

Конфиденциально
(из здания не выносить)
Экз. № 1

УТВЕРЖДАЮ

Генеральный директор
ООО «УК Вахитовского
района»



2014 г.

ИНСТРУКЦИЯ

пользователей по безопасной обработке персональных данных на объектах вычислительной техники (ОВТ) ООО «УК Вахитовского района»

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование принадлежат ООО «УК Вахитовского района» и предоставляются работникам для осуществления ими их должностных обязанностей.

АРМ, имеющие подключение к ЛВС и не имеющие подключение к ЛВС; серверы, ПО, оборудование ЛВС, коммуникационное оборудование, пользователи - образуют систему Объекта информатизации (ОИ).

АРМ - автоматизированное рабочее место;

ПО - программное обеспечение;

ЛВС - локально-вычислительная сеть;

ОИ - объект информатизации;

ОВТ - объект вычислительной техники (составная часть ОИ);

НСД - несанкционированный доступ;

СЗИ - система защиты информации;

НИ - носители информации;

АИБ - администратор информационной безопасности.

Конфиденциальная информация, в том числе персональные данные - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации; характер сведений, обуславливающий их сбор, обработку и распространение на условиях соответствующего правового режима. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ «О персональных данных».

1 Общие положения

1.1 Настоящая Инструкция разработана с целью приведения в соответствие с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и исполнения законодательных требований при обработке персональных данных в ООО «УК Вахитовского района» и является руководством для пользователя по работе с персональными данными и компьютерами сети ООО «УК Вахитовского района».

1.2 Целью настоящей Инструкции является регулирование работы пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, более эффективного использования сетевых ресурсов и уменьшения риска умышленного или неумышленного нарушения порядка работы с персональными данными.

1.3 Пользователь ОВТ - лицо, производящее обработку персональных данных на данном объекте ВТ, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.4 Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ОВТ, несет персональную ответственность за свои действия, повлекшие причинение вреда субъекту персональных данных, обрабатываемых в ООО «УК Вахитовского района».

2 Обязанности пользователя ОВТ

2.1 Выполнять на АРМ только те процедуры, которые определены для них в «Регламенте разграничения прав доступа» к информационным (программным) ресурсам объектов вычислительной техники ООО «УК Вахитовского района».

2.2 Знать и соблюдать установленные требования по обработке персональных данных, учету, хранению и пересылке носителей информации, а также руководящих и организационно-распорядительных документов на данных ОВТ.

2.3 Пользователи перед началом обработки на АРМ файлов, хранящихся на съемных носителях информации, должны осуществить проверку файлов на наличие компьютерных вирусов в соответствии с Инструкцией по антивирусному контролю.

2.4 Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них

информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.5 Обеспечивать беспрепятственный доступ АИБ к своему компьютеру.

2.6 Выполнять предписания АИБ, направленные на обеспечение безопасности объекта информатизации.

2.7 Соблюдать установленный порядок разграничения доступа к информационным ресурсам.

2.8 Немедленно ставить в известность АИБ обо всех фактах и попытках НСД к обрабатываемой на АРМ информации или об ее исчезновении (искажении).

2.9 В случае увольнения работник обязан без напоминания со стороны руководства ООО «УК Вахитовского района» вернуть все документы и материалы, относящиеся к деятельности ООО «УК Вахитовского района». В том числе: отчеты, инструкции, переписку, списки работников, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности ООО «УК Вахитовского района», полученные в течение срока работы.

2.10 При работе с информацией, содержащей крипто ключи:

2.10.1 Секретные ключи электронно-цифровых подписей и шифрования (**дискеты, диски, флэш-накопители, идентификаторы типа ключа i-Button** **содержащие ключевую информацию**) должны храниться в сейфах под ответственностью лиц, на то уполномоченных. Доступ не уполномоченных лиц к носителям секретных ключей и шифрования должен быть исключен.

2.10.2 Крипто ключи должны выниматься из сейфа исключительно в рабочее время. Все остальное время должны храниться в сейфе.

2.10.3 Работник, приступающий к работе, должен проверить целостность пломб и печатей на сейфе и убедиться, что крипто ключи находятся на месте.

2.10.4 В случае круглосуточной работы пункта, работник, приступающий к работе должен убедиться, что ключи находятся на месте и не повреждены.

2.10.5 Пользователь не должен передавать ключи кому-либо. В случае компрометации ключевой информации, ответственность возлагается на пользователя.

