	ГОУВПО «Марийский государственный университет»
	Инструкция СМК
И СМК 6.2.2.02-2011	***Инструкция пользователя при обработке персональных данных на объектах вычислительной техники. Автоматизированное рабочее место на базе автономной ПЭВМ***

УТВЕРЖДАЮ
Ректор Марийского государственного университета
_____В.И.Макаров
«__» _____ 2011г

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция пользователя при обработке персональных данных на объектах вычислительной техники. Автоматизированное рабочее место на базе автономной ПЭВМ

И СМК 6.2.2.02 - 2011

Версия 1.0 Изменение 0

СОГЛАСОВАНО
Первый проректор – проректор по учебной работе,
представитель руководства по качеству
_____ В.А. Иванов
«23» мая 2011г

Йошкар – Ола 2011

Предисловие

1 РАЗРАБОТАНА Информационно-вычислительным центром ГОУВПО «Марийского государственного университета».

Руководитель разработки: Г.И. Миронов, проректор по учебной работе.

Разработчик: Курандин Л.В., начальник ИВЦ.

2 Утверждена и введена в действие _____ от «25» мая 2011г

Дата введения «25» мая 2011г

3 Введена впервые.

Содержание

1 Назначение и область применения

1.1 Настоящая инструкция является нормативным документом и устанавливает единый порядок работы пользователя при обработке персональных данных на объектах вычислительной техники.

1.2 Требования инструкции обязательны для применения во всех подразделениях университета, непосредственно связанных с обработкой персональных данных на объектах вычислительной техники.

1.3 Владельцем настоящей инструкции является проректор по учебной работе.

2 Нормативные ссылки

Настоящая инструкция разработана в соответствии с требованиями следующих нормативных документов:

ПРИКАЗ ФСТЭК от 5 февраля 2010 г. N 58 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О МЕТОДАХ И СПОСОБАХ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ О персональных данных;

Трудовой кодекс РФ;

Иные федеральные нормативно-правовые акты в области защиты персональных данных и информации;

Положение «О защите персональных данных ГОУВПО «Марийский государственный университет»;

Приказы ректора (в области работы с персональными данными);

ГОСТ Р ИСО 9000-2001 СМК. Основные положения и словарь;

ГОСТ Р ИСО 9001-2008 СМК. Требования;

ДП СМК 4.2.3.01 Управление документацией.

3 Термины, определения, обозначения и сокращения

Администратор вычислительной сети (также называемый *сетевой администратор*, англ. *network administrator*) — сотрудник, отвечающий за работу компьютерной сети предприятия в штатном режиме.

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Идентификатор - логин и пароль пользователя.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Компью́терный ви́рус — разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.

Конфигурация – в области информационных и компьютерных систем - это определенный набор комплектующих, исходя из их предназначения, номера и основных характеристик. Зачастую конфигурация означает выбор аппаратного и программного обеспечения, прошивок и сопроводительной документации. Конфигурация влияет на функционирование и производительность компьютера.

Конфиденциальность персональных данных - обязательное для соблюдения Университетом или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Конфиденциальность — необходимость предотвращения утечки (разглашения) какой-либо информации.

Несанкционированный доступ к информации — доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации. Так же иногда несанкционированным доступом называют получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

Носи́тель информа́ции (информацио́нный носи́тель) — любой материальный объект или среда, содержащий (несущий) информацию, способный достаточно длительное время сохранять в своей структуре занесённую в/на него информацию — камень, дерево, бумага, металл, пластмассы, кремний (и др. виды полупроводников), лента с намагниченным слоем (в бобинах и кассетах), пластик со специальными свойствами (для оптической записи информации — CD, DVD и т. д.), ЭМИ (электромагнитное излучение), и т. д. и т. п.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Персона́льные да́нные (или **личные данные**) — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь — лицо или организация которое использует действующую систему для выполнения конкретной функции.

Прикладная программа или **приложение** — программа, предназначенная для выполнения определенных пользовательских задач и рассчитанная на непосредственное взаимодействие с пользователем. В большинстве операционных систем прикладные программы не могут обращаться к ресурсам компьютера напрямую, а взаимодействуют с оборудованием и проч. посредством операционной системы.

Программное обеспечение — совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ. Также — совокупность программ, процедур и правил, а также документации, относящихся к функционированию системы обработки данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Систе́мное програ́ммное обеспече́ние — это комплекс программ, которые обеспечивают эффективное управление компонентами вычислительной системы, такими как процессор, оперативная память, каналы ввода-вывода, сетевое оборудование, выступая как «межслойный интерфейс» с одной стороны которого аппаратура, а с другой приложения пользователя. В отличие от прикладного программного обеспечения, системное не решает конкретные прикладные задачи, а лишь обеспечивает работу других программ, управляет аппаратными ресурсами вычислительной системы и т.д.

