МИНОБРНАУКИ РОССИИ

DIRECTUM-15000-753811

федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ»)

П Р И К А З

11.08.2017 № 1357

О порядке обеспечения безопасности информации в ФГАОУ ВО «СПбПУ»

Руководствуясь Федеральным законом «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006, «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации» (СТР-К), принятыми решением Коллегии Гостехкомиссии России № 7.2 от 02.03.2001, в целях обеспечения информационной безопасности ФГАОУ ВО «СПбПУ», а также для выполнения требований плана устранения нарушений и недостатков, выявленных в ходе проведения проверки комиссией Управления Федеральной службы по техническому и экспортному контролю по Северо-Западному федеральному округу

ПРИКАЗЫВАЮ:

1. Директорам институтов, руководителям подразделений, по согласованию с проректором по безопасности, назначить администраторов по обеспечению безопасности информации в структурных подразделениях, обрабатывающих персональные данные (конфиденциальную информацию) в электронной форме. Срок исполнения - до 20.08.2017.
2. Утвердить и ввести в действие с 20.08.2017 инструкцию администратора по обеспечению безопасности информации (Приложение № 1).
3. Утвердить и ввести в действие с 20.08.2017 инструкцию пользователя информационной системы персональных данных (конфиденциальной информации) (Приложение № 2).
4. Утвердить типовую форму журнала учета машинных носителей персональных данных (конфиденциальной информации) (Приложение № 3).
5. Администраторам по обеспечению безопасности информации в подразделениях, обрабатывающих персональные данные (конфиденциальную информацию) в электронной форме, организовать ведение журнала учета машинных носителей персональных данных (конфиденциальной информации). Срок исполнения - до 01.09.2017.

Первый проректор В.В. Глухов

Приложение № 1
к приказу от 11.08.2017 № 1357

ИНСТРУКЦИЯ
администратора по обеспечению безопасности информации

1. Общие положения

1.1 Настоящая Инструкция разработана в соответствии Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», методическими рекомендациями ФСТЭК России от 15.02.2008, утвержденными приказом ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», ГОСТ Р ИСО/МЭК 17799-2015 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, является дополнением к приказу ректора от 03.07.2007 № 149 «О работе с конфиденциальной информацией» и устанавливает порядок работы администратора по обеспечению безопасности информации.

1.2 Настоящий документ определяет основные обязанности, права и ответственность администраторов по обеспечению безопасности информации в структурных подразделениях ФГАОУ ВО «СПбПУ», обрабатывающих персональные данные (конфиденциальную информацию) в электронной форме.

1.3 Администраторы по обеспечению безопасности информации назначаются приказом ректора или первого проректора из числа штатных сотрудников подразделений, по представлению руководителя структурного подразделения и после согласования с проректором по безопасности.

1.4 Администраторы по обеспечению безопасности информации руководствуются локальными нормативными актами Университета и настоящей Инструкцией.

1.5 Администраторы по обеспечению безопасности информации координируют и контролируют работу пользователей информационных систем по вопросам обеспечения безопасности информации на основании настоящей инструкции.

1.6 Действие настоящей Инструкции распространяется на сотрудников ФГАОУ ВО «СПбПУ», назначенных приказом администраторами по обеспечению безопасности информации.

2. Основные термины, сокращения и определения

2.1 Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

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

2.3 Администратор по обеспечению безопасность информации – технический специалист, ответственный за защиту информационной системы от несанкционированного доступа к информации, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники.

2.4 Средства защиты информации – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, вещных элементов, используемых для решения различных задач по защите информации, а также программы, специально предназначенные для выполнения

функций, связанных с защитой информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

2.5 Автоматизированная система управления – комплекс аппаратных и программных средств, а также персонала, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия.

2.6 АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным программным обеспечением) для выполнения определенной производственной задачи.

2.7 Машинный носитель информации – материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники.

2.8 ПК – персональный компьютер.

