	Министерство образования и молодежной политики Свердловской области
	Государственное автономное профессиональное образовательное учреждение Свердловской области **«Екатеринбургский техникум химического машиностроения»**
	Порядок доступа работников ГАПОУ СО «ЕТХМ»

Рассмотрено
на заседании Совета
ГАПОУ СО «ЕТХМ»
Протокол № 3,
от « 31 » января 2020 г.

УТВЕРЖДЕНО
Приказом директора
ГАПОУ СО «ЕТХМ»
№ 24 - о/д от « 03 » февраля 2020 г.

ПОРЯДОК
ДОСТУПА РАБОТНИКОВ ГОСУДАРСТВЕННОГО АВТОНОМНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ «ЕКАТЕРИНБУРГСКИЙ ТЕХНИКУМ ХИМИЧЕСКОГО МАШИНОСТРОЕНИЯ» В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА И РАСПОЛОЖЕНЫ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Екатеринбург
2020 г.

Введено в действие с 03.02.2020 г.

1. Общие положения

1.1. Настоящий Порядок доступа работников в помещения ГАПОУ СО «Екатеринбургский техникум химического машиностроения» (далее - Учреждение), в которых ведется обработка информации ограниченного доступа, в том числе персональных данных, (далее - Информации) не содержащей сведения, составляющие государственную тайну, и расположены средства криптографической информации разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» и другими нормативными правовыми актами.

1.2. Обеспечение безопасности Информации от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении Информации достигается, в том числе, установлением правил доступа в помещения, где обрабатывается Информация с использованием и/или без использования средств автоматизации.

1.3. Размещение информационных систем (далее-ИС), в которых обрабатывается Информация, должно осуществляться в пределах контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Для помещений, в которых обрабатывается Информация (далее - Помещения) и расположены средства криптографической защиты информации (далее - СКЗИ), организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей Информации и средств защиты информации, криптосредств и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

2. Допуск в помещения, в которых ведётся обработка информации ограниченного доступа

2.1. В помещения, где размещены технические средства, позволяющие осуществлять обработку Информации, а также хранятся носители Информации, допускаются только работники, уполномоченные на обработку Информации (в соответствии с Перечнем лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных

системах», а также только лица, имеющие право доступа в помещения Учреждения, где осуществляется обработка Информации.

2.2. При оборудовании Помещений должны выполняться требования к размещению, монтажу крипто средств, а также другого оборудования, функционирующего с крипто средствами.

2.3. Нахождение в помещениях с ИС лиц, не включенных в перечни, указанные в пункте 2.1. настоящего порядка, возможно только в присутствии работника, уполномоченного на обработку Информации в данном помещении. Время нахождения в помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

2.4. Работники, допущенные к обработке Информации, не должны покидать Помещение, не убедившись, что доступ посторонних лиц к Информации невозможен. Запрещается оставлять материальные носители Информации без присмотра в незапертом помещении.

2.5. Помещения, в которых ведется обработка Информации и расположены средства криптографической информации, должны быть оснащены входными дверьми с замками. Кроме того, должно быть обеспечено постоянное закрытие дверей таких помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

2.6. Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

2.7. После окончания рабочего дня дверь каждого помещения, в котором ведется обработка Информации, закрывается на ключ и ставится на сигнализацию.

2.8. В нерабочее время помещения, в которых осуществляется функционирование СКЗИ, должны ставиться на охрану, при этом все окна и двери должны быть надежно закрыты, ключевые документы убраны в запираемые шкафы (сейфы).

2.9. Ключ на технические устройства, сигнализирующие о несанкционированном вскрытии помещений ответственный сдает/получает ответственному сотруднику под подпись в журнале при назначении/увольнении на должность. Ключ выдается сотрудником, ответственным за ведение журнала учёта ключей от помещений.

3. Допуск лиц в помещения

3.1. Для предотвращения просмотра извне окна Помещений должны быть защищены шторами или жалюзи.

3.2. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц,

оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Помещения.

3.3. При утрате ключа от хранилища или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых документов и технической и эксплуатационной документации к СКЗИ в хранилище, от которого утрачен ключ, устанавливает ответственный за использование СКЗИ.

3.4. Внутренний контроль за соблюдением порядка доступа в помещения, проводится в порядке, определенном в плане проведения внутреннего контроля соответствия требованиям по защите. Контроль и управление физическим доступом к информационным системам и средствам криптографической защиты должны предусматривать:

- поддерживание в актуальном состоянии Перечня лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах;
- санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены - выдача ключей от помещений строго в соответствии с утвержденным перечнем лиц;
- учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены - выдача ключей от помещений под подпись в соответствующем журнале.

3.5. В обычных условиях помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ или ответственным пользователем СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

3.6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка Информации и расположены средства

криптографической информации, возлагается на сотрудников структурных подразделений, уполномоченных на обработку Информации в Учреждении.

3.7. В случае нарушения настоящего Порядка работники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

Разработал:
Заместитель директора по УПР Н.В. Катанэ