	ГОУВПО «Марийский государственный университет»
	Инструкция СМК
И СМК 6.2.2.03-2011	*Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные, с использованием средств автоматизации*

УТВЕРЖДАЮ

Ректор Марийского государственного университета

_____В.И.Макаров

«23» мая _____2011г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные, с использованием средств автоматизации

И СМК 6.2.2.03 - 2011

Версия 1.0 Изменение О

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»_____2011г

Дата введения «25»_____2011г

3 Введена в первые.

Содержание

1 Назначение и область применения

1.1 Настоящая инструкция является нормативным документом, устанавливающим единый порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации.

1.2 Требования инструкции обязательны для применения во всех подразделениях университета, непосредственно связанных с обеспечением конфиденциальности при обращении с информацией, содержащей персональные данные.

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 и обозначения

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

Документ - материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования.

Идентификатор - логин и пароль пользователя.

Инсталляция (установка) — процесс установки программного обеспечения на компьютер конечного пользователя.

Информационная система - взаимосвязанная совокупность средств, методов и персонала, используемая для сохранения, обработки и выдачи информации с целью решения конкретной задачи.

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.

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;

Компьютерный вирус — 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.

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.

Носитель информации (информационный носитель) — 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.

Персональные данные (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 клюя,* иногда *донгл* от англ. *dongle*) — аппаратное средство, предназначенное для защиты программного обеспечения и данных от копирования, нелегального использования и несанкционированного распространения.

Обозначения:

В настоящем документе приняты следующие 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

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

4.2 Общие требования по защите персональных данных в автоматизированных системах

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

4.3 Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

4.3.1 Организация учета носителей персональных данных.

Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу съемных носителей персональных данных по прилагаемой форме (Приложение А) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Сотрудники структурных подразделений получают учтенный съемный носитель от уполномоченного сотрудника структурного подразделения для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.3.2 Правила использования съемных носителей персональных данных.

Запрещается:

• хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

• выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.3.3 Порядок действий при утрате или уничтожении съемных носителей персональных данных.

О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией».

По результатам уничтожения носителей составляется акт по прилагаемой форме (Приложение Б).

5 Ответственность и полномочия

Ответственным за обеспечение конфиденциальности при обращении с информацией, содержащей персональные данные является проректор по учебной работе.

Приложение А

ЖУРНАЛ

учета съемных носителей персональных данных

_____

наименование структурного подразделения

Начат «____» _____200_ г.

Окончен «____» _____ 200_ г.

На _____листах

_____ _____

Должность и ФИО ответственного за хранение Подпись

№ п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*
1						
2						
3						
4						
5						

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение Б

«УТВЕРЖДАЮ»

_____ _____

«_____»_____20 г

АКТ

уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом _____ от _____

№ _____ в составе:

_____

(должности, ФИО)

_____

(должности, ФИО)

_____

(должности, ФИО)

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
	2	3	4

Всего съемных носителей_____

(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены

_____

путем (разрезания, демонтажа и т.п.) ,

_____

измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья

_____ _____

(наименование предприятия) (Дата)

Председатель комиссии Подпись Дата

Члены комиссии

(ФИО) Подпись Дата

Лист согласования

Инструкцию разработал:

Начальник ИВЦ — 12.05.11 — Л.В. Курандин

Согласовано:

Проректор по учебной работе — 18.05.11 — 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 — 20.05.2011г — Р.В. Босович

Лист регистрации изменений

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