Общество с ограниченной ответственностью «Дента-Л»
ООО «Дента-Л»

ПРИКАЗ

«09» января 2017 г. № 26

г. Ставрополь

об утверждении документов
по использованию средств
защиты информации

Во исполнение требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Регламент процедур по установке и использованию программного обеспечения в учреждении; Требования к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных; Инструкцию по организации парольной защиты; Инструкцию по организации антивирусной защиты; Инструкцию по учету машинных носителей и мобильных технических средств, предназначенных для работы; Инструкцию пользователя по обеспечению безопасности при возникновении нештатных ситуаций в информационных системах; Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации; Инструкцию о порядке проведения разбирательств по фактам несоблюдения условий хранения носителей персональных данных; Инструкцию по обеспечению защиты конфиденциальной информации, обрабатываемой в локальной вычислительной сети согласно приложениям.
2. Ответственному за организацию работы по обработке и защите персональных данных – заместителю генерального директора по медицинской части Савченко Ю. А. ознакомить под роспись работников с настоящим приказом.
3. Контроль за исполнением настоящего приказа оставляю за собой.
4. Приказ вступает в силу со дня его подписания.

Руководитель организации **Генеральный директор** _____ **А. И. Латиган**
(должность) (личная подпись) (расшифровка подписи)

С приказом (распоряжением) работник ознакомлен _____ 09 01 2017 г.
(личная подпись)

Приложение № 1
к приказу от «09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

РЕГЛАМЕНТ

процедур по установке и использованию программного обеспечения в учреждении

1. Общая часть

1.1. Настоящее Положение разработано в соответствии с Гражданским кодексом РФ, ГОСТ Р ИСО/МЭК 17799-2005, и другими нормативными правовыми актами, и устанавливает правила использования программного обеспечения вычислительной техники в ООО «Дента-Л» (далее Организация), а также определяет права и обязанности работников в процессе эксплуатации всех видов программного обеспечения в Организации.

2. Основные термины, сокращения и определения

- **АРМ** – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО), для выполнения определенной производственной задачи.
- **АС** – автоматизированная система Организации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.
- **ИТ** – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации Организации с использованием средств компьютерной и другой техники.
- **Лицензионное Соглашение** – документ, регламентирующий передаваемые конечному пользователю права на использование ПО, формулируется правообладателем.
- **Паспорт ПК (паспорт АРМ)** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
- **ПК** – персональный компьютер – комплекс вычислительной техники с установленным системным ПО, используется одним или несколькими пользователями АС в производственных целях.

- **ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
- **ПО прикладное** – офисное программное обеспечение (в том числе, разработанное специалистами Организации); информационно-справочные системы; АС для решения производственных, хозяйственных и управленческих задач Организации; системы проектирования и управления.
- **ПО системное** – операционные системы, средства антивирусной защиты, средства создания резервных копий, драйверы устройств, административные утилиты, средства организации сетевых сервисов.
- **ПО специализированное** – ПО систем управления технологическими процессами на производстве, ПО системного администрирования/управления ресурсами вычислительных сетей.
- **Правообладатель** – автор, его наследник, а также любое физическое или юридическое лицо, которое обладает исключительным правом на программу для ЭВМ или базу данных в силу закона или договора.
- **Перечень** – документ «Перечень программного обеспечения, разрешенного для использования на компьютерах ООО «Дента-Л». Содержит перечень коммерческого ПО, разрешенного к использованию в Организации в текущем году. Утверждается один раз в год приказом Руководителя Организации

3. Права и обязанности пользователя программного обеспечения

3.1 Пользователь допускается к использованию в работе компьютеров и установленного на них ПО в порядке и объеме, не противоречащем законодательству Российской Федерации и локальным актам.

3.2 Пользователю запрещается:

входить в операционную систему под учетной записью администратора;

устанавливать самостоятельно ПО;

вносить изменения в установленное ПО (включая обновление версии продукта);

удалять ПО.

3.3 Пользователь, нарушивший пункт 3.2 настоящего регламента, несет ответственность, установленную действующим законодательством Российской Федерации и локальными актами.

4. Права и обязанности ответственного за получение, распределение и установку программного обеспечения

4.1 Ответственный за получение, распределение и установку ПО оформляет служебную записку на закупку ПО с обоснованием необходимости его приобретения.

