Приложение № 7
к приказу Комитета по внешним
связям Санкт-Петербурга
от 27.01.2015 № 1-П

# ИНСТРУКЦИЯ
## пользователя автоматизированной системы обработки конфиденциальной информации и персональных данных в Комитете по внешним связям Санкт-Петербурга

### 1. Общие положения

1.1. Настоящая Инструкция разработана для обеспечения защиты конфиденциальной информации, в том числе персональных данных, в автоматизированных системах, используемых в Комитете по внешним связям Санкт-Петербурга (далее – Комитет).

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.2. Наиболее вероятными каналами утечки информации для автоматизированных систем (далее – АС) являются:

несанкционированный доступ к информации, обрабатываемой в автоматизированной системе;

хищение технических средств, с хранящейся в них информацией, или отдельных носителей информации;

просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;

воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

1.3. Работа с конфиденциальной информацией, персональными данными, а также со служебными документами ограниченного распространения (далее – информация ограниченного распространения), строится на следующих принципах:

принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный сотрудник, выдача документов осуществляется под роспись;

принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

1.4. Ответственность за организацию защиты информации ограниченного распространения в Комитете возлагается на администратора безопасности информации Комитета (далее – администратор безопасности).

Ответственность за обеспечение безопасности информации ограниченного распространения возлагается на лиц, производящих ее обработку (далее -пользователи АС).

1.5. Техническое обслуживание компьютерной и организационной техники, сопровождение программного обеспечения, установка нового оборудования, мебели и т.п., а также уборка и ремонт помещения должны проводиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего, в порядке, исключающем нарушения правил обработки информации ограниченного распространения. Обработка информации ограниченного распространения в период проведения этих работ запрещается.

1.6. Вынос компьютерной техники, на которой проводилась обработка информации ограниченного распространения, за пределы Смольного с целью ее ремонта, замены и т. п. без согласования с администратором безопасности запрещен. При принятии решения о выносе компьютерной техники, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения Комитета. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы.

1.7. По фактам и попыткам несанкционированного доступа к информации ограниченного распространения, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

## 2. Обязанности пользователя АС

2.1. Перед допуском к работе в информационной системе персональных данных Комитета пользователь АС знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности автоматизированной обработки информации.

2.2. Сотрудник Комитета, получивший доступ к информации ограниченного распространения, обеспечивает ее защиту. Информация, полученная сотрудником в связи с выполнением служебных обязанностей,

доводится до строго ограниченного круга должностных лиц лишь в части, непосредственно относящейся к их служебной деятельности, в том числе после прекращения доступа к информации ограниченного распространения.

В случае увольнения с государственной гражданской службы из Комитета, назначения на должность в другое структурное подразделение Комитета сотрудник обязан сдать все документы и материалы, полученные (разработанные) в период прохождения государственной гражданской службы в структурном подразделении Комитета, его руководителю или назначенному для этой цели должностному лицу.

2.3. Работа сотрудника с информацией ограниченного распространения разрешается в условиях, исключающих возможность несанкционированного получения информации посторонними лицами.

2.4. Каждый сотрудник Комитета, участвующий в рамках своих служебных обязанностей в процессах автоматизированной обработки информации ограниченного распространения Комитета, несет персональную ответственность за свои действия *(сотрудники, виновные в нарушении режима защиты персональных данных, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность)* и обязан:

2.4.1. Строго соблюдать установленные правила обеспечения безопасности информации ограниченного распространения при работе с программными и техническими средствами АС Комитета.

2.4.2. Использовать для работы только учтенные установленным порядком съемные накопители информации (гибкие магнитные диски, карты памяти, компакт диски и т.д.);

2.4.3. Хранить в тайне свой аутентификатор (пароль доступа в АС);

2.4.4. Передавать для хранения в установленном порядке (при необходимости) свои реквизиты разграничения доступа только администратору безопасности.

2.4.5. Выполнять требования по антивирусной защите в части, касающейся действий пользователей АС.

2.4.6. Строго выполнять Правила обработки персональных данных в Комитете.

2.4.7. Немедленно ставить в известность своего непосредственного руководителя и администратора безопасности в следующих случаях:

в случае утери носителя с информацией ограниченного распространения;

при подозрении компрометации личного пароля;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АС Комитета;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АС Комитета, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

обнаружения непредусмотренных отводов кабелей и подключенных устройств;

обнаружения фактов и попыток несанкционированного доступа к информации и случаев нарушения установленного порядка обработки защищаемой информации;

2.4.8. При уходе с рабочего места активизировать средства защиты от несанкционированного доступа к информации, нажав сочетание клавиш на клавиатуре «Ctrl+Alt+Del» и выбрав пункт «Блокировка».

2.4.9. Копировать документы, содержащие информацию ограниченного распространения, с разрешения председателя Комитета, заместителей председателя Комитета. При этом копии регистрировать в учетных документах установленным порядком.

2.4.10. Выполнять требования администратора безопасности, касающиеся обеспечения безопасности информации ограниченного распространения.

2.5. Пользователю АС категорически запрещается:

2.5.1. Использовать компоненты программного и аппаратного обеспечения АС Комитета в неслужебных целях.

2.5.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АС Комитета или устанавливать дополнительно любые программные и аппаратные средства.

2.5.3. Осуществлять обработку информации ограниченного распространения в условиях, позволяющих доступ к ней посторонних (не допущенных к данной информации) лиц.

2.5.4. Записывать и хранить информацию ограниченного распространения на неучтенных носителях информации (гибких магнитных дисках и т.п.).

2.5.6. Оставлять включенным без присмотра АС, не активизировав средства защиты от несанкционированного доступа к информации.

2.5.7. Оставлять без личного присмотра на АС или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие информацию ограниченного распространения, оставлять не запертыми после окончания рабочего дня сейфы (шкафы) и служебные помещения.

2.5.8. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении, которые могут привести к ознакомлению с информацией ограниченного распространения посторонних лиц. Об обнаружении такого рода ошибок ставить в известность администратора безопасности.

2.5.9. Производить перемещения технических средств АС без согласования с администратором безопасности.

2.5.10. Вскрывать корпуса технических средств АС и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором безопасности и без оформления соответствующего акта.

2.5.11. Подключать к АС нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

2.5.12. Осуществлять ввод пароля в присутствии посторонних лиц.

2.5.13. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АС.

2.5.14. Использовать информацию ограниченного распространения для подготовки открытых публикаций, докладов, научных работ и т.д.;

2.5.15. Сообщать устно или письменно кому бы то ни было информацию ограниченного распространения, если это не вызвано служебной необходимостью.

## 3. Ответственность

3.1. Сотрудник (работник) несет ответственность за соблюдение требований настоящей Инструкции, а также других документов в области защиты информации.

3.2. За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, сотрудники могут быть привлечены к дисциплинарной или иной, предусмотренной действующим законодательством ответственности.