

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»



В.Д. Нечаев

2025 г.

№ 02-01-09/166

к приказу

от 04.04.2025 № 749-н

ПОЛОЖЕНИЕ

об обработке персональных данных
в ФГАОУ ВО «Севастопольский государственный университет»

Севастополь
2025

Содержание

1. Общие положения.....	3
2. Организация обработки персональных данных	4
3. Жизненный цикл обработки персональных данных.....	6
4. Передача персональных данных	7
5. Хранение и использование ПД работников.....	8
6. Уничтожение (обезличивание) персональных данных	10
7. Использование средств вычислительной техники для обработки персональных данных	10
8. Обеспечение конфиденциальности персональных данных	12
9. Заключительные положения.....	15
Приложение 1. Сводная таблица действий в ответ на обращения субъектов персональных данных, их представителей и запросы Роскомнадзора	17

1. Общие положения

1.1. Положение об обработке персональных данных в ФГАОУ ВО «Севастопольский государственный университет» (далее соответственно – Университет, Положение) разработано во исполнение требований пункта 2 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Положение определяет требования к обработке персональных данных (далее также – ПД) в структурных подразделениях Университета, в том числе с использованием средств вычислительной техники и информационных систем.

1.3. Требования настоящего Положения не распространяются на обработку ПД, связанную с организацией хранения, комплектования, учета и использования содержащих ПД архивных документов в соответствии с законодательством об архивном деле в Российской Федерации, а также обработкой ПД, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.4. Целью защиты ПД является предотвращение ущерба собственнику – субъекту ПД.

1.5. Документы, которые регламентируют требования к обработке персональных данных:

1.5.1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ, статья 137 «Нарушение неприкосновенности частной жизни».

1.5.2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ, статья 13.11 «Нарушение законодательства Российской Федерации в области персональных данных».

1.5.3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ, глава 14 «Защита персональных данных работника».

1.5.4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.5.5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – закон № 152-ФЗ).

1.5.6. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации от 15.09.2008 № 687.

1.5.7. Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденное постановлением Правительства Российской Федерации от 16.03.2009 № 228.

1.5.8. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

1.5.9. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом

Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 18.02.2013 № 21.

1.5.10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденные приказом Федеральной службы безопасности Российской Федерации (далее – ФСБ России) от 10.07.2014 № 378.

1.5.11. Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 14.12.2012 «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве».

1.5.12. Политика ФГАОУ ВО «Севастопольский государственный университет» в отношении обработки персональных данных, утверждена приказом временно исполняющего обязанности ректора от 12.03.2025 № 512-п.

1.6. В настоящем Положении используются термины и определения в соответствии с Федеральным законом «О персональных данных», а также следующие термины и определения:

1.6.1. Средство вычислительной техники (СВТ) – персональная ЭВМ с установленной операционной системой и офисным программным обеспечением общего назначения.

1.6.2. Информационная система – программно-аппаратный комплекс, предназначенный для автоматизации определенного вида деятельности Университета.

1.6.3. СЗИ – средства защиты информации, имеющие действующие сертификаты соответствия, выданные ФСБ России для средств криптографической защиты информации и выданные ФСТЭК России для иных средств защиты информации.

1.6.4. Защищенная вычислительная среда – совокупность операционной системы, программ общего назначения и СЗИ, реализующих требования к защите ПД на СВТ.

1.6.5. ДИС – Дирекция информатизации и связи.

2. Организация обработки персональных данных

2.1. Ответственность за общую организацию обработки ПД в Университете несет лицо, назначенное организационно-распорядительным документом в соответствии с требованиями статьи 22.1 Закона № 152-ФЗ (далее – Лицо, ответственное за организацию обработки ПД). Лицо, ответственное за организацию обработки ПД, получает указания

непосредственно от ректора и подотчетно ректору. Ректор вправе делегировать свои полномочия в части обработки ПД проректорам и другим работникам Университета в соответствии с пунктом 4.59 Устава ФГАОУ ВО «Севастопольский государственный университет», утвержденного приказом Минобрнауки России от 28.12.2018 № 1382.