2.9 ПО – программное обеспечение вычислительной техники.

2.10 Вредоносное ПО – программное обеспечение или изменения в программном обеспечении, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.11 Коммерческое ПО – программное обеспечение сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

2.12 Пользователь информационной системы – сотрудник Университета, использующий информационную систему, автоматизированное рабочее место, мобильные устройства и машинные носители информации для выполнения своих служебных обязанностей.

3. Права и обязанности администратора по обеспечению безопасности информации

3.1 Устанавливать разграничение полномочий пользователей и порядок доступа к информационным ресурсам, порядок использования основных и вспомогательных технических средств и систем.

3.2 Вести учет нештатных ситуаций.

3.3 Информировать руководство и уполномоченных работников информационной безопасности об инцидентах и попытках несанкционированного доступа к информации, элементам автоматизированных систем управления по результатам функционирования и контроля систем технической защиты информации.

3.4 Осуществлять администрирование сервисами и механизмами безопасности автоматизированных систем управления, комплексами и средствами технической защиты информации и контроля.

3.5 Готовить предложения по совершенствованию технологических мер защиты информации.

3.6 Контролировать работы по установке, модернизации и профилактике аппаратных и программных средств, созданию, учету, хранению и использованию резервных и архивных копий массивов данных и электронных документов.

3.7 Принимать участие в работах по внесению изменений в программно-аппаратную конфигурацию автоматизированных систем управления и контролировать ее соответствие требованиям обеспечения безопасности информации.

3.8 Вести учет носителей информации, осуществлять их хранение, прием, выдачу ответственным исполнителям, контролировать правильность их использования.

3.9 Требовать от пользователей информационных систем выполнения инструкций по обеспечению безопасности и защите информации.

3.10 Иметь доступ к программно-аппаратным ресурсам и информации на АРМ пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.

3.11 Блокировать или ограничивать использование машинных носителей информации.

3.12 Участвовать в проведении служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов информационной системы.

3.13 Непосредственно обращаться к руководителям подразделений с требованием прекращения работы в информационной системе при несоблюдении установленной технологии обработки информации и невыполнении требований по обеспечению безопасности информации.

3.14 Вносить свои предложения по совершенствованию мер защиты информации в Университете.

3.15 Разрабатывать план аварийного восстановления информационных систем в течение фиксированного времени и участвовать в его реализации.

3.16 Разрабатывать и реализовывать политики доступа в Интернет, создавать и вносить изменения в настройки доступа.

3.17 Вести сопровождение и техническую поддержку систем безопасности информации.

3.18 Организовывать обращения в службу поддержки производителя программного обеспечения и оборудования информационных систем.

3.19 Выполнять активацию, хранить идентификаторы активации и осуществлять контроль обновления лицензий коммерческого ПО.

4. Порядок использования, учета, хранения и обращения с машинными носителями персональных данных (конфиденциальной информации) (далее - машинные носители информации), твердыми копиями и их утилизации

4.1 Под использованием машинных носителей информации в информационной системе Университета понимается их подключение к инфраструктуре информационной системы с целью обработки, приема и передачи информации.

4.2 В информационной системе допускается использование только учтенных машинных носителей информации, которые подвергаются регулярной ревизии и контролю.

4.3 К предоставленным сторонней организацией машинным носителям информации предъявляются те же требования по обеспечению безопасности информации, что и для стационарных АРМ (администратор по обеспечению безопасности информации определяет целесообразность применения дополнительных мер защиты информации).

4.4 Все находящиеся на хранении и в обращении машинные носители информации в Университете подлежат учёту.

4.5 Каждый машинный носитель информации с записанной на нем информацией должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.6 Администратор по обеспечению безопасности информации осуществляет учет и выдачу машинных носителей информации. Факт выдачи и регистрации машинного носителя информации фиксируется в журнале учета машинных носителей информации.

