниченного доступа, зашифрованную с использованием средств криптографической защиты информации, то допускается хранение такого носителя информации вне шкафа или сейфа.

Все технические средства и электроприборы (за исключением устройств, для которых определен круглосуточный режим работы) должны быть обесточены.

2.9 Открытие и закрытие Помещений должны фиксироваться в специальном ***Журнале открытия и закрытия помещений, в которых ведется обработка информации ограниченного доступа***, с указанием лица, осуществившего открытие и закрытие Помещения.

2.10 При закрытии Помещений, не подключенных к автоматизированной системе контроля и управления доступом, двери Помещений подлежат опечатыванию с использованием личных печатей работников.

2.11 При закрытии Помещений, металлические шкафы (сейфы), расположенные в них и предназначенные для хранения съемных машинных

носителей ПДн и не подключенные к автоматизированной системе контроля и управления доступом, подлежат опечатыванию с использованием личных печатей работников.

2.12 При открытии Помещения в начале рабочего дня работник обязан провести визуальный осмотр с целью установления целостности двери, замков и печати в случае, если для данного Помещения применяемся процедура опечатывания. В случае возникновения подозрений о попытке взлома двери или замка работник обязан уведомить об этом сотрудников охраны и Ответственного за защиту информации. При этом самостоятельная попытка вскрытия такого Помещения самим работником запрещается.

2.13 В случае возникновения нештатных ситуаций в Помещениях, создающих угрозу жизни и здоровью работников, находящихся в данных Помещениях (возникновение пожара, повреждение конструкций здания и т.п.), в первую очередь необходимо обеспечить безопасность самих работников, не взирая на сохранность материальных носителей ПДн и осуществляющих их обработку средств вычислительной техники.

В случае возникновения нештатных ситуаций, не несущих непосредственной угрозы жизни и здоровью работников (отключение электропитания, поломка средств вычислительной техники и т.п.), работники обязаны уведомить об этом Ответственного за защиту информации.

В случае необходимости принятия в нерабочее время экстренных мер (при срабатывании пожарной или охранной сигнализации, авариях в сетях электро- и водоснабжения, и т.п.), Помещение может быть вскрыто ответственным персоналом, в том числе сотрудниками, не допущенными к обработке информации ограниченного доступа (сотрудниками охраны, пожарным расчетом и т.п.).

2.14 Уборка Помещений должна производиться под контролем сотрудника, имеющего доступ в Помещение и постоянно в нем работающего.

2.15 Вынос технических средств обработки информации ограниченного доступа за пределы контролируемой зоны с целью их ремонта, замены, утилизации и т.п. без согласования с Ответственным за защиту информации, запрещен. При принятии решения о выносе средств вычислительной техники, электронные носители информации должны быть демонтированы и сданы на хранение Ответственному за защиту информации. В случае действия гарантийных обязательств фирмы-поставщика средств вычислительной техники, вскрытие корпуса и демонтаж носителей информации должны быть предварительно согласованы с ней.

2.16 Установка нового оборудования, мебели и т.п. или их замены, а также ремонт Помещения должны проводиться только по согласованию с Ответственным за защиту информации.