2.2. Лицо, ответственное за организацию обработки ПД, несет ответственность за соблюдение сроков выполнения действий, предусмотренных Законом № 152-ФЗ, в случаях поступления обращений от субъектов ПД, их представителей и запросов от Роскомнадзора в соответствии с приложением № 1 к настоящему Положению.

2.3. Центрами ответственности за обработку ПД на всех этапах жизненного цикла обрабатываемых ПД являются структурные подразделения Университета.

2.4. Ответственность за организацию обработки ПД в структурных подразделениях Университета несет руководитель соответствующего структурного подразделения.

2.5. В случае реорганизации структурных подразделений Университета вышестоящий руководитель принимает решение о передаче обрабатываемых ПД в другое структурное подразделение или, при необходимости, об уничтожении или обезличивании обрабатываемых ПД. Уничтожение ПД выполняется согласно актуальным Правилам уничтожения ПД. По результатам выполненных работ составляются Акты, которые подписываются исполнителями, согласуются Лицом, ответственным за организацию обработки ПД, и утверждаются вышестоящим руководителем.

2.6. Структурные подразделения Университета регулярно, не реже одного раза в год, планируют и проводят мероприятия по проведению внутреннего контроля действий работников на соответствие требованиям нормативных и иных документов в области защиты ПД. Перечень планируемых мероприятий определяет руководитель соответствующего структурного подразделения Университета. Результаты контроля, а также перечень мер, принятых по результатам контроля, отражаются в отчетах о проведении внутреннего контроля, копии которых направляются Лицу, ответственному за организацию обработки ПД.

2.7. Лицо, ответственное за организацию обработки ПД, проводит дистанционный контроль соблюдения требований по защите ПД путем анализа представленных структурными подразделениями отчетов и, при необходимости, лично проводит проверку состояния информационной безопасности в структурных подразделениях Университета. Проведение таких проверок Лицом, ответственным за организацию обработки ПД, санкционируется ректором или уполномоченным им лицом.

2.8. Ответственность за неисполнение или ненадлежащее исполнение требований законодательства Российской Федерации в области защиты ПД несет каждое лицо, имеющее доступ к соответствующим ПД. Лица,

получившие доступ к ПД, обязаны не раскрывать третьим лицам и не распространять ПД без согласия субъекта ПД, если иное не предусмотрено федеральными законами.

2.9. При обработке ПД каждое структурное подразделение Университета обязано:

2.9.1. Ознакомить под подпись в листах ознакомления лиц, непосредственно осуществляющих обработку ПД, с положениями законодательства Российской Федерации о ПД, в том числе требованиями к защите ПД, Политикой ФГАОУ ВО «Севастопольский государственный университет» в отношении обработки ПД, настоящим Положением, иными локальными нормативными актами Университета по вопросам обработки ПД (актуальный перечень документов для ознакомления размещается на официальном сайте Университета).

2.9.2. Информировать лиц, осуществляющих обработку ПД, о факте обработки ими ПД, в том числе с использованием информационных систем ПД, категориях, обрабатываемых ПД, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми и иными актами;

2.9.3. Утвердить и поддерживать в актуальном состоянии Перечни лиц, осуществляющих обработку ПД либо имеющих к ним доступ;

2.9.4. При обнаружении фактов несанкционированного доступа к ПД направлять Лицу, ответственному за организацию обработки ПД, сведения об обнаруженных фактах и о мерах, принятых в отношении таких фактов;

2.9.5. Не допускать фиксации на одном материальном носителе информации ПД, цели обработки которых заведомо не совместимы.

2.10. Обязанность предоставления доказательства получения согласия субъекта ПД на обработку его ПД или на передачу его ПД третьим лицам, в том числе полученных в электронном виде, возлагается на структурное подразделение, в котором такие согласия хранятся.

2.11. Лица, допущенные к обработке ПД, должны знать:

- цели, для которых собираются или собраны ПД;
- места хранения обрабатываемых ими ПД;
- критерии достижения целей обработки обрабатываемых ими ПД;
- срок или условие прекращения обработки обрабатываемых ими ПД;
- правовые основания обработки ПД;
- необходимость получения согласия субъекта ПД в письменной, электронной или иной форме для обрабатываемых ПД;
- необходимость уведомления субъекта ПД о факте обработки его ПД.