4.7 Пользователи могут получать машинный носитель для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает машинный носитель информации для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.8 Любое взаимодействие (обработка, прием, передача информации), инициированное пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных заранее с администратором по обеспечению безопасности информации).

4.9 Информация об использовании машинных носителей информации в информационной системе, при необходимости, может быть предоставлена лицу,

ответственному за организацию обработки персональных данных (конфиденциальной информации) в Университете.

4.10 В случае выявления фактов несанкционированного и/или нецелевого использовании машинных носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой утверждается проректором по безопасности Университета. По факту выясненных обстоятельств составляется акт расследования инцидента и передается первому проректору Университета для принятия соответствующих мер.

4.11 Хранение и использование машинных носителей информации должно осуществляться в соответствии с техническими условиями изготовителя. Не допускается превышение срока эксплуатации, установленного изготовителем машинных носителей информации.

4.12 Информация, хранящаяся на машинных носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

4.13 При отправке или передаче информации адресатам на машинные носители информации записываются только предназначенные адресатам данные. Отправка информации адресатам на машинных носителях информации осуществляется в порядке, установленном для документов для служебного пользования.

4.14 Вынос машинных носителей информации для непосредственной передачи адресату осуществляется только с письменного распоряжения руководителя структурного подразделения.

4.15 Право на перемещение машинных носителей информации предоставляется только тем пользователям, которым оно необходимо для выполнения должностных обязанностей.

4.16 В случае утраты или уничтожения машинных носителей информации либо разглашения содержащихся в них сведений, об этом немедленно ставится в известность руководитель соответствующего структурного подразделения. По факту утраты носителя составляется акт. Соответствующие отметки вносятся в журнал учета машинных носителей информации.

4.17 Вышедшие из строя машинные носители информации ремонту не подлежат. Такие носители уничтожаются методом разборки и физического разрушения.

4.18 Машинные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей информации осуществляется комиссией. Уничтожение машинных носителей информации должно обеспечивать полное физическое и невосстановимое уничтожение содержащейся на них информации. По результатам уничтожения машинных носителей информации составляется акт по прилагаемой форме (Приложение №1), который подлежит хранению в течение пяти лет.

4.19 В случае увольнения или перевода сотрудника в другое структурное подразделение, предоставленные ему машинные носители информации изымаются.

5. Организация хранения резервных копий персональных данных (конфиденциальной информации) на электронных носителях информации

5.1 Электронные документы хранятся на физически обособленных электронных носителях информации, обычно на оптических компакт-дисках (CD, DVD) и размещаются отдельно от других документов в специально оборудованных местах. Архивный шифр электронных документов, хранимых на обособленных электронных носителях, указывается на вкладыше, вложенном в футляр носителя.

5.2 В процессе хранения электронных документов в архиве, не реже одного раза в год производится технический контроль физического состояния носителей электронных документов и воспроизводимости электронных документов.

5.3 Электронные носители с резервными копиями информации не выдаются для работы обычным пользователям и служат только для восстановления в случае аварии или поломки основного машинного носителя информации.

5.4 Электронные носители с резервными копиями рекомендуется хранить в отдельном, специально оборудованном помещении.

6. Организация антивирусной защиты

6.1 К использованию на АРМ допускается антивирусное программное обеспечение, сертифицированное ФСТЭК России и централизованно закупленное у разработчиков или их дистрибьюторов.

6.2 Установка и настройка параметров антивирусного программного обеспечения на АРМ осуществляется администратором по обеспечению безопасности информации в соответствии с руководством администратора, входящим в комплект программного обеспечения.

6.3 Антивирусный контроль на АРМ должен производиться ежедневно в автоматическом режиме.

6.4 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая с помощью съемных (внешних) носителей информации. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на АРМ.

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).

6.5 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в год. В случае обнаружения вредоносных программ (вирусов и т. п.) носители (единицы хранения электронных документов, содержащие вредоносные компьютерные программы) изымаются администратором по обеспечению безопасности информации у пользователя информационной системы для последующей обработки.