4.2 Ответственный за получение, распределение и установку ПО принимает решение:

- об установке приобретенного ПО в соответствии с условиями соответствующей лицензии;
- о внесении изменений в установленное ПО, включая обновление версии программного продукта;
- об удалении неиспользуемого или поврежденного ПО, а также ПО, использование которого может причинить вред имуществу;
- о проведении работ по восстановлению ПО из резервных копий в соответствии с документацией на используемое ПО;
- об установке или удалении свободно распространяемого ПО.

Все названные операции производятся работником, имеющими допуск к данным операциям.

4.3 Ответственный за получение, распределение и установку ПО обеспечивает условия безопасного, защищенного от доступа посторонних лиц, хранения дистрибутивов ПО и сопутствующей документации (лицензионного соглашения, лицензий, сертификатов, платежных документов, руководства пользователя и т.д.).

4.4 Ответственный за получение, распределение и установку ПО проводит ежемесячный мониторинг установленного ПО.

4.5 В случае обнаружения нелицензионного ПО, установленного пользователем, ответственный за получение, распределение и установку ПО составляет докладную на имя руководителя с указанием лица, осуществившего такую установку, выводит компьютер из эксплуатации до момента проверки данного факта комиссией. На время проведения проверки лицо, указанное в докладной записке, отстраняется от работы на компьютере.

4.8 Ответственный за получение, распределение и установку ПО несет дисциплинарную ответственность за своевременность предоставления и достоверность информации.

5. Права и обязанности специалиста, обслуживающего программное обеспечение

5.1 Специалист, обслуживающий ПО, назначается руководителем. по согласованию с ответственным за получение, распределение и установку ПО в учреждении.

5.2 Специалисту, обслуживающему ПО, в соответствии с решением ответственного за получение, распределение и установку ПО разрешается:

устанавливать ПО;

вносить изменения в установленное ПО (включая обновление версии продукта);

удалять ПО.

5.3 Специалист, обслуживающий ПО, обязан:

производить настройку устанавливаемого ПО;

контролировать исполнение требований лицензионных соглашений установленного ПО;

поддерживать ПО в работоспособном состоянии;
осуществлять еженедельный мониторинг установленного ПО;
сообщать ответственному за получение, распределение и установку ПО в подразделении о выявленных нарушениях.

5.4 Специалист, обслуживающий ПО, несет ответственность за ненадлежащее исполнение или неисполнение обязанностей, предусмотренных пунктами 5.2 и 5.3 настоящего регламента, в соответствии с действующим законодательством Российской Федерации.

6. Порядок проведения проверки по факту использованию нелицензионного программного обеспечения

6.1 Для проверки фактов, изложенных в докладной записке ответственного за получение, распределение и установку ПО приказом руководителя создается комиссия.

6.2 Комиссия в течение 3 рабочих дней проводит проверку по факту использования нелицензионного ПО или по факту неправомерного удаления, внесения изменений в лицензионное ПО. Результаты проверки оформляются актом

6.3 По результатам рассмотрения акта проверки принимаются следующие решения: о наложении дисциплинарного взыскания на лицо, в отношении которого проводилась проверка; о направлении материалов проверки в правоохранительные органы для возбуждения уголовного дела или дела об административном правонарушении в отношении лица, осуществившего неправомерные операции с ПО; о возмещении материального ущерба.

6.4 Лицо, осуществившее неправомерную установку, удаление, внесение изменений в ПО, принадлежащее несет административную, уголовную, гражданско-правовую ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 3
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ТРЕБОВАНИЯ

к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных

Настоящие Требования определяют порядок оборудования выделенных помещений и условия размещения в них технических средств (персональных компьютеров, серверов и т.п.), используемых для обработки персональных данных.

Расположение выделенных помещений и размещаемых в них технических средств должно исключать возможность бесконтрольного проникновения в эти зоны посторонних лиц и гарантировать сохранность находящихся в них конфиденциальных документов, содержащих персональные данные.

Размещение оборудования и технических средств, предназначенных для обработки персональных данных, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

Внутренняя планировка и расположение рабочих мест в выделенных помещениях должны обеспечивать исполнителям сохранность доверенных им конфиденциальных документов и сведений, содержащих персональные данные.