3. Жизненный цикл обработки персональных данных

3.1. Жизненный цикл обработки ПД в структурных подразделениях Университета, состоит из трех этапов.

Первый этап – самостоятельный сбор ПД структурным подразделением Университета либо получение ПД от другого структурного подразделения.

Второй этап – обработка ПД, в том числе хранение, передача для обработки другим структурным подразделениям Университета.

Третий этап – уничтожение или обезличивание ПД.

3.2. Необходимость самостоятельного сбора ПД для новых целей сбора ПД структурные подразделения Университета согласуют с Лицом, ответственным за организацию обработки ПД, путем направления информации на официальную электронную почту лица, назначенного ответственным за организацию обработки ПД.

3.3. Лицо, ответственное за организацию обработки ПД, вправе запросить у структурных подразделений сведения, предусмотренные частью 3 статьи 22.1 Закона № 152-ФЗ.

4. Передача персональных данных

4.1. Передача ПД из одного структурного подразделения в другое допускается только между лицами, допущенными к обработке соответствующих ПД, и должна быть санкционирована устно или письменно руководителями соответствующих структурных подразделений.

4.2. При передаче ПД работниками Университета должны быть соблюдены следующие требования:

- не сообщать ПД субъекта третьей стороне без письменного согласия субъекта ПД, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПД, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

- предупреждать лиц, получающих ПД субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных ПД;

- не сообщать ПД субъекта в коммерческих целях без его письменного согласия;

- передавать ПД субъекта представителям субъектов ПД в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми ПД субъекта которые необходимы для выполнения указанными представителями их функций;

- не отвечать на вопросы, связанные с передачей ПД субъекта по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими работниками своих непосредственных должностных обязанностей, адресатам в чью компетенцию входит получение такой информации.

4.3. Передача ПД для обработки другим юридическим и физическим лицам, а также получение ПД для обработки от других юридических и физических лиц возможны только в следующих случаях:

– в соответствии с договорами (контрактами) о поручении обработки ПД, заключенных с соблюдением требований частей 3, 4, 5 статьи 6 Закона № 152-ФЗ, при наличии согласий субъектов ПД на передачу их ПД;

– для осуществления и выполнения возложенных законодательством Российской Федерации на Университет функций, полномочий и обязанностей, в том числе в соответствии с трудовым, налоговым, пенсионным законодательством, законодательством о социальной защите, о воинском учете и др. без необходимости получения согласий субъектов ПД;

– для исполнения договоров, стороной которых либо выгодоприобретателями или поручителями по которым являются субъекты ПД, без необходимости получения согласия субъектов ПД, ПД которых передаются, включая направление сведений в коммерческие банки для зачисления денежных средств на личные зарплатные или студенческие карты, выпущенные на основании договоров между банками и субъектами ПД или между банками и Университетом в интересах субъектов ПД.

4.4. В целях обеспечения контроля правомерности использования переданных по запросам ПД лицами, их получившими, сведения о лице, направившем запрос, дата передачи ПД или дата уведомления об отказе в их предоставлении, а также состав переданной информации фиксируются в Журнале учета передачи персональных данных. Форма такого Журнала утверждена локальным актом Университета.

5. Хранение и использование ПД субъекта ПД

5.1. Хранение ПД должно осуществляться в форме, позволяющей определить субъекта ПД Университета, не дольше, чем этого требуют цели обработки ПД, если срок хранения ПД не установлен федеральным законом, договором, стороной которого является субъект ПД. Обрабатываемые ПД подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Хранение ПД субъекта ПД Университета может осуществляться на бумажных и машинных носителях, доступ к которым ограничен списком лиц, допущенных к обработке ПД.

5.2. Все машинные носители ПД подлежат учету. Форма Журнала учета машинных носителей персональных данных утверждается локальным актом Университета.

5.3. ПД субъектов ПД, содержащиеся на машинных носителях ПД, должны храниться на автоматизированных рабочих местах и серверах информационных систем ПД Университета, установленных в пределах помещений, утвержденных Приказом об обеспечении безопасности помещений, в которых размещены информационные системы ПД.

5.4. ПД субъектов ПД, содержащиеся на материальных носителях ПД, должны храниться в пределах помещений, утвержденных Приказом об обеспечении безопасности материальных носителей персональных данных.

5.5. Хранение ПД субъектов ПД должно происходить в порядке, исключающем их утрату или неправомерное использование.

5.6. Использование ПД субъектов ПД Университетом осуществляется исключительно в целях выполнения требований законодательства Российской Федерации, включая трудовое законодательство, а также для выполнения функций, полномочий и обязанностей, возложенных на Университет в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации.

5.7. Обработка ПД субъектов ПД Университета осуществляется только специально уполномоченными лицами, перечень которых утверждается приказом Университета, при этом указанные в приказе работники должны иметь право получать только те ПД субъекта, которые необходимы для выполнения непосредственных должностных обязанностей.

5.8. Лица, осуществляющие обработку ПД без использования средств автоматизации (в том числе работники Университета или лица, осуществляющие такую обработку по договору с Университетом), должны быть проинформированы о факте обработки ими ПД, обработка которых осуществляется Университетом без использования средств автоматизации, категориях обрабатываемых ПД, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными нормативными актами организации.

5.9. Передача ПД субъектов ПД между структурными подразделениями Университета осуществляется только между работниками, включенными в перечень лиц, имеющих доступ к ПД.

5.10. Обработка ПД субъектов ПД должна осуществляться как в виде документов на бумажных носителях, так и в электронном виде (файлы, базы данных) и только в пределах помещений Университета.

5.11. Университет вправе поручить обработку ПД субъекта ПД другим юридическим или физическим лицам на основании договора (далее – поручение) с согласия субъекта ПД, если иное не предусмотрено Законом № 152-ФЗ. Лицо, осуществляющее обработку ПД по поручению Университета, обязано соблюдать принципы и правила обработки ПД, предусмотренные Федеральным законом № 152-ФЗ.

5.12. Работники Университета и иные лица, получающие доступ к ПД, обязаны не раскрывать третьим лицам и не распространять ПД без согласия субъектов ПД, если иное не предусмотрено федеральным законодательством в сфере защиты ПД.

6. Уничтожение (обезличивание) персональных данных

6.1. Структурные подразделения Университета обязаны уничтожить либо обезличить обрабатываемые, в том числе хранимые, ПД в следующих случаях:

- при достижении целей обработки ПД;
- при утрате необходимости в достижении целей обработки ПД;
- при поступлении отзыва согласия субъекта ПД на обработку его ПД, если нет других законных оснований для обработки ПД;
- если стало известно, что ПД являются неполными, устаревшими, неточными, при невозможности их уточнения;
- если стало известно, что ПД являются незаконно полученными;
- если стало известно, что ПД не являются необходимыми для заявленной цели обработки ПД.

В случае, когда к ПД имеют доступ несколько структурных подразделений Университета, за уничтожение либо обезличивание ПД несет ответственность структурное подразделение, производившее сбор таких ПД.

6.2. Уничтожение либо обезличивание ПД выполняется путем:

- уничтожения, разрушения материального носителя ПД способом, не позволяющим восстановить находящиеся на нем ПД;
- вымарывания ПД на бумажных носителях;
- гарантированного стирания ПД на машинных носителях информации или полного форматирования машинных носителей информации.

6.3. Уничтожение ПД выполняют лица, допущенные к обработке уничтожаемых ПД. В случае, когда лица, допущенные к обработке уничтожаемых ПД, не могут самостоятельно уничтожить ПД, в их присутствии уничтожение производят иные лица, без возможности ознакомления с уничтожаемыми ПД.

7. Использование средств вычислительной техники для обработки персональных данных

7.1. Обработка ПД на СВТ, не оснащенных СЗИ, не допускается.

7.2. Обработка ПД на СВТ, оснащенных СЗИ с истекшим сроком действия сертификата соответствия, не допускается.