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Файл — наименование (имя) совокупности данных, в т. ч. документа на машиночитаемом носителе (например, дискете), основной элемент хранения данных в компьютере, позволяющий отличать эту совокупность данных от других, находить, изменять, удалять или выполнять с ней другие операции.

Электронный ключ (также *аппаратный ключ*, иногда *донгл* от англ. *dongle*) — аппаратное средство, предназначенное для защиты программного обеспечения и данных от копирования, нелегального использования и несанкционированного распространения.

Обозначения

ГОСТ Р	- национальный стандарт Российской Федерации
ГОУВПО	-Государственное образовательное учреждение высшего профессионального образования
ИВЦ	- информационно-вычислительный центр
ИСО	- международная организация по стандартизации
МарГУ	- Марийский государственный университет
ПЭВМ	-персональные электронно-вычислительные машины
РК	- Руководство по качеству
СМК	- система менеджмента качества
ФЗ	- федеральный закон
И	- инструкция
ЮО	- юридический отдел
УМУ	- учебно-методическое управление

4 Описание процедуры

4.1 Общие положения

4.1.1 Предмет Инструкции определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) ГОУВПО «Марийский государственный университет».

4.1.2 Общие требования к пользователю:

- пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ;
- пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

4.2 Обязанности пользователя

4.2.1 Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции.

4.2.2 При обработке персональных данных, ПЭВМ должна быть отключена от сетей общего пользования и сети Интернет, до стирания остаточной информации с жесткого диска ПЭВМ.

4.2.3 При работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, сотрудников, не допущенных к обрабатываемой информации, или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами.

4.2.4 Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при их обработке.

4.2.5 После окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ.

4.2.6 Оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой с использованием ПЭВМ.

4.2.7 Не устанавливать на используемые для обработки персональных данных ПЭВМ посторонних программных средств.

4.2.8 Знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий.

4.2.9 Знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

4.2.10 Помнить личные пароли, персональные идентификаторы, не оставлять без присмотра, не записывать свои пароли в очевидных местах: внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры, на отдельных листах бумаги т.д. Хранить пароли допускается в запирающемся ящике стола или сейфе.

4.2.11 Знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов.

4.2.12 При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

4.2.13 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание

файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

4.2.14 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

4.3 Пользователю запрещается:

4.3.1 Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации.

4.3.2 Удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности.

4.3.3 Самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ.

4.3.4 Самостоятельно устанавливать и или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей.

4.3.5 Осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ.

4.3.6 Сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ.

4.3.7 Отключать (блокировать) средства защиты информации.

4.3.8 Производить какие-либо изменения в подключении и размещении технических средств.

4.3.9 Производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

4.3.10 Оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4.3.11 Пересылка персональных данных по общедоступным сетям связи, в том числе Интернет, категорически запрещается.

4.4 Правила пользователя ПЭВМ

4.4.1 Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий

4.4.2 Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

4.5 Ответственность пользователей ПЭВМ

Пользователь ПЭВМ несёт ответственность

4.5 1 За ненадлежащее выполнение требований настоящей инструкции.

4.5.2 За несоблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов.

4.5.3 За сохранность и работоспособное состояние средств вычислительной техники ПЭВМ, сохранность персональных данных.

4.5.4 При нарушениях правил, связанных с обработкой персональных данных, пользователь несет ответственность, установленную действующим законодательством Российской Федерации и нормативными актами ГОУВПО «Марийский государственный университет».

5 Ответственность и полномочия

Ответственным за организацию разработки и введение инструкции в действие является проректор по учебной работе.

Лист согласования

Инструкцию разработал:

Начальник ИВЦ — 12.05.11 — Л.В. Курандин

Согласовано:

Проректор по учебной работе — 19.05.11 — Г.И. Миронов

Гл.бухгалтер, начальник УБУФиП — 19.05.11 — Н.В. Чеснокова

Начальник ЮО — 17.05.11 — Е.В. Лапина

Начальник УМУ — 20.05.11 — В.Н. Максимов

Начальник управления кадрами — 18.05.11 — Е.В. Маркова

Экспертиза проведена:

Начальник ОМКО — 20.05.2011 г. — Р.В. Босович

Лист регистрации изменений

Номер изменения	Номера листов			Основание для внесения изменений	Подпись	Расшифровка подписи	Дата	Дата введения изменения
	замененных	новых	аннулированных					