Допуск в выделенные помещения вспомогательного и обслуживающего персонала (уборщицы, электромонтеры, сантехники и т.д.) производится только при служебной необходимости и в сопровождении ответственного за помещение, при этом необходимо принять меры, исключающие визуальный просмотр конфиденциальных документов, содержащих персональные данные.

Приложение № 5
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ
в информационных системах персональных данных ООО «Дента-Л»

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»

1.2. С целью ограничения доступа к информационным системам (далее – ИС) ООО «Дента-Л» устанавливается единая система установки паролей на базе общего и прикладного программного обеспечения средств защиты информации.

1.3. Личные пароли должны выбираться пользователями **самостоятельно**, с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места и т. д.), а также общепринятые сокращения;
- в пароле должны присутствовать символы трех категорий - прописные,

строчные, десятичные цифры;

- запрещается выбирать пароли, которые использовались ранее.

1.4. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файл, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

1.5. Личный пароль сотрудника, допущенного к информационным ресурсам ИС, составляет его секрет и разглашению не подлежит.

1.6. Удаление учетной записи пользователя ИС в случае его увольнения должно производиться немедленно после окончания последнего сеанса работы данного пользователя.

1.7. Имя пользователя и индивидуальный пароль являются идентификатором пользователя в ИС.

1.8. При авторизации в ИС пользователь обязан ввести свое имя пользователя и набрать индивидуальный пароль, после чего он получает доступ к отведенным для него ресурсам.

1.9. С целью контроля над реализацией прав доступа пользователей к информационным ресурсам ИС должно быть организовано ведение аудита ИС с использованием встроенных механизмов операционной системы и средств защиты информации.

1.10. Действия пользователей, допущенных к информационным ресурсам, хранимым на сервере ИС, могут протоколироваться. Ответственность за уничтожение, изменение информации несет пользователь, под чьим именем операция была зарегистрирована, если в результате расследования не определено конкретное виновное лицо.

1.11. Нарушение пользователями целостности установленного программного обеспечения, а также самовольное установление программ, не предназначенных для выполнения должностных обязанностей, категорически запрещается.

2. Порядок плановой и внеплановой смены личного пароля

2.1. Плановая смена паролей должна проводиться регулярно, но не реже одного раза в 3 месяца.

2.2. Внеплановая смена любого пароля пользователя ИС производится:

- по просьбе самого пользователя;
- по требованию администратора безопасности ИС.

2.3. В случае временного прекращения полномочий пользователя ИС (болезнь, отпуск, командировка и т. п.) администратором безопасности ИС производиться блокировка учетной записи пользователя по представлению служебной записки руководителем.

2.4. Внеплановая смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администраторов безопасности ИС и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению ИС в целом, либо полномочия по управлению системой защиты информации данной ИС, а значит, кроме личного пароля, им были известны пароли других пользователей.

3. Действия при компрометации пароля

3.1. В случае компрометации личного пароля хотя бы одного пользователя ИС смена паролей производится в объеме, зависящем от полномочий владельца скомпрометированного пароля.

3.2. По всем фактам компрометации паролей проводят служебное расследование.

3.3. Каждый пользователь ИС получает свое пользовательское имя учетной записи, которое составляется администратором безопасности ИС и доводится пользователю.

3.4. Все пользователи ИС, должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, за разглашение парольной информации и сохранность информации на отведенных ему разделах сервера.

Приложение № 7
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
в информационных системах персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- - Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- - постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- - приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»

1.2. Настоящая инструкция определяет требования к организации защиты информационных систем ПДн ООО «Дента-Л» от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИС, за их выполнение.

1.3. К использованию в ООО «Дента-Л» допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.4. Установка средств антивирусного контроля на компьютерах осуществляется Администратором безопасности ИСПДн. Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль системных файлов.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (DVD (CD)-ROM, flash-накопители и т. п.).

2.3. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера.

2.4. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.6. Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании заявки начальника отдела. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором безопасности ИС на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера на автоматизированном рабочем месте (АРМ) Администратором безопасности ИС должна быть выполнена антивирусная проверка.

2.7. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в электронном журнале антивирусного средства (операционной системы).

2.8. 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.) сотрудник самостоятельно или вместе с Администратором безопасности ИС должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

2.9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего руководителя и Администратора безопасности ИС, владельца зараженных файлов, а также других сотрудников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отдельном съемном носители Администратору безопасности ИС;
- по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору безопасности ИС, в которой необходимо указать предположительный источник (отправителя, владельца и т. д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в ООО «Дента-Л» и соблюдение требований настоящей инструкции возлагается на Администратора безопасности ИС.