7.3. Используемые СЗИ должны обеспечивать реализацию мер по обеспечению безопасности ПД, необходимых для обеспечения требуемого уровня защищенности ПД, указанных в Составе и содержании организационных и технических мер по обеспечению безопасности ПД при их обработке в информационных системах ПД, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

7.4. Перечень СЗИ, закупаемых и применяемых в Университете для защиты ПД, согласуется с ДИС и утверждается директором ДИС.

7.5. Ответственность за ненадлежащую организацию оснащения СВТ необходимыми СЗИ, их настройки, подключения к информационно-телекоммуникационной сети несет руководитель структурного подразделения, ответственного за создание и/или обслуживание соответствующих СВТ.

7.6. Ответственность за ненадлежащую организацию замены СЗИ с истекшим сроком действия сертификата соответствия на СЗИ с актуальным сроком несет руководитель структурного подразделения, ответственного за обслуживание соответствующих СВТ.

7.7. Требования по защите ПД, обрабатываемых с использованием СВТ, реализуются на СВТ защищенной вычислительной средой. ПД могут обрабатываться как с использованием информационных систем ПД, так и с использованием офисного программного обеспечения общего назначения.

7.8. Работники ДИС не реже, чем один раз в три года, планируют и проводят оценку эффективности реализованных в рамках системы защиты ПД мер по обеспечению безопасности ПД для эксплуатируемых видов защищенной вычислительной среды, по результатам которых оформляется Акт.

7.9. Пользователям СВТ запрещается самовольно вносить изменения в конфигурацию и настройки СЗИ, а также самовольно подключать устройства в информационно-телекоммуникационную сеть, предназначенную для обработки, хранения и/или передачи ПД.

7.10. В случае, если эксплуатационная документация на информационную систему ПД предполагает назначение лица, ответственного за администрирование СЗИ (администратора информационной безопасности), его функции выполняет лицо, назначенное администратором такой информационной системы ПД.

7.11. В Дирекции комплексной безопасности назначается должностное лицо (работник), ответственный за обеспечение безопасности ПД в информационной системе контроля и управления доступом.

7.12. Пользователи СВТ обязаны соблюдать правила пользования СЗИ при эксплуатации СВТ.

7.13. Ответственность за ненадлежащую организацию физического доступа к СВТ, невыполнение требований к помещениям и оснащению рабочих мест несут руководители соответствующих эксплуатирующих структурных подразделений. Требования к помещениям определяются Положением об организации пропускного и внутриобъектового режимов на объектах ФГАОУ ВО «Севастопольский государственный университет».

7.14. Ответственность за предоставление логического доступа к информационным системам несут работники, выполняющие администрирование соответствующих СВТ и информационных систем.

7.15. Документами, определяющими перечень лиц, доступ которых к ПД, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей, являются Заявки на предоставление доступа к соответствующей информационной системе.

7.16. Утвержденные Заявки хранятся у администраторов, предоставляющих доступ к соответствующим информационным системам.

7.17. Выполнение пусконаладочных, сервисных и ремонтных работ лицами, не допущенными к обработке ПД, разрешается только в информационных системах, не содержащих ПД либо без предоставления доступа таким лицам к хранящимся в информационных системах ПД.

7.18. Обязанность предоставления доказательств получения согласий субъектов ПД на обработку их ПД, полученных в электронной форме, а также обязанность архивного хранения согласий, полученных в электронной форме, возлагается на администратора информационной системы ПД, в которой такие согласия собраны. В случае вывода такой информационной системы ПД из эксплуатации и продолжения обработки собранных ПД, директор ДИС принимает решение об организации хранения архивных копий согласий субъектов ПД, собранных в электронной форме, и предоставлении доказательств получения указанных согласий.

7.19. В случае необходимости передачи сторонней организации в ремонт или утилизацию технического средства или машинного носителя информации, содержащего ПД, передающие работники обязаны уничтожить или обезличить ПД, хранящиеся на носителях ПД.

8. Обеспечение конфиденциальности персональных данных

8.1. В соответствии с пунктом 1 Перечня сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 06.03.1997 № 188, ПД относятся к конфиденциальной информации.

