ПРИЛОЖЕНИЕ 7
к распоряжению администрации
Белоярского района
от __ _____ 2016 года № ___

ИНСТРУКЦИЯ

по эксплуатации средств защиты информации объекта вычислительной техники

I. Общие положения

1.1. Данная инструкция регламентирует порядок эксплуатации средств защиты информации в администрации Белоярского района.

1.2. Данные требования обязательны для всех органов администрации Белоярского района, работающих со средствами защиты информации.

II. Термины и определения

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Антивирусная защита** – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

2.3. **Антивирусный программный продукт** – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

2.4. **Защита информации** – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.6. **Информация** – сведения (сообщения, данные) независимо от формы их представления *(ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.7. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.9. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

III. Общие положения

3.1. Ввод в эксплуатацию средств защиты информации проводится в соответствии с формуляром и другими эксплуатационными документами.

3.2. Перед эксплуатацией средств защиты информации необходимо внимательно ознакомиться с эксплуатационной и технической документацией (формуляр, правила работы, руководство пользователя и др.) входящий в комплект со средствами защиты информации.

3.3. Пользователи ИСПДн, эксплуатирующие средства защиты информации обязаны:

3.3.1. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

3.3.2. знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее – АРМ).

3.3.3. во всех сложных ситуациях обращаться к администратору безопасности.

3.3.4. ежедневно, в начале работы, производить на рабочем месте запуск антивирусного программного обеспечения (далее – ПО), не допускать блокирования или выключения антивирусного средства в процессе работы. Пользователь не должен вносить изменения в конфигурацию установленного администратором безопасности антивирусного ПО.

3.3.5. в обязательном порядке проводить антивирусную проверку съемных носителей информации.

3.3.6. немедленно вызывать администратора безопасности ИСПДн и поставить в известность руководителя органа администрации Белоярского района при обнаружении:

1) нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

2) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации средств защиты информации, а также в других программных или аппаратных средствах АРМ;

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

3.4. Всем сотрудникам администрации Белоярского района, являющимся пользователями ИСПДн, категорически ЗАПРЕЩАЕТСЯ:

3.4.1. использовать компоненты программного и аппаратного обеспечения средств защиты информации ИСПДн администрации Белоярского района в неслужебных целях;

3.4.2. самовольно вносить какие-либо изменения в конфигурацию средств защиты информации, АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных или администратором безопасности;

3.4.3. привлекать третьих лиц к работам по установке и настройке средств защиты информации, системного ПО, замене комплектующих, входящих в состав системного блока, любые виды работ по системному, сетевому администрированию, администрированию баз данных, а также администрированию систем телекоммуникаций и защиты.

3.4.4. оставлять без присмотра своё АРМ, не активизировав блокировки доступа или оставлять своё АРМ включенным по окончании работы;

3.4.5. оставлять без присмотра ключевые носители;

3.4.6. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

3.4.7. Пользователи ИСПДн обязаны исполнять все обязанности, возложенные на него требованиями настоящей инструкции.

3.5. Администратор безопасности ИСПДн обязан:

3.5.1. Устанавливать и осуществлять настройку средств защиты информации в рамках компетенции;

3.5.2. Устанавливать и обновлять версии антивирусного программного обеспечения. При необходимости осуществлять проверку памяти на наличие вирусов, производит лечение или удаление зараженных файлов;

3.5.3. Хранить дистрибутивы программного обеспечения, установленного в ИСПДн, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц;

3.5.4. Заниматься обслуживанием установленных средств криптографической защиты информации (в том числе персональных данных);

3.5.5. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

IV. Ответственность

4.1. Сотрудники администрации Белоярского района, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

4.2. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) администрации Белоярского района, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник администрации Белоярского района, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба администрации Белоярского района (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

4.3. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

4.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

4.5. Глава администрации Белоярского района администрации Белоярского района за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение: Лист ознакомления с «Инструкцией по эксплуатации средств защиты информации объекта вычислительной техники» на 1 л. в 1 экз.

Приложение
к инструкции по эксплуатации
средств защиты информации
объекта вычислительной техники

Лист ознакомления с
«Инструкцией по эксплуатации средств защиты информации
объекта вычислительной техники»

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом
1	2	3	4