3.2. Периодический контроль над состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции сотрудниками ООО «Дента-Л» осуществляется Администратором безопасности ИС.

Приложение № 9
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

Инструкция
по учету машинных носителей и мобильных технических средств, предназначенных для работы

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- «Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»

1.2. Инструкция определяет порядок учета машинных носителей и мобильных технических средств предназначенных для работы в информационных системах ООО «Дента-Л».

1.3. В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства).

1.4. Под использованием носителей информации в информационных системах понимается их подключение к инфраструктуре информационной системы с целью обработки, приема, передачи информации между ресурсами информационной системы и носителями информации.

1.5. Администратором безопасности ИСПДн должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

Учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

1.6. Все находящиеся на хранении и в обращении носители конфиденциальной информации подлежат регистрации в «Журнале учета машинных носителей». Каждый носитель должен иметь уникальный учетный номер.

1.7. Журнал учета машинных носителей ведется администратором безопасности персональных данных в печатном или электронном виде.

2. Порядок работы с машинными носителями

2.1. В информационной системе запрещается использование не входящих в ее состав **(находящихся в личном использовании)** съемных машинных носителей информацию.

2.1. В информационной системе допускается использование только учтенных носителей информации и мобильных технических средств, для которых определен владелец (пользователь, организация, ответственные за соблюдение требований защиты информации).

2.2. Допуск работника к машинным носителям персональных данных определяется на основании имеющих у пользователей прав доступа и служебных обязанностей.

2.3. Работники ООО «Дента-Л» получают учтенный машинный носитель от Администратора безопасности ИСПДн на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончанию работ пользователь сдает машинный носитель для хранения Администратору безопасности ИСПДн, с проставлением соответствующий отметки в журнале учета.

2.4. При использовании сотрудниками носителей персонифицированной информации необходимо:

- соблюдать требования настоящей инструкции;
- использовать носители информации исключительно для выполнения служебных обязанностей;
- ставить в известность администратора безопасности о любых фактах нарушениям требований настоящей инструкции;
- бережно относиться к носителям информации;
- хранить съемные носители персональных данных в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

2.5. При использовании машинных носителей персональных данных запрещается:

- хранение машинных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;
- вынос машинных носителей с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.;
- использование для хранения и обработки персональных данных машинных носителей информации, не поставленных на учет в установленном порядке.

2.6. Любое взаимодействие (обработка, прием, передача информации), инициированное работниками ООО «Дента-Л» между ИС и неучтенным носителем, рассматривается как несанкционированное. Администратор безопасности ИСПДн оставляет за собой право блокировать или ограничивать использование носителей информации.

2.7. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей персонифицированной информации, проводится служебная проверка комиссией, состав которой определяется директором ООО «Дента-Л».

2.8. По факту выясненных обстоятельств составляется акт расследования инцидента и передается директору ООО «Дента-Л» для принятия мер согласно локальным внутренним нормативным актам и действующему законодательству.

2.9. Информация, хранящаяся на учтенных машинных носителях, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

2.10. При отправке или передаче персональных данных сторонней организации, на машинных носителях записываются только предназначенные адресатам данные.

2.11. Отправка персональных данных сторонней организации на машинных носителях осуществляется в порядке, установленном для документов имеющих гриф «ДСП» (для служебного пользования).

2.12. Вынос машинных носителей персональных данных для непосредственной передачи сторонней организации осуществляется только с письменного разрешения руководителя организации.

2.13. О фактах утраты или уничтожения машинных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений, немедленно ставится в известность ответственный за организацию обработки персональных данных и директор ООО «Дента-Л». О факте утраты носителя составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей.

2.14. Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей с персонифицированной информацией осуществляется комиссией, назначенной приказом руководителя. По результатам уничтожения носителей составляется акт по прилагаемой форме.

2.15. При увольнении или переводе сотрудника в другое структурное подразделение, предоставленные носители персональных данных изымаются.

2.16. Носители персональных данных, предназначенные для обработки без использования средств автоматизации, учитываются в рамках общего делопроизводства.

2.17. Сотрудники, нарушившие требования настоящей инструкции, несут ответственность в соответствии с действующим законодательством и внутренними нормативными актами.