8.2. Конфиденциальность ПД при их обработке в Университете обеспечивается:

8.2.1. Установлением и поддержанием в актуальном состоянии Перечня лиц, осуществляющих обработку ПД либо имеющих к ним доступ, в том числе с использованием информационных систем ПД.

8.2.2. Обязанностью лиц, допущенных к обработке ПД, не раскрывать третьим лицам и не распространять ПД без согласия субъекта ПД, если иное не предусмотрено федеральным законом, в соответствии с требованиями статьи 7 Закона № 152-ФЗ.

8.2.3. Обеспечением режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях, где обрабатываются, в том числе хранятся, ПД.

8.2.4. Определением мест хранения ПД.

8.2.5. Учетом машинных носителей ПД.

8.2.6. Применением для защиты ПД в информационных системах ПД и информационно-вычислительных сетях СЗИ, прошедших в установленном порядке процедуру оценки соответствия.

8.2.7. Использованием средств криптографической защиты информации для организации каналов связи, предназначенных для передачи ПД, между обособленными подразделениями Университета, а также другими предприятиями и организациями.

8.3. Обеспечение сохранности материальных носителей ПД при их хранении.

8.3.1. Структурные подразделения Университета при хранении ПД самостоятельно определяют условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ, исходя из количества носителей ПД и необходимой технологии их обработки.

8.3.2. Для обеспечения таких условий могут применяться следующие меры:

- хранение носителей ПД в надежно запираемых сейфах, металлических шкафах, предметах мебели, ключи от которых доступны только лицам, допущенным к обработке соответствующих ПД;

- хранение носителей ПД в закрывающихся предметах мебели, оборудованных средствами контроля за их вскрытием, например, с использованием металлических печатей для пластилина. Нахождение посторонних лиц в помещениях, где расположены такие места хранения носителей ПД, допускается только в присутствии лиц, имеющих рабочие места в помещении, или их прямых руководителей;

- хранение носителей ПД в открытых предметах мебели при ограничении доступа посторонних лиц в помещение или в отгороженную зону помещения, где находятся места хранения носителей ПД;

- иные, согласованные с лицом, ответственным за организацию обработки ПД, меры, позволяющие обеспечить условия сохранности ПД.

8.3.3. Перечень реализуемых мер утверждается руководителем соответствующего структурного подразделения Университета в письменной форме.

8.3.4. Ответственность за отсутствие утвержденного перечня необходимых мер, их реализации и контроля за их соблюдением несет руководитель соответствующего структурного подразделения Университета.

8.3.5. Ответственность за несоблюдение утвержденных мер, а также за хранение ПД вне предусмотренных для этого мест, несет лицо, обрабатывающее соответствующие ПД.

8.4. Передача сведений, содержащих ПД, юридическим и физическим лицам.

8.4.1. На документах, содержащих ПД, передаваемых юридическим и физическим лицам, должна проставляться пометка «Конфиденциально» или «Содержит персональные данные».

8.4.2. ПД могут быть направлены юридическим и(или) физическим лицам только при наличии конкретных, заранее определенных и законных целей. Передаче подлежат только ПД, которые отвечают заявленным целям их обработки и не должны быть избыточными по отношению к заявленным целям их обработки.

8.4.3. Пересылка информации, содержащей ПД, юридическим и физическим лицам должна осуществляться следующими способами.

8.4.3.1. В бумажном виде:

- доставка лично нарочным на бумажных носителях информации лично адресату;
- доставка в конвертированном виде через почтовые службы, в том числе отделения связи Министерства связи, спецсвязь.

8.4.3.2. В электронном виде:

- доставка лично нарочным на электронных носителях информации лично адресату;
- по защищенным с применением прошедших в установленном порядке процедуру оценки соответствия средств криптографической защиты информации каналам передачи данных, не принадлежащих Университету;
- с использованием прошедшей в установленном порядке процедуру оценки соответствия защищенной электронной почты, в том числе с использованием программы VipNet Client Деловая почта;
- в зашифрованном виде с применением квалифицированной электронной подписи по открытым каналам связи, в том числе с использованием официальной электронной почты Университета;
- с использованием Системы межведомственного электронного взаимодействия (СМЭВ);
- с использованием государственных информационных систем (ГИС).

