

НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ИНСТИТУТ БИЗНЕСА И ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Ректор НОУ ВПО "СИБИТ"
С.В.Грисько
"30" 2017г.



**ПОЛОЖЕНИЕ
ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ**

Омск 2017

1. Общие положения

Настоящее Положение разработано в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее — Федеральный закон), постановления Правительства РФ от 01 ноября 2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", правилами обработки персональных данных в НОУ ВПО "СИБИТ" и иных нормативных документов по вопросам безопасности персональных данных (далее — ПДн).

Настоящее Положение устанавливает порядок обеспечения безопасности ПДн на всех этапах осуществления деятельности НОУ ВПО "СИБИТ".

Требования настоящего Положения являются обязательными для исполнения всеми сотрудниками НОУ ВПО "СИБИТ".

Настоящее Положение подлежит периодической ревизии на предмет соответствия закрепленного порядка обеспечения безопасности ПДн положениям Федерального закона и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике НОУ ВПО "СИБИТ" в отношении обработки персональных данных, локальным актам НОУ ВПО "СИБИТ". Ревизия осуществляется при проведении планового внутреннего контроля или аудита по вопросам обеспечения безопасности ПДн.

Настоящее Положение является внутренним документом НОУ ВПО "СИБИТ" и не подлежит опубликованию или распространению.

Требования настоящего Положения доводятся до сведения всех сотрудников НОУ ВПО "СИБИТ" при приеме на работу, по результатам ревизии настоящего Положения и во время планового инструктажа сотрудников НОУ ВПО "СИБИТ" по вопросам обеспечения безопасности ПДн.

В настоящем Положении под ПДн понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), являющимся сотрудником или контрагентом НОУ ВПО "СИБИТ", а также гражданину, обратившемуся в НОУ ВПО "СИБИТ".

Действие настоящего Положения не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации, в частности,

на документы Архивного фонда Российской Федерации, отнесенные к государственной собственности, до передачи на постоянное хранение, временно, в пределах сроков, установленных Федеральной архивной службой России, хранящиеся в организации.

2. Обеспечение безопасности персональных данных

НОУ ВПО "СИБИТ" обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. НОУ ВПО "СИБИТ" самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом или другими федеральными законами.

2.1. Меры, направленные на предотвращение нарушений законодательства Российской Федерации.

В НОУ ВПО "СИБИТ" на основании приказа назначена комиссия по вопросам информационной безопасности в НОУ ВПО "СИБИТ", с возложением на нее обязанностей согласно Положению о комиссии по вопросам информационной безопасности.

В НОУ ВПО "СИБИТ" на основании приказа ректора назначен ответственный за организацию обработки персональных данных в НОУ ВПО "СИБИТ", с возложением на него обязанностей согласно должностной инструкции об ответственном за организацию обработки персональных данных.

Определены цели обработки персональных данных.

Определен состав персональных данных, необходимых для реализации заявленных целей.

Определены сроки обработки (хранения) персональных данных.

Утверждены типовые формы документов, содержащих персональные данные.

Введены правила разграничения прав доступа к персональным данным и в помещения, где осуществляется их обработка и (или) хранение.

Утвержден порядок сбора, обработки, хранения и уничтожения персональных данных.

Организован учет материальных носителей, содержащих персональные данные, и их движения при осуществлении обработки персональных данных.

Обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности,

путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Сотрудники НОУ ВПО "СИБИТ", непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику НОУ ВПО "СИБИТ" в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

Осуществлено информирование лиц, осуществляющих обработку персональных данных без использования средств автоматизации (в том числе сотрудников НОУ ВПО "СИБИТ" или лиц, осуществляющих такую обработку по договору с НОУ ВПО "СИБИТ") о факте обработки ими персональных данных, о категориях обрабатываемых персональных данных, об особенностях и правилах осуществления такой обработки, об установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами НОУ ВПО "СИБИТ".

Внесены в должностные инструкции сотрудников НОУ ВПО "СИБИТ" положения о соблюдении конфиденциальности персональных данных.

В НОУ ВПО "СИБИТ" соблюдены следующие условия использования типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма):

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес НОУ ВПО "СИБИТ", фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в

процессе их обработки, общее описание используемых Законодательным Собранием способов обработки персональных данных;

б) типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма, содержащая персональные данные субъектов персональных данных, составлена таким образом, чтобы каждый субъект персональных данных имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, приняты меры по обеспечению отдельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных, осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Обеспечение физической сохранности материальных носителей, содержащих персональные данные, путем их хранения в специально отведенных для этого помещениях, оборудованных пассивными и (или) активными средствами защиты (запираемые двери с работающим запорным механизмом; ограждающие конструкции на окнах и иных проемах, размер которых позволяет физическому лицу проникнуть в помещение; запираемые шкафы, в том числе металлические шкафы или сейфы; системы пожарной сигнализаций, круглосуточный режим охраны штатными охранниками, стационарными постами охраны, системами видеонаблюдения, системой контроля управления доступом, контрольно-опечатывающими устройствами).