Приложение № 11
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных».

1.2. Данная инструкция определяет порядок действий пользователя при возникновении нештатной ситуации при работе с персональными данными в информационной системе персональных данных (далее – ИС) ООО «Дента-Л» и по реагированию на нештатные ситуации, связанные с работой в ИС.

1.3. Пользователем ИС (далее – Пользователь) является сотрудник ООО «Дента-Л» , участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС согласно приказу списка лиц, которым необходим доступ к персональным данным, обрабатываемым в ИС, для выполнения своих

должностных обязанностей.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Общий порядок действий при возникновении нештатных ситуаций

2.1. В настоящем документе под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС, а так же с вероятностью потери защищаемой информации.

2.2. К нештатным ситуациям относятся следующие ситуации:

- сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, ошибки в работе программы и т. п.);
- отключение электричества;
- сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);
- выход из строя сервера;
- потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т. п.);
- обнаружен вирус;
- обнаружена утечка информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);
- взлом системы (web-сервера, файл-сервера и др.) или несанкционированный доступ;
- попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);
- компрометация ключей (утеря носителя ключевой информации (Rutoken, E-token и т. п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к

устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место, взлом учётной записи пользователя);

- компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);
- физическое повреждение ЛВС или ПЭВМ (не включается ПК, при попытке включения отображается синий или черный экраны, повреждены провода и т. п.);
- стихийное бедствие;
- иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИС и возможность потери защищаемой информации, и названные таковыми пользователем ИС или администратором безопасности ИС.

2.3. При возникновении нештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность администратора безопасности. В случае, если поставить в известность администратора не представляется возможным (администратор безопасности отсутствует на рабочем месте), пользователем, обнаружившим нештатную ситуацию, составляется служебная записка в свободной форме с описанием нештатной ситуации, и передается руководителю подразделения.

2.4. Администратор безопасности ИСПДн проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего непосредственного руководителя начальника для определения дальнейших действий. Здесь и далее – в случае отсутствия администратора безопасности, все действия и меры в отношении нештатной ситуации, описанные в настоящей инструкции, выполняет сотрудник отдела, временно назначенный начальником отдела, либо сам начальник.

2.5. По факту возникновения и устранения нештатной ситуации заносится запись в «Журнал учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах ИС ООО «Дента-Л»

2.6. При необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

3. Особенности действий при возникновении наиболее распространенных нештатных ситуаций

3.1. Сбой программного обеспечения. Администратор безопасности ИСПДн совместно с сотрудником отдела, у которого произошла нештатная ситуация, выясняют причину сбоя. Если исправить ошибку своими силами не удалось, разработчику ПО направляется информационное сообщение с сопроводительными материалами о возникшей ситуации.

3.2. Отключение электричества. Администратор безопасности ИСПДн совместно с сотрудником отдела, у которого произошла нештатная ситуация, проводят анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

3.3. Сбой в локальной вычислительной сети (ЛВС). Администратор безопасности ИСПДн проводит анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

3.4. Выход из строя сервера. Администратор безопасности ИСПДн, ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера (если есть) для обеспечения непрерывной работы ООО «Дента-Л». При необходимости производятся работы по восстановлению ПО и данных из резервных копий.

3.5. Потеря данных. При обнаружении потери данных Администратор безопасности ИСПДн проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий.

3.6. Обнаружен вирус. При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится компетентным в этой области сотрудником. Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны. После успешной

ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться «Инструкцией по организации антивирусной защиты», инструкцией по эксплуатации применяемого антивирусного ПО. После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ЭВМ ООО «Дента-Л» с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий. Проводится служебное расследование по факту появления вируса в ЭВМ (ЛВС).

3.7. Обнаружена утечка информации. При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

3.8. Взлом системы (Web-сервера, файл-сервера и др.) или несанкционированный доступ (НСД). При обнаружении взлома сервера ставится в известность Администратор безопасности ИСПДн. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянских закладок. Возможен временный переход на резервный сервер. Учитывая, что программные закладки могут быть не обнаружены антивирусным ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС ООО «Дента-Л», после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ. По факту взлома сервера проводится служебное расследование.

3.9. Попытка несанкционированного доступа (НСД). При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн. При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД (данный журнал ведется автоматизированным способом средствами защиты информации от несанкционированного доступа). По

результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

3.10. Компрометация ключей. При обнаружении утечки информации ставится в известность Администратор безопасности и начальник подразделения. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

3.11. Компрометация пароля. При обнаружении утечки информации ставится в известность Администратор безопасности. При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т.д.). При необходимости, проводится служебное расследование.

3.12. Физическое повреждение ЛВС или ПЭВМ. Ставится в известность Администратор безопасности ИСПДн. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

3.13. Стихийное бедствие. При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими поведение в чрезвычайных ситуациях, принятых в учреждении.

4. Меры против возникновения нештатных ситуаций

4.1. Администратором безопасности ИСПДн периодически, не реже 1 раза в год, должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

4.2. В общем случае, для предотвращения нештатных ситуаций необходимо четкое соблюдение требований нормативных документов Министерства и инструкций по эксплуатации оборудования и ПО.

4.3. Рекомендации по предотвращению некоторых типичных

нештатных ситуаций:

- Сбой программного обеспечения - применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на ЭВМ (проверка диска и др.).
- Отключение электричества - использовать источники бесперебойного питания на критически важных технологических участках Министерства.
- Сбой ЛВС - обеспечение бесперебойной работы ЛВС . путем применения надежных сетевых технологий и резервных систем.
- Выход из строя серверов - применять надежные программно-технические средства. Допускать к работе с серверным оборудованием только квалифицированных специалистов.
- Потеря данных - периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации. Проводить с администраторами информационной безопасности (и сотрудниками) разъяснительные и обучающие собрания. Обеспечить резервное копирование данных.
- Обнаружение вируса - соблюдать требования «Инструкции по организации антивирусной защиты».
- Утечка информации - применять средства защиты от НСД. Регулярно проводить анализ журналов попыток НСД и работы по совершенствованию системы защиты информации.
- Попытка несанкционированного доступа (НСД) - по возможности, установить регистрацию попыток НСД на всех технологических участках, где возможен несанкционированный доступ, с оповещением Администратора информационной безопасности о попытках НСД.
- Компрометация паролей - соблюдать требования «Инструкции по организации парольной защиты».
- Физическое повреждение ЛВС или ПЭВМ - физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним.
- Стихийное бедствие - проводить обучающие собрания и тренировки персонала по вопросам гражданской обороны.

Приложение № 13
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ИНСТРУКЦИЯ
О ПОРЯДКЕ РЕЗЕРВИРОВАНИЯ
и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах

1. Общие положения

1.1. Настоящая инструкция разработана с целью организации порядка резервирования и восстановления работоспособности технических средств (далее — ТС) и программного обеспечения (далее – ПО), баз данных (далее – БД) и средств защиты информации (далее — СЗИ) в информационных системах (далее – ИС), и разработана на основании:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации утвержденного».

1.2. Настоящая инструкция определяет порядок резервирования и восстановления работоспособности ТС и ПО, БД и СЗИ, и определяет порядок действий ответственных лиц, связанных с функционированием (ИС), меры и средства поддержания непрерывности работы и восстановления работоспособности ИС.

1.3. Целью настоящего документа является превентивная защита элементов ИС от предотвращения потери защищаемой информации.

Задачами данной инструкции являются:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИС, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

1.6. Ответственным сотрудником за реагирование на инциденты безопасности и контроль мероприятий по предотвращению инцидентов, приводящих к потере защищаемой информации, назначается Администратор безопасности ИСПДн.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИС;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в «Журнал учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах ИС».

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники, предпринимают меры по

восстановлению работоспособности. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством.

3. Технические меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа;
- системы жизнеобеспечения ИС.

3.2. Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все помещения, в которых размещаются элементы ИС, материальные носители ПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных рабочих станций и серверов;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы,

концентраторы, мосты и т. д.);

- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.6. Для обеспечения отказоустойчивости критичных компонентов ИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИС должны использоваться территориально удаленные системы кластеров.

3.7. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на съемный носитель (ленту, жесткий диск и т. п.).

4. Организационные меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

4.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в день инкрементальным способом, и не реже одного раза в неделю полный объем данных;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

4.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

4.4. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

4.5. Носители должны храниться не менее года, для возможности восстановления данных.

5. Ответственность

5.1. Ответственность за поддержание установленного в настоящей инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности информации.