8.4.4. Документы, полученные от юридических и физических лиц, содержащие ПД, обрабатываются в Университете в соответствии с требованиями законодательства РФ о ПД и настоящего Положения. По окончании обработки поступивших документов такие документы уничтожаются способом, не позволяющим восстановить ПД, либо ПД, содержащиеся в них, вымарываются.

8.5. Предоставление ответов о подтверждении документов об образовании российского образца.

8.5.1. Университет направляет информацию о документах об образовании и (или) о квалификации, документах об обучении российского образца в федеральную информационную систему «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» и, при необходимости, органу исполнительной власти субъекта Российской Федерации.

8.5.2. Университет не предоставляет юридическим и физическим лицам сведения о документах об образовании и (или) о квалификации, документах об обучении российского образца.

8.5.3. Юридические и физические лица получают сведения о выданных документах об образовании и (или) о квалификации, документах об обучении российского образца в соответствии с требованиями постановления Правительства Российской Федерации от 31.05.2021 № 825 «О федеральной информационной системе «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении»» на официальном сайте Рособнадзора по ссылке в сети Интернет http://obrnadzor.gov.ru/ru/activity/main_directions/reestr_of_education/.

8.5.4. Юридические и физические лица могут получать подтверждения фактов проставления апостилей на официальном сайте Рособнадзора в Федеральной базе данных об апостилях, проставленных на документах государственного образца об образовании, об ученых степенях и ученых званиях по ссылке в сети Интернет http://obrnadzor.gov.ru/ru/activity/main_directions/confirmation_of_documents/.

8.6. Предоставление сведений, содержащих ПД субъектов ПД, по запросам юридических и физических лиц, в том числе сведений о выданных документах об образовании и (или) о квалификации, документах об обучении украинского образца.

8.6.1. Юридические и физические лица получают в Университете сведения, содержащие ПД, только в случае предоставления согласия субъекта ПД на передачу его ПД соответствующему юридическому или физическому лицу в любой позволяющей подтвердить факт получения такого согласия форме.

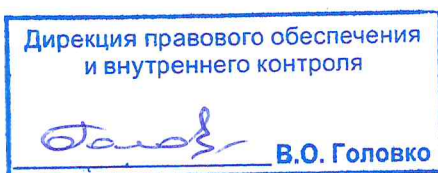
8.6.2. Структурное подразделение Университета, предоставившее ПД третьим лицам, обязано сохранять согласия субъектов ПД на передачу их ПД третьим лицам в течение 3 (трех) лет после истечения срока действия согласия или его отзыва, если иное не предусмотрено федеральным законом, договором (согласно пункту 441 Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения, утвержденному приказом Росархива от 20.12.2019 № 236), с целью предоставления доказательства в соответствии с требованиями части 3 статьи 9 Закона № 152-ФЗ, за исключением случаев, когда данные предоставляются по запросам органов, осуществляющих деятельность в рамках настоящего согласия, позволяющей запрашивать ПД без согласия субъекта ПД.

9. Заключительные положения

9.1. Настоящее Положение вступает в силу с момента его утверждения приказом ректора Университета.

9.2. Внесение изменений и дополнений в настоящее Положение осуществляется путем подготовки изменений или проекта Положения в новой редакции и утверждения его в установленном порядке.

9.3. Настоящее Положение подлежит регистрации и хранению подлинного экземпляра в составе документов организационного характера номенклатуры дел отдела делопроизводства и архивного обеспечения Дирекции административных процессов. Заверенная копия Положения подлежит хранению в Дирекции информатизации и связи.