6.6 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения АРМ, администратором по обеспечению безопасности информации должна быть выполнена антивирусная проверка.

6.7 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.) администратор по обеспечению безопасности информации должен произвести внеочередную полную антивирусную проверку АРМ.

6.8 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов, администратору по обеспечению безопасности информации необходимо:

- приостановить работу на АРМ;
- незамедлительно поставить в известность о факте обнаружения компьютерного вируса владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение и уничтожение зараженных файлов.

6.9 Ответственность за работоспособность и обновление антивирусного программного обеспечения возлагается на администратора по обеспечению безопасности информации.

7. Порядок ежедневного обслуживания информационных систем персональных данных (конфиденциальной информации) администратором по обеспечению безопасности информации

7.1 Выполнение мониторинга событий по информационной безопасности, выявление и исправление ошибок программных приложений для обеспечения их штатного функционирования.

7.2 Внесение необходимых изменений в настройки программных приложений.

7.3 Мониторинг работы служб обновлений операционных систем и программного обеспечения, проверка и установка обновлений.

7.4 Выполнение мониторинга работы средств фильтрации почтовых сообщений, внесение изменений в настройки.

8. Ответственность администратора по обеспечению безопасности информации

8.1 На администратора по обеспечению безопасности информации возлагается персональная ответственность за качество проводимых работ по обеспечению информационной безопасности в соответствии с настоящей инструкцией.

8.2 Администратор по обеспечению безопасности информации несет ответственность по действующему законодательству за разглашение конфиденциальной информации, и сведений ограниченного распространения, ставших известными ему в связи с осуществлением служебных полномочий.

Инструкцию разработал:

Начальник отдела защиты
конфиденциальной информации _____ А.Ю. Синицын
(подпись)

Приложение №1
к Инструкции администратора по обеспечению безопасности информации

Акт
об уничтожении машинных носителей
персональных данных (конфиденциальной информации)

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор машинных носителей персональных данных (конфиденциальной информации) и установила, что информация, записанная на них, не подлежит дальнейшему использованию (хранению) и подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Учетный номер машинного носителя	Примечание

Всего машинных носителей
_____
(цифрами и прописью)

На указанных носителях персональные данные (конфиденциальная информация) уничтожены путем:
_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители персональных данных (конфиденциальной информации) уничтожены путем
_____
(разрезания, демонтажа, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

Примечание:
1. Акт составляется раздельно на каждый способ уничтожения машинных носителей.
2. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

Приложение № 2
к приказу от 11.08.2017 № 1357

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных (конфиденциальной информации)

1. Общие положения

1.1 Настоящая Инструкция разработана в соответствии Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», методическими рекомендациями ФСТЭК России от 15.02.2008, утвержденными приказом ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», ГОСТ Р ИСО/МЭК 17799-2015 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, является дополнением к приказу ректора от 03.07.2007 № 149 «О работе с конфиденциальной информацией» и устанавливает порядок работы пользователя, выполняющего автоматизированную обработку персональных данных (конфиденциальной информации).

1.2 Действие настоящей Инструкции распространяется на сотрудников ФГАОУ ВО «СПбПУ», выполняющих автоматизированную обработку персональных данных (конфиденциальной информации).

2. Основные термины, сокращения и определения

2.1 Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

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

2.3 Администратор по обеспечению безопасность информации – технический специалист, ответственный за защиту информационной системы от несанкционированного доступа к информации, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники.

2.4 Средства защиты информации – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, вещных элементов, используемых для решения различных задач по защите информации, а также программы, специально предназначенные для выполнения функций, связанных с защитой информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

2.5 Автоматизированная система управления – комплекс аппаратных и программных средств, а также персонала, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия.

2.6 АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным программным обеспечением) для выполнения определенной производственной задачи.

2.7 Машинный носитель информации – материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники.

