АНТИТЕРРОРИСТИЧЕСКАЯ КОМИССИЯ АРСЕНЬЕВСКОГО ГОРОДСКОГО ОКРУГА

ул. Ленинская 10А, г. Арсеньев, Приморский край, 692337, тел.: (42361) 4-37-40, E-mail: atk@ars.town

ПРАВИЛА

обработки, копирования, передачи и хранения служебной информации ограниченного распространения содержащейся в паспорте безопасности объекта

Паспорт безопасности объекта имеет пометку «Для служебного пользования» если ему не присваивается гриф секретности в соответствии с законодательством Российской Федерации и содержит служебную информацию ограниченного распространения (далее – информация ограниченного доступа) которая подлежит защите в соответствии с законодательством Российской Федерации.

При создании условий для обеспечения защиты информации ограниченного доступа, содержащейся в паспортах безопасности в соответствии с требованиями нормативных правовых актов Российской Федерации, регламентирующих порядок обращения с информацией ограниченного доступа следует руководствоваться следующими требованиями:

1. Обсуждение вопросов антитеррористической защищенности:

1.1. Во время обсуждения вопросов антитеррористической защищенности объектов в помещениях:

не допускается использование средств аудио- и видеозаписи, радиоустройств, в том числе средств сотовой связи;

установленные в помещениях проводные средства телефонной связи, а также все бытовые электроприборы на время проведения обсуждения должны быть отключены. Технические средства, сертифицированные по требованиям безопасности, или средства, прошедшие специальные исследования и, имеющие предписания на эксплуатацию, могут не отключаться;

окна помещений рекомендуется закрывать шторами (жалюзи);

доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в помещении, ограничивается.

2. Обработка информации ограниченного доступа:

2.1. Обработка информации ограниченного доступа должна производиться с использованием средств вычислительной техники (далее – СВТ), оснащенных системой защиты информации, в составе которой присутствуют система защиты информации от несанкционированного доступа и сертифицированное ФСБ и ФСТЭК России антивирусное программное обеспечение. В СВТ должны отсутствовать любые радиоинтерфейсы (беспроводные сетевые адаптеры, Bluetooth-адаптеры, GSM/GPRS/UMTS/LTE-модемы и т.п.), в том числе работающие по сети электропитания и с использованием излучений в инфракрасном (ИК) диапазоне.

2.2. СВТ, на котором производится обработка информации ограниченного

доступа, должно быть установлено таким образом, чтобы исключить несанкционированный просмотр выводимой на технические средства отображения и печати информации. В момент обработки информации ограниченного доступа в помещении не должно находиться посторонних лиц, не допущенных к данной информации.

2.3. **Не допускается** обработка информации ограниченного доступа на СВТ, подключенных (или имеющих возможность подключения) к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет.

Обработка информации ограниченного доступа с использованием социальных интернет-сетей («Facebook», «ВКонтакте», «Одноклассники» и т.д.), а также интернет-сервисов и программного обеспечения, таких как WhatsApp, Viber, Skype, Google, Yahoo и других, **запрещается.**

Размещение информации ограниченного доступа на ресурсах информационно-телекоммуникационной сети Интернет запрещается.

2.4. В случае если рабочее место не позволяет организовать выделенное СВТ для обработки информации ограниченного доступа, перед началом обработки информации ограниченного доступа на своем рабочем месте необходимо произвести следующие действия:

а) отключить используемое СВТ от сети общего пользования и информационно-телекоммуникационной сети Интернет путем физического извлечения Ethernet-кабеля из разъема СВТ;

б) извлечь из СВТ все съемные машинные носители информации (CD/DVD диски, Flash-накопители, внешние жесткие диски и т.п.), не требуемые для обработки информации ограниченного доступа;

в) извлечь из разъемов СВТ любые USB-устройства, использующие радиоинтерфейсы (мобильные телефоны, USB-модемы, Bluetooth-адаптеры и т.п.);

г) убедиться, что антивирусное программное обеспечение включено (резидентный модуль «Монитор») и имеет актуальную базу данных угроз;

д) при планируемом выводе на печать документов, содержащих информацию ограниченного доступа, убедиться, что используемый принтер имеет прямое проводное подключение к СВТ и не является сетевым;

е) убедиться, что в оперативной памяти СВТ не загружены прикладные программные средства, не участвующие в обработке информации ограниченного доступа (путем просмотра «Диспетчера задач»).