2.2. Меры, направленные на выявление нарушений законодательства Российской Федерации.

Периодическое проведение внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам НОУ ВПО "СИБИТ".

Проверка осуществляется ответственным лицом за организацию обработки персональных данных в НОУ ВПО "СИБИТ".

В ходе проверки осуществляется:

- анализ нормативных правовых актов и локальных актов НОУ ВПО "СИБИТ" на предмет правового обоснования обработки НОУ ВПО "СИБИТ" персональных данных;
- анализ актуальности целей обработки персональных данных;
- анализ соответствия состава и объема обрабатываемых персональных данных заявленным целям;
- анализ процесса обработки персональных данных на предмет соответствия утвержденному порядку;
- анализ достаточности предпринимаемых мер по обеспечению безопасности персональных данных;

– анализ локальных актов НОУ ВПО "СИБИТ" на соответствие требованиям по обеспечению безопасности персональных данных.

По результатам проверки проводятся мероприятия по устранению выявленных нарушений.

Периодическое проведение проверки наличия и состояния документов и дел, содержащих персональные данные. Проверка проводится в целях установления фактического наличия документов и дел, соответствия их количеству, числящемуся по учетным документам.

В ходе проверки осуществляется:

- установление фактического наличия документов и дел, находящихся на хранении;
- выявление и устранение недостатков в учете документов и дел;
- выявление отсутствующих документов и дел и организация их розыска.

Проверка наличия и состояния документов и дел, содержащих персональные данные, проводится не реже чем один раз в квартал, а также перед передачей их на хранение.

Единовременные проверки наличия и состояния документов и дел проводятся:

- после перемещения документов и дел в другое помещение;
- после чрезвычайных происшествий, вызвавших перемещение (эвакуацию) документов и дел или доступ в хранилища посторонних лиц;
- при смене лица, ответственного за хранение;
- при прекращении деятельности НОУ ВПО "СИБИТ".

При проверке наличия и состояния документов и дел необходимо:

- сохранять порядок расположения документов и дел на стеллажах и первичных средствах хранения;
- подкладывать на свои места, обнаруженные во время проверки, неправильно подложенные документы и дела;
- изымать документы и дела, не внесенные в опись.

Внесение в опись неучтенных документов и дел в ходе проверки запрещается. Неучтенные документы и дела помещаются вслед за учтенными документами и делами для последующей обработки и описания.

До начала работы по проверке наличия и состояния документов и дел изучаются результаты предыдущих проверок: проверяется правильность нумерации документов и дел в каждом годовом разделе сводной описи, соответствие нумерации документов и дел итоговым записям в описях.

Проверка наличия и состояния документов и дел проводится путем сверки описательных статей описи с описанием документов и дел на

обложках или лицевых страницах (шифра, названия фондообразователя и его структурных подразделений, делопроизводственных индексов дел, дат дел, количества листов).

Делать какие-либо пометки или записи в ходе проверки в описях дел и других учетных документах запрещается.

Дела и документы, выданные сотрудникам НОУ ВПО "СИБИТ", во временное пользование другим организациям проверяются по книгам и актам выдачи и считаются имеющимися в наличии.

Лист проверки наличия и состояния документов и дел составляется непосредственно в ходе проверки; листы проверки нумеруются по порядку номеров в пределах проверки каждого хранилища и подписываются исполнителем. Если в результате проверки недостатков не обнаружено, лист проверки не сохраняется.

По окончании проверки наличия и состояния документов и дел по каждой описи, в конце описи после заверительной надписи делается запись "проверено", проставляется дата проверки; запись подписывается проводившими проверку сотрудниками с указанием их должностей.

Если проверкой обнаружена недостача дел и документов, то организуется их розыск.

В этих целях необходимо:

- изучить все учетные документы по выдаче документов и дел из хранилища;
- организовать розыск не обнаруженных при проверке документов и дел в соответствующих структурных подразделениях, в деятельности которых образовались необнаруженные документы и дела;
- проверить документы и дела находящиеся рядом хранилищ;
- изучить акты о выделении дел к уничтожению, акты выдачи дел во временное пользование, ранее составленные акты проверки наличия и состояния проверяемого хранилища.

Розыск проводится в течение одной недели после завершения проверки наличия документов и дел.

Найденные в итоге розыска документы и дела подкладываются на места, а по факту наличия необнаруженных документов и дел должно проводиться служебное расследование.

