Приложение 4
к приказу директора
ГБПОУ КК УТМиПТ
от 25.03.2024 г. № 64/1

ПРАВИЛА
доступа в помещения государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий», в которых ведется обработка защищаемой информации, в том числе персональных данных

1. Общие положения

1.1. Настоящие Правила устанавливают порядок доступа в помещения государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация), в которых ведется обработка конфиденциальной и защищаемой информации, в том числе персональных данных (далее – Информация).

1.2. Правила разработаны в целях обеспечения безопасности информации, обрабатываемой в образовательной организации, на средствах вычислительной техники информационных систем, на материальных носителях информации, а также для обеспечения внутриобъектового режима.

1.3. Настоящий Порядок устанавливает правила доступа в следующие помещения образовательной организации:

помещения, в которых происходит обработка информации, как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения (при наличии);

помещения, в которых хранятся материальные носители информации и их резервные копии;

помещения, в которых установлены средства криптографической защиты информации (далее – СКЗИ) и хранятся носители ключевой информации, в том числе средства электронной подписи (далее – Спецпомещения).

1.4. Настоящий Порядок разработан в соответствии с:

1.4.1 Федеральным законом Российской Федерации от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

1.4.2 постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.4.3 приказом Федеральной службой безопасности России от 10 июля 2014 г. № 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»;

1.4.4 приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 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».

1.5. В каждом структурном подразделении образовательной организации назначается ответственное лицо за доступ в помещения.

1.6. Работники образовательной организации, допущенные в помещения, обязаны:

выполнять требования обеспечения безопасности информации;

соблюдать режим конфиденциальности при обращении с информацией, носителями информации и СКЗИ (в том числе ключевыми документами к ним);

своевременно выявлять попытки посторонних лиц получить сведения об Информации, об используемых СКЗИ или ключевых документах к ним;

предусматривать раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

2. Общие требования к оборудованию помещений и регламентации доступа в них

2.1. Режим обеспечения безопасности помещений, в которых осуществляется обработка Информации (далее – Помещения) должен быть организован таким образом, чтобы препятствовать возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2.2. Ограждающие конструкции помещений, должны предполагать существенные трудности для нарушителя по их преодолению (например, металлические решетки на окнах, металлическая дверь, система контроля и управления доступом и так далее).

2.3. Помещения должны быть оснащены надежными входными дверьми с замками, а также средствами опечатывания помещений по окончании рабочего дня.

2.4. Окна помещений, расположенных на первых этажах зданий, а также окна, находящиеся около мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

2.5. Доступ посторонних лиц в помещения, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица из числа работников, допущенных в помещение. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с защищаемой информацией. Такими мерами являются:

размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации;

размещение документации на бумажных носителях, содержащих информацию, исключающее просмотр информации на них (документация убирается в папки, ящики тумбочек/столов, либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

2.6. В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка информации, должны быть надежно закрыты, материальные носители должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

2.7. При необходимости повышенного уровня обеспечения безопасности помещений могут использоваться системы видеонаблюдения и системы контроля и управления доступом.

3. Особенности доступа в спецпомещения

3.1. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

3.2. Расположение спецпомещений, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.3. Двери спецпомещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытия только для санкционированного прохода.

3.4. При утрате ключа от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей (с документальным оформлением).

3.5. Доступ работников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов).

3.6. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц из числа работников образовательной организации.

3.7. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя подразделения или замещающего его лица.

3.8. Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается