**Министерство науки и высшего образования Российской Федерации** Федеральное государственное автономное образовательное учреждение высшего образования

**«Самарский государственный экономический университет»**

**ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ (АДМИНИСТРАТОРА БЕЗОПАСНОСТИ)**

**В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ АВТОНОМНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

Самара

2022 год

**СОДЕРЖАНИЕ**

[ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ 3](#_Toc54025103)

[1 Общие положения 4](#_Toc54025104)

[2 Нормативно-правовая база 5](#_Toc54025105)

[3 Должностные обязанности администратора безопасности ПДн 6](#_Toc54025106)

[4 Права и ответственность ответственного за обеспечение безопасности ПДн 9](#_Toc54025107)

[5 ЛИСТ ОЗНАКОМЛЕНИЯ 10](#_Toc54025108)

# ИСПОЛЬЗУЕМЫЕ ****СОКРАЩЕНИЯ****

|  |  |  |
| --- | --- | --- |
| АРМ | – | Автоматизированное рабочее место |
| АРМ ИСПДн  | – | Информационная система персональных данных |
| НСД | – | Несанкционированный доступ |
| ПДн | – | Персональные данные |
| РФ | – | Российская Федерация |
| СЗИ | – | Средство защиты информации |
| Университет | – | Федеральное государственное автономное образовательное учреждение высшего образования «Самарский государственный экономический университет» |
| ФСБ России | – | Федеральная служба безопасности России |
| ФСТЭК России | – | Федеральная служба по техническому и экспортному контролю России |

1. Общие положения

Настоящая инструкция ответственного за обеспечение безопасности персональных данных (администратора безопасности ПДн) в Федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет» (далее – ФГАОУ ВО «СГЭУ», Университет) определяет общие функции, права и обязанности ответственного сотрудника ФГАОУ ВО «СГЭУ» по вопросам обеспечения информационной безопасности ПДн при их обработке в АРМ информационных системах персональных данных (далее –АРМ АРМ ИСПДн) ФГАОУ ВО «СГЭУ».

Администратор безопасности ПДн в ФГАОУ ВО «СГЭУ» назначается Приказом Ректора Университета и является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники АРМ ИСПДн Университета.

Методическое руководство работой администратора безопасности ПДн в части защиты ПДн осуществляется лицом, ответственным за организацию обработки ПДн в ФГАОУ ВО «СГЭУ».

Администратор безопасности ПДн в ФГАОУ ВО «СГЭУ» выполняет работы по обеспечению безопасности ПДн в соответствии с указаниями лица, ответственного за организацию обработки ПДн в ФГАОУ ВО «СГЭУ», должностными обязанностями, данной Инструкцией, организационно-распорядительными документами Университета и нормативными документами Российской Федерации (далее – РФ) в области обработки и защиты Пдн.

1. Нормативно-правовая база

Настоящая инструкция разработана в соответствии со следующими нормативно-правовыми актами РФ:

* Федеральный закон от 30 декабря 2001 года № 197 «Трудовой кодекс Российской Федерации»;
* Федеральный закон 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 27 июля 2006 года № 152 «О персональных данных»;
* Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания 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».
1. Должностные обязанности администратора безопасности ПДн

Основными задачами администратора безопасности ПДн в ФГАОУ ВО «СГЭУ» являются:

* сопровождение средств защиты информации (в том числе криптографических) (далее – СЗИ) и защита от несанкционированного доступа (далее – НСД) основных технических средств и систем;
* организация разграничения доступа к АРМ ИСПДн Университета;
* контроль эффективности применяемых мер защиты информации.