Дела, причина отсутствия которых подтверждена соответствующими документами, исключаются в установленном порядке из описей и других учетных документов. После рассмотрения результатов розыска и принятия решения руководителем организации необнаруженные документы снимаются с учета.

2.3. Меры по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

В случае выявления неправомерной обработки персональных данных НОУ ВПО "СИБИТ" осуществляет блокирование неправомерно обрабатываемых персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") с момента обнаружения неправомерной обработки персональных данных. В случае выявления неточных персональных данных НОУ ВПО "СИБИТ" осуществляет блокирование неточных (неполных) персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") с момента выявления неточных персональных данных, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой НОУ ВПО "СИБИТ" или лицом, действующим по поручению НОУ ВПО "СИБИТ", НОУ ВПО "СИБИТ" в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению НОУ ВПО "СИБИТ". В случае если обеспечить правомерность обработки персональных данных невозможно, НОУ ВПО "СИБИТ" в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных НОУ ВПО "СИБИТ" уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных

данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также и указанный орган.

В случае достижения цели обработки персональных данных НОУ ВПО "СИБИТ" прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между НОУ ВПО "СИБИТ" и субъектом персональных данных, либо, если НОУ ВПО "СИБИТ" не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных НОУ ВПО "СИБИТ" прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между НОУ ВПО "СИБИТ" и субъектом персональных данных, либо если НОУ ВПО "СИБИТ" не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

В случае отсутствия возможности уничтожения персональных данных в течение указанного срока НОУ ВПО "СИБИТ" осуществляет блокирование

таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению НОУ ВПО "СИБИТ") и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

2.4. Меры по обеспечению безопасности персональных данных при их автоматизированной обработке.

Безопасность персональных данных, обрабатываемых в информационной системе персональных данных, обеспечивается в соответствии с п.19 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных", приказом ФСТЭК от 18 февраля 2013 года № 21 и иными нормативно-правовыми актами.

К основным мерам по обеспечению безопасности Персональных данных при их автоматизированной обработке относятся:

- определение угроз безопасности персональных данных при их обработке в информационной системе персональных данных и составление модели угроз;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- учет машинных носителей персональных данных;
- идентификация и проверка подлинности пользователя при входе в систему по паролю;
- система контроля управления доступом, предусматривающая контроль доступа в помещения информационной системы посторонних лиц сотрудниками НОУ ВПО "СИБИТ";
- регистрация входа (выхода) пользователя в систему (из системы);
- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, неизменность программной среды;
- применение средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

2.5. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения уровней защищенности персональных данных в НОУ ВПО "СИБИТ".

2.5.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа

уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Для обеспечения безопасности ПДн НОУ ВПО "СИБИТ" реализуются следующие меры по идентификации и аутентификации субъектов доступа и объектов доступа:

- идентификация и аутентификация пользователей, являющихся сотрудниками НОУ ВПО "СИБИТ";
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации.

2.5.2. Меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.

Для обеспечения безопасности ПДн НОУ ВПО "СИБИТ" реализуются следующие меры по управлению доступом субъектов доступа к объектам доступа:

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- регламентация и контроль использования в информационной системе технологий беспроводного доступа;
- регламентация и контроль использования в информационной системе мобильных технических средств;
- управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

2.5.3. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Для обеспечения безопасности ПДн в НОУ ВПО "СИБИТ" реализуются следующие меры по регистрации событий безопасности:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности.

2.5.4. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Для обеспечения безопасности ПДн в НОУ ВПО "СИБИТ" реализуются следующие меры по антивирусной защите:

- реализация антивирусной защиты;

– обновление базы данных признаков вредоносных компьютерных программ (вирусов).

2.5.5. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Для обеспечения безопасности ПДн в Законодательном Собрании в качестве меры по контролю (анализу) защищенности персональных данных используется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

2.5.6. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Для обеспечения безопасности ПДн в НОУ ВПО "СИБИТ" реализуются следующие меры по защите технических средств:

1) Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключая несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

2) Размещение устройств вывода (отображения) информации, исключая ее несанкционированный просмотр.

2.5.7. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Для обеспечения безопасности ПДн в НОУ ВПО "СИБИТ" в качестве меры по защите информационной системы, ее средств, систем связи и передачи данных используется обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны;

2.5.8. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Для обеспечения безопасности ПДн в НОУ ВПО "СИБИТ" реализуются следующие меры по управлению конфигурацией информационной системы и системы защиты персональных данных:

- определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;

- управление изменениями конфигурации информационной системы и системы защиты персональных данных;

- анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с сотрудником, ответственным за обеспечение обработки персональных данных;

- документирование информации об изменениях в конфигурации информационной системы и системы защиты персональных данных.