2.8 ПК – персональный компьютер.

2.9 ПО – программное обеспечение вычислительной техники.

2.10 Вредоносное ПО – программное обеспечение или изменения в программном обеспечении, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.11 Коммерческое ПО – программное обеспечение сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

2.12 Пользователь информационной системы – сотрудник Университета, использующий информационную систему, автоматизированное рабочее место, мобильные устройства и машинные носители информации для выполнения своих служебных обязанностей.

3. Обязанности пользователя информационной системы

3.1 Хранить в тайне конфиденциальные сведения, ставшие известными пользователю информационной системы, в соответствии с родом работы.

3.2 Хранить в тайне идентификатор и пароль, используемые пользователем для входа в информационную систему.

3.3 При обработке персональных данных (конфиденциальной информации) руководствоваться правилами работы с общесистемным и прикладным программным обеспечением.

3.4 Соблюдать порядок учета, обращения, хранения и уничтожения конфиденциальной информации и выходных документов (распечаток) в соответствии с требованиями конфиденциального делопроизводства.

3.5 Для предотвращения несанкционированного доступа к информации, при краткосрочном отсутствии пользователь информационной системы обязан блокировать консоль ПК или выключать ее. Для блокировки консоли ПК пользователю информационной системы необходимо нажать на клавиатуре комбинацию клавиш «CTRL» + «ALT» + «DEL» - «Блокировка» («Winkey» + «L»). После этого разблокировка ПК производится только после правильного ввода своего пароля пользователем информационной системы.

3.6 Использовать только штатные программные и технические средства. Установка новых программных и основных технических средств, должна согласовываться с администратором по обеспечению безопасности информации**.**

Проводить антивирусные проверки машинных носителей информации, на которых могут содержаться потенциально инфицированные файлы.

3.7 Проводить контроль над соблюдением требований по защите конфиденциальной информации в информационной системе. О фактах несанкционированного доступа к конфиденциальной информации или нарушении правил разграничения доступа к информации, обрабатываемой в ИС, докладывать администратору по обеспечению безопасности информации.

4. Пользователю информационной системы запрещается:

4.1 Использовать нештатные технические средства и системы; самостоятельно вносить изменения в состав, конфигурацию, и размещение АРМ.

4.2 Использовать нештатные программные средства и самостоятельно вносить изменения в их состав.

4.3 Осуществлять попытки обхода ограничений политик информационной безопасности.

4.4 Использовать аппаратные и программные средства, позволяющие обойти ограничения, наложенные средствами информационной безопасности.

4.5 Вносить изменения в средства защиты информации, используемые в информационной системе.

4.6 Допускать к работам в информационной системе лиц, не имеющих допуска к этим работам.

4.7 Передавать конфиденциальную информацию по сети Интернет без применения специальных средств защиты информации.

4.8 Производить копирование конфиденциальной информации на неучтенные машинные носители информации.

4.9 Использовать в качестве носителей конфиденциальной информации неучтенные в специальном журнале съемные накопители.

4.10 Использовать информационную систему в целях, не связанных с выполнением служебных обязанностей, в том числе тех, которые могут повлечь нанесение ущерба и убытков.

4.11 Передавать пароли. Каждый пользователь информационной системы обязан соблюдать конфиденциальность пароля.

4.12 Подключать неслужебные компьютеры к информационной системе. Для удаленного подключения к информационной системе следует использовать средства удаленного доступа, предоставленные администратором по обеспечению безопасности информации**.**

4.13 Обрабатывать информацию в случае, если имеют место неисправности, создающие предпосылки для утечки конфиденциальной информации.

4.14 Проводить обработку конфиденциальной информации при неисправно работающих средствах защиты информации.

4.15 Обрабатывать информацию, если требования настоящей Инструкции, СТР-К и других РД и НМД по защите конфиденциальной информации не выполнены.

5. Порядок использования, учета, хранения и обращения с машинными носителями информации персональных данных (конфиденциальной информации), твердыми копиями и их утилизации

5.1 Под использованием машинных носителей информации в информационной системе Университета понимается их подключение к инфраструктуре информационной системы с целью обработки, приема и передачи информации.

5.2 В информационной системе допускается использование только учтенных машинных носителей информации, которые подвергаются регулярной ревизии и контролю.

5.3 К предоставленным сторонней организацией машинным носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения безопасности информации определяется администраторами по обеспечению безопасности информации).

5.4 Все находящиеся на хранении и в обращении машинные носители информации в Университете подлежат учёту.

5.5 Каждый машинный носитель информации с записанной на нем информацией должен иметь этикетку, на которой указывается его уникальный учетный номер.

5.6 Учет и выдачу машинных носителей информации осуществляет администратор по обеспечению безопасности информации. Факт выдачи и регистрации машинного носителя информации фиксируется в журнале учета машинных носителей информации.

5.7 Пользователи могут получать машинный носитель для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает машинный носитель информации для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5.8 При использовании сотрудниками машинных носителей информации необходимо:

5.8.1 Соблюдать требования настоящей Инструкции.

5.8.2 Использовать машинные носители информации исключительно для выполнения своих служебных обязанностей.

5.8.3 Ставить в известность администратора по обеспечению безопасности информации о любых фактах нарушения требований настоящей Инструкции.

5.8.4 Бережно относиться к машинным носителям информации.

5.8.5 Обеспечивать физическую безопасность машинных носителей информации всеми разумными способами, в условиях, исключающих несанкционированное копирование, изменение или уничтожение информации, а также хищение носителей.

5.8.6 Хранить носители в служебных помещениях, в закрываемом на ключ шкафу (сейфе).

5.8.7 Извещать администраторов по обеспечению безопасности информации о фактах утраты (кражи) машинных носителей информации.

5.9 При использовании машинных носителей информации запрещено:

5.9.1 Использовать машинные носители персональных данных (конфиденциальной информации) в личных целях.

5.9.2 Передавать машинные носители информации другим лицам (за исключением администраторов по обеспечению безопасности информации).

5.9.3 Хранить машинные носители информации вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

5.9.4 Выносить машинные носители информации из служебных помещений для работы с ними на дому либо в других помещениях на не аттестованных АРМ.

5.10 Любое взаимодействие (обработка, прием, передача информации), инициированное пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных заранее с администратором по обеспечению безопасности информации). Администратор по обеспечению безопасности информации оставляет за собой право блокировать или ограничивать использование машинных носителей информации.

5.11 Сведения об использовании машинных носителей информации, могут быть предоставлены лицу, ответственному за организацию обработки персональных данных в Университете.

5.12 Хранение и использование машинных носителей информации должно осуществляться в соответствии с техническими условиями изготовителя. Не допускается превышение срока эксплуатации, установленного изготовителем машинных носителей информации.

5.13 Информация, хранящаяся на машинных носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

5.14 При отправке или передаче информации адресатам на машинные носители информации записываются только предназначенные адресатам данные. Отправка информации адресатам на машинных носителях информации осуществляется в порядке, установленном для документов для служебного пользования.

5.15 Вынос машинных носителей информации для непосредственной передачи адресату осуществляется только с письменного распоряжения руководителя структурного подразделения.

5.16 Право на перемещение машинных носителей информации предоставляется только тем пользователям, которым оно необходимо для выполнения должностных обязанностей.

5.17 В случае утраты или уничтожения машинных носителей информации либо разглашении содержащихся в них сведений, об этом немедленно ставится в известность руководитель соответствующего структурного подразделения. По факту утраты носителя составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей информации.

5.18 Вышедшие из строя машинные носители информации ремонту не подлежат. Такие носители уничтожаются методом разборки и физического разрушения.