ж) по окончании обработки информации ограниченного доступа необходимо произвести стирание остаточной информации на несъемных носителях (жестких дисках) и в оперативной памяти путем перезагрузки СВТ.

3. Копирование (размножение, тиражирование) документов:

3.1. Копирование (размножение, тиражирование) документов с пометкой «Для служебного пользования» (далее – документы ДСП) производится только с разрешения руководителя объекта.

3.2. Для размножения (тиражирования) документов ДСП могут быть

использованы ксерографические копировально-множительные аппараты, которые по принципу действия не создают каналов побочных электромагнитных излучений и наводок.

Признаками таких аппаратов являются:

отсутствие кабельных вводов для подключения внешних устройств (ПЭВМ, монитора, вычислительной сети и т.д.);

отсутствие в комплекте аппарата накопителей (устройств памяти) для долговременного хранения информации.

4. Обмен информацией ограниченного доступа:

4.1. Передача информации ограниченного доступа по открытым радиоканалам, проводным каналам связи (в том числе по факсу), выходящим за пределы объекта, **запрещается**.

4.2. Обмен информацией ограниченного доступа между СВТ различных пользователей должен производиться посредством оптических дисков (CD-R/DVD-R), учтенных в соответствующем делопроизводстве. Использование в качестве носителей съемных устройств, подключаемых к портам USB (USB-Flash и т.п.) **не допускается**.

4.3. Использование средств информационного обмена, в том числе сети Интернет для передачи информации ограниченного доступа, допускается только при условии шифрования всей передаваемой информации. Шифрование информации должно производиться специальными, сертифицированными ФСБ и ФСТЭК России средствами криптографической защиты.

4.4. Пересылка документов ДСП в другие организации производится подразделениями фельдъегерской или специальной связи, а через отделения «Почты России» – заказными или ценными почтовыми отправлениями.

На конверте указывается адрес и наименования получателя и отправителя, номера вложенных документов, а в правом верхнем углу конверта проставляются пометки:

«Для служебного пользования» или «ДСП».

4.5. В случае пересылки документов ДСП при помощи электронной почты документ или пакет документов должен быть подписан усиленной квалифицированной электронной подписью отправителя и зашифрован при помощи сертифицированных ФСБ и ФСТЭК России средств криптографической защиты информации на открытом ключе получателя.

5. Условия хранения:

5.1. Условия хранения документов ДСП должны предотвращать свободный доступ к ним.

5.2. Хранение информации ограниченного доступа в СВТ в нерабочее время **запрещается**.

5.3. Хранение учтенных съемных машинных носителей служебной информации производится в служебных помещениях в надежно запираемых шкафах (ящиках, хранилищах), металлических сейфах. При необходимости шкафы (ящики, хранилища), сейфы и служебные помещения могут опечатываться личными металлическими номерными печатями.

6. Информация ограниченного доступа без письменной санкции руководителя

объекта разглашению (распространению) не подлежит.

За разглашение информации ограниченного доступа, а также нарушение порядка обращения с носителями сведений, содержащими такую информацию, виновное лицо привлекается к дисциплинарной ответственности.

О фактах утраты документов, содержащих информацию ограниченного доступа или разглашения такой информации, ставится в известность руководитель объекта и назначается комиссия для расследования обстоятельств утраты или разглашения.

Секретарь комиссии О.В. Зыков

СОГЛАСОВАНО

Начальник отдела в г. Арсеньеве
УФСБ России по Приморскому краю,
заместитель председателя комиссии

_____ С.А. Каськов
(личная подпись) (инициалы, фамилия)

06.08.2018