2.10.6 Категорически запрещается:

- снимать несанкционированные копии с носителей информации;
- знакомить с содержанием электронной информации лиц, не допущенных к этому;
- выводить секретные ключи на дисплей компьютера или принтер;
- записывать на носитель секретных ключей и шифрования постороннюю информацию;
- выносить из помещения цифровые носители с ключевой

информацией;

- озвучивать вслух в разговоре с работниками или в разговоре по телефону логины и пароли.

2.10.7 При компрометации секретных ключей шифрования и прочей электронной информации принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры по смене ключей шифрования и паролей. По факту компрометации организуется служебное расследование, результаты которого отражаются в акте и доводятся до сведения руководства ООО «УК Вахитовского района». В акте указываются рекомендации по локализации последствий компрометации, наказанию виновных и по предотвращению подобных случаев.

3 Пользователям ОВТ запрещается

3.1 Записывать и хранить информацию на неучтенных носителях информации.

3.2 Оставлять во время работы магнитные НИ (или объекты ВТ с НИ) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации.

3.3 Отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на данных АРМ; производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств.

3.4 Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

3.5 Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации.

3.6 Сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам АРМ.

3.7 Работать на АРМ при обнаружении каких-либо неисправностей.

3.8 Хранить НИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей.

3.9 Хранить на учтенных НИ программы и данные, не относящиеся к рабочей информации.

3.10 Осуществлять электропитание и заземление АРМ от штатных сетей электропитания и заземления.

3.11 Привлекать посторонних лиц для производства ремонта АРМ без согласования с Администратором информационной безопасности.

3.12 Использовать программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с Администратором информационной безопасности.

3.13 Повреждать, уничтожать или фальсифицировать информацию.

3.14 Вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование без ведома АИБ, изменять настройки BIOS, а также производить любые действия, связанные с изменением текущей конфигурации системы, самовольно подключать компьютер к сети.

3.15 Передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

3.16 Использовать иные формы доступа к сети Интернет, за исключением разрешенных Администратором информационной безопасности.

3.17 Закрывать доступ к информации паролями без согласования с АИБ.

4 Организация парольной защиты при работе на объектах информатизации

4.1 Личные пароли доступа к объекту информатизации, системе защиты от НСД, выдаются пользователям Администратором информационной безопасности, при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 8-ми буквенно-цифровых символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля, обязательно должны присутствовать буквы

в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

4.2 Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

- своевременно сообщать Администратору информационной безопасности обо всех внештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

4.3 При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;
- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

5 Порядок применения парольной защиты

5.1 Полная плановая смена паролей на ОВТ проводится один раз в 3 месяца.

5.2 Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя ОВТ должна производиться в следующих случаях:

- в случае подозрения на дискредитацию пароля;

- по окончании срока действия;

- в случае прекращения полномочий (увольнение, переход на другую работу внутри ООО «УК Вахитовского района») пользователя после окончания последнего сеанса работы данного с системой;

- по указанию Администратора информационной безопасности.

5.3 Для предотвращения доступа к персональным данным, находящимся в ПЭВМ, минуя ввод пароля, пользователь во время перерыва в работе обязан осуществить блокирование системы, например, нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню, или выключить ПЭВМ.

Порядок применения (смены) паролей при работе на ПЭВМ, оборудованных системой защиты информации от НСД, приведен в эксплуатационной документации на СЗИ.

6 Технология обработки персональных данных

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование,

удаление, уничтожение персональных данных.

6.1 При первичном допуске к работе на АРМ пользователь должен ознакомиться с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, получить персональный идентификатор и личный текущий пароль у Администратора информационной безопасности.

6.2 Пользователь включает компьютер, визуально убеждается в целостности пломб, исправности и нормальном функционировании АРМ.

6.3 В процессе работы пользователь создает файлы и массивы информации на АРМ с применением операционных систем Windows.

6.4 При необходимости вывод персональных данных из АРМ осуществляется следующим образом:

- копированием на учетные носители;
- на печатающее устройство (принтер).

7 Ответственность

7.1 Пользователь по безопасной обработке персональных данных на ОВТ отвечает за информацию, хранящуюся на его АРМ и правильную эксплуатацию вверенного ему АРМ.

7.2 Пользователь несет личную ответственность за весь информационный обмен между его АРМ и другими компьютерами ЛВС и за ее пределами.

7.3 За нарушение настоящей Инструкции пользователь может быть отстранен от работы с АРМ.

7.4 Нарушение данной Инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом конфиденциальной информации, нарушение работы АРМ пользователей, системы или ЛВС, может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством.