РД-04	Инструкция по пользованию информационной системой персональных данных	

УТВЕРЖДАЮ

Начальник ОГБУ
«Костромская городская станция
по борьбе с болезнями животных»

_____С.С. Петров

« 03 » 09 2014г.

ИНСТРУКЦИЯ
по пользованию информационной системой персональных данных
в ОГБУ «Костромская городская станция по борьбе с болезнями животных»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция определяет основные принципы безопасного использования информационной системы сотрудниками ОГБУ «Костромская городская станция по борьбе с болезнями животных» в соответствии с требованиями Федеральных законов от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. ОСНОВНЫЕ ПОНЯТИЯ

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

Информационные ресурсы – документы и массивы документов в информационных системах.

Пользователь – сотрудник, использующий для своих должностных обязанностей средства электронной вычислительной техники.

Автоматизированное рабочее место пользователя (АРМ) – персональный компьютер с предустановленным программным обеспечением.

Персональный компьютер (ПК) — компьютер, предназначенный для эксплуатации одним пользователем, то есть для личного использования.

3. ОБЩИЕ ПРАВИЛА РАБОТЫ НА АРМ

Для исполнения служебных обязанностей, Пользователю на период работы в ОГБУ «Костромская городская станция по борьбе с болезнями животных»

предоставляется автоматизированное рабочее место. В процессе эксплуатации ПК Пользователям запрещается:

3.1. Открывать корпус системного блока и вносить изменения в конфигурацию ПК;

3.2. Без получения санкции руководителя изменять настройки программного обеспечения и параметры доступа к информационным ресурсам;

3.3. Отключать антивирусное программное обеспечение, а также предусмотренные средства защиты;

3.4. Подключать к ПК неучтенные внешние запоминающие устройства (активное сетевое оборудование, незарегистрированные компьютеры и т.д.), если это не связано с исполнением должностных обязанностей сотрудника;

3.5. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты для организации несанкционированного доступа к информационным ресурсам компании. При обнаружении такого рода ошибок необходимо информировать своего непосредственного руководителя обо всех фактах нарушения данной Инструкции.

3.6. Осуществлять действия направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам информационной сети и перехват информации, циркулирующей в ИС;

3.7. Оставлять переносные компьютеры и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже. При наличии риска утраты ПК и (или) средств хранения информации, необходимо принять меры по его минимизации (например, убирать переносной компьютер на обеденный перерыв и после завершения рабочего дня в закрывающийся на ключ шкаф, не оставлять незакрытым помещение, в котором находится оборудование информационной системы, использовать замки для переносных компьютеров);

3.8. Осуществлять обработку конфиденциальной информации на ПК, не оснащенном принятыми в компании средствами защиты информации, а также в присутствии лиц, не имеющих права доступа к данной информации, если при этом указанные лица могут ознакомиться с обрабатываемой информацией;

3.9. Записывать и хранить конфиденциальную информацию на неучтённых носителях информации (Flash-карта, CD-диск, носимый HDD и т.п), а также оставлять без личного присмотра на рабочем месте или где бы то ни было носители информации и распечатки, содержащие подобную информацию;

3.10. Допускать к работе на ПК лиц, не имеющих прав доступа к информационным ресурсам.

3.11. Оставляя рабочее место, даже на короткое время, Пользователь обязан заблокировать экран своего монитора.

3.12. По окончании рабочего времени при отсутствии служебной необходимости обесточивать ПК и другую оргтехнику во избежание её выхода из строя и в целях обеспечения противопожарной безопасности.

3.13. Доступ к информационным ресурсам, хранящимся на жестком диске ПК Пользователя, должен быть защищен паролем.

3.14. Пользователи обязаны обеспечивать безопасное хранение пароля, исключающее возможность его утери или разглашения.

3.15. Срок использования пароля составляет не более 90 дней. При смене пароля новое значение должно отличаться от предыдущего не менее чем в трёх-четырёх позициях.

3.16. В случае подозрения на компрометацию пароля доступа необходимо немедленно изменить пароль и проинформировать об этом своего непосредственного руководителя.

3.17. Пользователь обязан создавать пароль в соответствии со следующими требованиями:

- длина пароля должна быть не менее 6 символов;
- пароль должен состоять из строчных и прописных букв, а также небуквенных символов (т.е. цифр, знаков пунктуации, специальных символов);
- пароль не должен быть легко угадываемым (не должен включать повторяющуюся последовательность каких-либо символов (например, "55555555", "аааааааа", “12345678”, “qwerty”, “йцукен” и т.п.), пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, наименования, клички домашних животных, даты рождения и т.д.) и общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

3.18. При использовании телекоммуникационных возможностей сети Интернет пользователи обязаны выполнять следующие требования:

- использовать ресурсы Интернет только для выполнения своих служебных обязанностей;
- не посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтичного характера, а также использовать доступ к социальным сетям Интернет и развлекательным сайтам;
- не размещать в сети Интернет информацию о компании и её сотрудниках, если это не связано с выполнением служебных обязанностей;
- не использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом;

3.19. При работе с электронной почтой пользователи должны соблюдать следующие требования:

- запрещается использовать возможности электронной почты для отправки сообщений противозаконного, экстремистского или враждебного характера, а также содержащего в себе информацию неэтичного содержания;
- при получении электронных сообщений из незнакомого источника и/или сомнительного содержания не следует открывать файлы, вложенные в сообщение, так как они с большой долей вероятности могут содержать вирусы. Такие сообщения необходимо удалять;
- не следует отвечать на подозрительные письма и, тем более, сообщать любые данные о себе, о компании и её сотрудниках.

1. ПОРЯДОК РАБОТЫ С ИНФОРМАЦИОННОЙ СИСТЕМОЙ

4.1. Пользователь при работе с программными и техническими средствами, входящими в состав информационной системы, обязан строго выполнять установленные правила и несёт персональную ответственность за их несоблюдение.

4.2. Информационные ресурсы ОГБУ «Костромская городская станция по борьбе с болезнями животных» считаются собственностью организации, если иное не оговорено

соответствующими соглашениями. Организация оставляет за собой право протоколировать и контролировать действия работников при обработке информации в информационной системе.

4.3. Пользователи не имеют права предпринимать попыток получения доступа к информационным ресурсам, не получив официального разрешения на доступ к ним.

4.4. Пользователи не должны разглашать сведения о содержании информации, ставшей известной им в ходе выполнения должностных обязанностей, а также о процедурах и технической реализации защиты информации, принятых в организации.

4.5. Пользователи должны выполнять требования общих правил работы на АРМ и информировать своего непосредственного руководителя обо всех фактах нарушения данной Инструкции.

4.6. В целях повышения эффективности служебной деятельности для обмена открытыми информационными ресурсами (обновления программных продуктов, инструкции, правила и т.п.) могут использоваться съёмные материальные носители информации (Flash-карты, переносные жесткие диски, иные устройства записи и чтения), зарегистрированные и находящиеся на учете в ОГБУ «Костромская городская станция по борьбе с болезнями животных».

4.7. Выдача сотрудникам и учёт материальных носителей информации осуществляется ответственным за организацию работы по защите персональных данных, по Журналу учёта съёмных носителей.

2. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОРЯДКА

5.1. Ответственность за выполнение требований настоящей Инструкции возлагается на всех работников, являющихся пользователями информационной системы ОГБУ «Костромская городская станция по борьбе с болезнями животных».

5.2. Работник, нарушивший требования данной Инструкции, может быть подвергнут дисциплинарному наказанию в соответствии с законодательством РФ и трудовым договором.

Приложение: Схема распределенной локальной вычислительной сети ОГБУ «Костромская городская станция по борьбе с болезнями животных», на 1 листе.