 ВШПП СТО СИ ВШПП 3.7.009-2009	Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»
	Система менеджмента качества
	Положение о защите персональных данных



УТВЕРЖДАЮ
 Ректор НОУ ВПО СИ ВШПП

А.В.Бирюков

«12» июня 20 09г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Положение о защите персональных данных

СТО СИ ВШПП 3.7.009-2009

Версия 1.0

Дата введения: < 12 июня 2009г. >


Негосударственное образовательное
 учреждение высшего профессионального
 образования
 «Самарский институт - высшая школа
 приватизации и предпринимательства»
 Центр менеджмента качества образования
Контрольный экземпляр


СОГЛАСОВАНО

Ответственный представитель
 руководства по качеству

О.А.Корнилова

«11» июня 20 09г.

Разработчик	Должность	Подпись
Корнилова О.А.	Проректор по вопросам ка- чества обра- зования	

	Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»
	Положение о защите персональных данных
	СТО СИ ВШПП 3.7.009-2009

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целью данного Положения о защите персональных данных (далее – Положение) является защита персональных данных работников и студентов НОУ ВПО «Самарский институт – высшая школа приватизации и предпринимательства» (далее – институт) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, Федерального закона «Об информации, информатизации и защите информации», постановления Правительства РСФСР от 05.12.1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

1.3. Положение является обязательным локальным нормативным актом института (ст. 87 глава 14 Трудового Кодекса РФ), утверждается и вводится в действие приказом ректора и определяет основные требования к порядку получения, хранения, использования и передачи (далее - обработке) персональных данных работников. Изменения в положение вносятся также приказом ректора института.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные работника (ПДР) – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (статья 85 ТК РФ).

Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.


Обработка ПДР – получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности ПДР снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

Учитывая массовость и единое место обработки и хранения ПДР – соответствующий гриф ограничения на них не ставится. ПДР содержатся в основном документе персонального учета работников – личном деле работника.

2.2. В состав ПДР входят:

- личная карточка работника;
- личное дело сотрудника;
- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета;

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки;
- содержание трудового договора между работником и институтом;
- дополнительные документы (справка о доходах с предыдущего места работы,
- справка из органов государственной налоговой службы о предоставлении сведений об имущественном положении, медицинское заключение о состоянии здоровья и др.;
- анкетные и биографические данные;
- сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющих идентифицировать его личность (ст.2, № 24 ФЗ от 20.02.95); сведения о заработной плате;
- состав декларируемых сведений о наличии материальных ценностей; содержание декларации, подаваемой в налоговую инспекцию; подлинники и копии приказов по личному составу; основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям; копии отчетов, направляемые в органы статистики.


Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения – соответствующий гриф ограничения на них не ставится.

3. СБОР, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Все персональные данные работника следует получить у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение (п. 3 ст. 86 ТК РФ).

3.2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия (п. 4 ст. 86 ТК РФ). Работодатель также не имеет права получить и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом (п. 5 ст. 86 ТК РФ).

3.3. В случаях, непосредственно связанных с вопросами трудовых отношений, институт вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

3.4. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника и студента.


3.5. В целях обеспечения прав и свобод человека и гражданина институт при обработке персональных данных работника должен соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении на службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания, обрабатываемых персональных данных работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;
- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом;
- работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;
- работники не должны отказываться от своих прав на сохранение и защиту тайны;
- работодатель, работники и их представители должны совместно вырабатывать меры защиты персональных данных работника.

3.6. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.7. При передаче персональных данных работника институт должен соблюдать следующие требования:

- не сообщать данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правильно соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

- осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.8. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.


3.9. При передаче персональных данных работника институтом (в том числе и в коммерческих целях) за пределы учреждения работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

3.10. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.11. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.12. Порядок хранения и использования персональных данных работников в организации устанавливается работодателем с соблюдением Трудового кодекса. При этом в целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

3.13. В области защиты персональных данных обучающихся в институте ответственность несут инспекторы деканатов и кафедр, заместители деканов и деканы факультета.


3.14. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.15. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.16. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.17. Сотрудники института, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

3.18. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Право доступа к персональным данным сотрудника внутри организации имеют:

- ректор института;
- проректоры по направлениям деятельности;
- сотрудники бухгалтерии;
- инспектор по кадрам;
- руководители структурных подразделений;
- сотрудник организации – носитель этих данных.

4.2. Доступ к персональным данным студентов института имеют инспектора, заместители деканов и деканы факультетов.


4.3. Выдача трудовой книжки и копий документов, связанных с работой производится:

- по письменному заявлению работника работодатель обязан не позднее трех дней со дня подачи этого заявления выдать работнику копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказ об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и представляться работнику безвозмездно.
- при прекращении трудового договора работодатель обязан выдать работнику в день увольнения (последний день работы) трудовую книжку и по письменному заявлению работника копии документов, связанных с работой.
- в случае, если в день увольнения работника выдать трудовую книжку невозможно в связи с отсутствием работника либо его отказом от получения трудовой книжки на руки, работодатель направляет работнику уведомление о необходимости явиться за трудовой книжкой либо дать согласие на отправку ее по почте. Со дня направления уведомления работодатель освобождается от ответственности за задержку выдачи трудовой книжки.

4.4. Другие сотрудники организации имеют доступ к персональным данным сотрудников организации только с их письменного согласия.

4.5. К числу массовых (внешних) потребителей персональных данных вне института можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

	Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»
	Положение о защите персональных данных
	СТО СИ ВШПП 3.7.009-2009

4.6. Надзорно-контролирующие органы имеют доступ к информации только в сфере своей компетенции.

4.7. Организации, в которые сотрудник института может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.8. Сведения о работающем или уже уволенном сотруднике института могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ


5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.3. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.4. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно - методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только ректору, руководителям структурных подразделений и в исключительных случаях, по письменному разрешению ректора – руководителю структурного подразделения, (например, при подготовке материалов для аттестации работника).


5.5. Персональные данные сотрудника института на электронных носителях должны быть защищены паролем, который сообщается руководителю службы управления персоналом и руководителю службы информационных технологий.

5.6. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.7. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности института, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

5.8. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

- пропускной режим организации;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств.

5.9. Кроме мер защиты персональных данных, установленных законодательством, институт, работники и их представители могут выработать совместные меры защиты персональных данных работников.

6. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА В ОБЛАСТИ ЗАЩИТЫ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.


6.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- на полную информацию о своих персональных данных и обработке этих данных;
- на требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством РФ;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.4. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

	Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»
	Положение о защите персональных данных
	СТО СИ ВШПП 3.7.009-2009

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в учетных документах на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.


7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник института, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или за-

	<p>Негосударственное образовательное учреждение высшего профессионального образования «САМАРСКИЙ ИНСТИТУТ – ВЫСШАЯ ШКОЛА ПРИВАТИЗАЦИИ И ПРЕДПРИНИМАТЕЛЬСТВА»</p>
	<p>Положение о защите персональных данных</p>
	<p>СТО СИ ВШПП 3.7.009-2009</p>

ведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

7.7. Нарушение порядка, сбора, хранения, использования или распространения информации о гражданах (персональных данных), установленного законом РФ и настоящим Положением влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