Для выполнения поставленных задач на администратора безопасности ПДн возлагаются следующие функции:

* допуск пользователей к техническим, программным средствам и информационным ресурсам АРМ ИСПДн Университета в соответствии с требованиями внутренних регламентов Университета;
* участие на стадии проектирования (внедрения) АРМ ИСПДн Университета в разработке технологии обработки ПДн по вопросам:
* организация порядка учета, хранения и обращения с документами и материальными носителями информации;
* подготовки инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей АРМ ИСПДн Университета по вопросам защиты информации, а также ответственных по защите информации в процессе автоматизированной обработки информации;
* сопровождение СЗИ, в том числе средств криптографической защиты информации, на стадии эксплуатации АРМ ИСПДн Университета, включая ведение служебной информации СЗИ (управление ключевой системой, сопровождение правил разграничения доступа), оперативный контроль за функционированием СЗИ;
* контроль выполнения требований действующих нормативных документов по вопросам обеспечения безопасности ПДн.

Для реализации поставленных задач и возложенных функций администратор безопасности ПДн обязан:

* вести журнал учета эксплуатационной и технической документации СЗИ в АРМ ИСПДн Университета;
* вести журнал учета средств криптографической защиты информации, применяемых в АРМ ИСПДн Университета;
* вести журнал учета машинных носителей, содержащих ПДн;
* вести журнал передачи материальных носителей ПДн;
* вести журнал регистрации и учета электронных носителей ПДн и иной конфиденциальной информации;
* вести журнал выдачи/сдачи электронных носителей ПДн и иной конфиденциальной информации.
* осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на автоматизированных рабочих местах (далее – АРМ) специальных программных и программно-аппаратных СЗИ;
* присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств, защищенных АРМ и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств АРМ ИСПДн Университета;
* периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование);
* проводить периодический инструктаж пользователей АРМ ИСПДн Университета по правилам работы с используемыми средствами и системами зашиты информации;
* участвовать в определении перечня защищаемых информационных ресурсов.
* участвовать в определении режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, кодирование файлов, подключение дополнительных алгоритмов криптографической защиты;
* участвовать в разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита;
* осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ ИСПДн Университета;
* контролировать и требовать соблюдения установленных правил по организации парольной защиты в АРМ ИСПДн Университета;
* принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и АРМ ИСПДн Университета;
* обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт (контролировать стирание информации на съемных носителях);
* проводить работу по выявлению возможности вмешательства в процесс функционирования АРМ ИСПДн Университета и осуществления НСД к информации и техническим средствам АРМ;
* участвовать в расследовании инцидентов информационной безопасности.

Администратору безопасности ПДн в ФГАОУ ВО «СГЭУ» запрещается:

* используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;
* использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий;
* передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки;
* производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы АРМ ИСПДн Университета, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей;
* нарушать правила эксплуатации оборудования АРМ ИСПДн Университета;
* корректировать, удалять, подменять журналы аудита.
1. Права и ответственность администратора безопасности ПДн

Администратор безопасности ПДн в ФГАОУ ВО «СГЭУ» имеет право:

* получать доступ к программным и аппаратным средствам АРМ ИСПДн Университета, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах Университета и АРМ пользователей;
* требовать от пользователей АРМ ИСПДн Университета выполнения инструкций по обеспечению безопасности информации в АРМ ИСПДн Университета;
* участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов АРМ ИСПДн Университета;
* осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;
* производить анализ защищенности АРМ ИСПДн Университета путем применения специального программного обеспечения, осуществления попыток взлома системы защиты АРМ ИСПДн Университета;
* вносить свои предложения по совершенствованию мер защиты в АРМ ИСПДн Университета.

Администратор безопасности (ответственный за обеспечение безопасности) ПДн в ФГАОУ ВО «СГЭУ» несет ответственность за:

* реализацию принятых Университетм организационно-распорядительных документов, определяющих политику информационной безопасности;
* программно-технические и криптографические средства защиты информации, средства вычислительной техники, сети обработки информации и АРМ ИСПДн Университета;
* разглашение сведений конфиденциального характера.
1. ЛИСТ ОЗНАКОМЛЕНИЯ

|  |  |  |
| --- | --- | --- |
| **ФИО** | **Должность** | **Подпись, дата** |
|  |  |  |