**Сводная таблица действий в ответ на обращения
субъектов персональных данных, их представителей
и запросы Роскомнадзора**

Обращение, запрос	Действия	Срок, не более	Форма ответа
Наличие ПД	Предоставление информации о наличии ПД	10 раб. дней с даты получения запроса (согласно ч. 1 ст. 20 Закона № 152-ФЗ)	Информация о наличии ПД в порядке, предусмотренном статьей 14 Закона № 152-ФЗ
	Отказ от предоставления информации о наличии ПД	10 раб. дней со дня обращения субъекта ПД (согласно ч. 2 ст. 20 Закона № 152-ФЗ)	Мотивированный ответ об отказе в письменной форме.
Ознакомление с ПД	Предоставление возможности ознакомления с ПД	10 раб. дней с даты получения запроса (согласно ч. 1 ст. 20 Закона № 152-ФЗ)	Предоставление возможности ознакомления с ПД
	Отказ от предоставления информации о наличии ПД	10 раб. дней со дня обращения субъекта ПД (согласно ч. 2 ст. 20 Закона № 152-ФЗ)	Мотивированный ответ в письменной форме об отказе в предоставлении информации о наличии ПД
ПД являются неточными	Блокирование ПД	С момента обращения субъекта ПД о неточности его ПД или с момента получения запроса на период проверки (согласно ч. 1 ст. 21 Закона № 152-ФЗ)	Уведомление о внесенных изменениях
	Уточнение ПД и снятие блокировки ПД	7 рабочих дней со дня предоставления уточненных сведений (согласно ч. 2 ст. 21, а также ч. 3 ст. 20 Закона № 152-ФЗ)	

Дирекция правового обеспечения
и внутреннего контроля



В.О. Головки

*Положение об обработке персональных данных
в ФГАОУ ВО «Севастопольский государственный университет»*

Обращение, запрос	Действия	Срок, не более	Форма ответа
ПД являются неполными или неактуальными	Изменение ПД	7 рабочих дней со дня предоставления уточняющих сведений (согласно ч. 3 ст. 20 Закона № 152-ФЗ)	Уведомление о внесенных изменениях
ПД являются незаконно полученными или не являются необходимыми для заявленной цели обработки	Уничтожение ПД	7 рабочих дней со дня предоставления сведений о незаконном получении ПД или отсутствии необходимости ПД для заявленной цели обработки (согласно ч. 3 ст. 20 Закона № 152-ФЗ)	Уведомление о внесенных изменениях и предпринятых мерах
Отзыв согласия на обработку ПД, если нет иных оснований продолжать обработку ПД	Прекращение обработки и уничтожение ПД	30 дней с даты поступления отзыва (согласно ч. 5 ст. 21 Закона № 152-ФЗ)	Уведомление не требуется
	Невозможность уничтожения ПД в течение 30 рабочих дней - Блокирование и уничтожение ПД	6 месяцев (согласно ч. 6 ст. 21 Закона № 152-ФЗ)	
Неправомерность действий с ПД	Блокирование ПД	С момента обращения на период проверки (согласно ч. 1 ст. 21 Закона № 152-ФЗ)	Уведомление о результатах выполненных действий
	Прекращение неправомерной обработки ПД	3 рабочих дня с даты выявления (согласно ч. 3 ст. 21 Закона № 152-ФЗ)	
	Уничтожение ПД в случае невозможности обеспечения правомерности обработки ПД	10 рабочих дней с даты выявления (согласно ч. 3 ст. 21 Закона № 152-ФЗ)	
	Невозможность уничтожения ПД в течение 10 рабочих дней - Блокирование и уничтожение ПД	6 месяцев (согласно ч. 6 ст. 21 Закона № 152-ФЗ)	

Обращение, запрос	Действия	Срок, не более	Форма ответа
Достижение цели обработки ПД, если нет иных оснований для обработки ПД	Прекращение обработки ПД и уничтожение ПД	30 дней с даты достижения цели обработки ПД (согласно ч. 4 ст. 21 Закона № 152-ФЗ)	Уведомление не требуется
	Невозможность уничтожения ПД в течение 30 рабочих дней - Блокирование и уничтожение ПД	6 месяцев (согласно ч. 6 ст. 21 Закона № 152-ФЗ)	
Информация для осуществления деятельности Роскомнадзора	Предоставление затребованной информации по ПД	10 раб. дней (согласно ч. 4 ст. 20 Закона № 152-ФЗ)	Предоставление затребованной информации по ПД в Роскомнадзор

Дирекция правового обеспечения
и внутреннего контроля

 В.О. Головки

Положение об обработке персональных данных
в ФГАОУ ВО «Севастопольский государственный университет»