5.19 Машинные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей информации осуществляется администратором по обеспечению безопасности информации в составе комиссии. Уничтожение машинных носителей информации должно обеспечивать полное физическое и невосстановимое уничтожение содержащейся на них информации. По результатам уничтожения машинных носителей информации составляется акт, который подлежит хранению в течение пяти лет.

5.20 В случае увольнения или перевода сотрудника в другое структурное подразделение, предоставленные ему машинные носители информации изымаются.

6. Организация антивирусной защиты

6.1 К использованию на АРМ допускается антивирусное программное обеспечение, сертифицированное ФСТЭК России и централизованно закупленное у разработчиков или их дистрибьюторов.

6.2 Установка и настройка параметров антивирусного программного обеспечения на АРМ осуществляется администратором по обеспечению безопасности информации в соответствии с руководством администратора, входящим в комплект программного обеспечения.

6.3 Антивирусный контроль на АРМ должен производиться ежедневно в автоматическом режиме.

6.4 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая с помощью съемных (внешних) носителей информации. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на АРМ.

6.5 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).

6.6 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в год. В случае обнаружения вредоносных программ (вирусов и т. п.) носители (единицы хранения электронных документов, содержащие вредоносные компьютерные программы) передаются администратору по обеспечению безопасности информации для последующей обработки.

6.7 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера администратором по обеспечению безопасности информации, должна быть выполнена антивирусная проверка.

6.8 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.) сообщить администратору по обеспечению безопасности информации и произвести внеочередную полную антивирусную проверку АРМ.

6.9 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов, пользователю информационной системы необходимо:

- приостановить работу на АРМ;
- незамедлительно поставить в известность о факте обнаружения компьютерного вируса администратора по обеспечению безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение и уничтожение зараженных файлов.

6.10 Незамедлительно сообщать администратору по обеспечению безопасности информации обо всех обнаруженных неисправностях и отсутствии обновления антивирусного программного обеспечения.

7. Организация хранения резервных копий персональных данных (конфиденциальной информации)

7.1 Электронные документы хранятся на физически обособленных электронных носителях информации, обычно на оптических компакт-дисках (CD, DVD) и размещаются отдельно от других документов в специально оборудованных местах. Архивный шифр электронных документов, хранимых на обособленных электронных носителях, указывается на вкладыше, вложенном в футляр носителя.

7.2 В процессе хранения электронных документов в архиве организации не реже одного раза в год производится технический контроль физического состояния носителей электронных документов и воспроизводимости электронных документов.

7.3 Электронные носители с резервными копиями информации не выдаются для работы обычным пользователям и служат только для восстановления в случае аварии или поломки основного машинного носителя информации.

7.4 Машинные носители информации с резервными копиями хранить в отдельном, специально оборудованном помещении.

8. Ответственность

8.1 Сотрудники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующими нормативными документами Университета и законодательством.

Инструкцию разработал:

Начальник отдела защиты
конфиденциальной информации (подпись) А.Ю. Синицын

Приложение №3
к приказу от 11.08.2017 № 1357

ТИПОВАЯ ФОРМА ЖУРНАЛА
учета машинных носителей персональных данных (конфиденциальной информации)

1. Титульный лист журнала:

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»
(ФГАОУ ВО «СПбПУ»)

Уч. № _____ от «___» _____ 20___ г

ЖУРНАЛ
учёта машинных носителей конфиденциальной информации (персональных данных)

Журнал начат: «___»_____201__г.

Ответственный _____
должность

_____/_____/
подпись ФИО должностного лица

Журнал окончен:«___»_____201__г.

Ответственный _____
должность

_____/_____/
подпись ФИО должностного лица

На _____ лист___

2. Страницы журнала:

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования)/ дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, номер и дата акта)

DIRECTUM-15000-753811

Проект вносит	Согласовано
А.Ю. Синицын (11.08.2017 12:26:36)	А.А. Филимонов (11.08.2017 12:48:37) А.В. Иванов (11.08.2017 14:33:58)