Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Колледж «Звёздный»

ПРИНЯТ
Педагогическим советом
СПб ГБ ПОУ
«Колледж «Звёздный»
Протокол от «31» 08 2022 года № 11

УТВЕРЖДЕН
Приказом СПб ГБ ПОУ
«Колледж «Звёздный»

от «01» 09 2022 года № 69«А»-О

ЛОКАЛЬНЫЙ АКТ № 120

Положение о порядке организации и проведения работ по защите персональных данных в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Колледж «Звёздный»

X Документ подписан электр...
Пантелеенко Римма Александровна
Директор
Подписано: Пантелеенко Римма Александровна

Санкт-Петербург
2022

1. Термины, определения и сокращения

Администратор ИБ ИСПДн (Администратор ИБ) – назначенный приказом работник, который согласно своей инструкции отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах эксплуатации и модернизации.

Администратор по обработке ПДн в ИСПДн (Администратор ИСПДн) – назначенный приказом работник, который согласно своей инструкции отвечает за поддержание установленного уровня безопасности объектов защиты.

Аутентификация – процедура проверки принадлежности субъекту доступа предъявленного им идентификатора.

Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, при которых обработка необходима для уточнения ПДн).

Вредоносное программное обеспечение – программное обеспечение заведомо созданное для воздействия на информацию или активы информационной системы, и (или) получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети, использования ресурсов ЭВМ; причинения вреда (нанесения ущерба) владельцу информации, и (или) владельцу ЭВМ, и (или) владельцу сети ЭВМ;

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Информационная безопасность (ИБ) - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение "Колледж "Звездный", а также транспортных средств.

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн).

Субъект персональных данных (Субъект ПДн) – физическое лицо, к которому относятся ПДн.

Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в ИСПДн.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

2. Общие положения

2.1. Настоящее Положение о порядке организации и проведении работ по защите персональных данных (далее – положение) устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности ПДн при их обработке в организации.

2.2. Настоящее положение разработано в соответствии с действующим законодательством РФ, в том числе в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»

(далее – Федеральный закон № 152-ФЗ);

- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.3. Действие настоящего положения распространяется на всех работников, выполняющих обработку ПДн в ИСПДн. Работники СПб ГБ ПОУ "Колледж "Звездный" руководствуются положениями настоящего положения, документами, руководящими и нормативными документами ФСТЭК РФ и регламентирующими документами, разработанными и утвержденными в образовательном учреждении в целях защиты информации и персональных данных.

3. Организация обеспечения безопасности персональных данных

3.1. Безопасность ПДн достигается путем принятия необходимых правовых, организационных и технических мер для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в их отношении.

3.2. Для обеспечения безопасности ПДн приказом директора назначается ответственный за организацию обработки персональных данных в организации, администратор ИБ и администратор по обработке ПДн в ИСПДн:

3.2.1. осуществлять внутренний контроль за соблюдением работниками образовательного учреждения установленных требований по обеспечению безопасности ПДн;

3.2.2. организовывать проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

3.2.3. осуществлять контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ИСПДн;

3.2.4. организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

3.2.5. периодически инициировать процедуры определения угроз безопасности ПДн при их обработке в ИСПДн;

3.2.6. организовывать и контролировать процедуры обнаружения фактов несанкционированного доступа к ПДн; фактов, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;

3.2.7. организовывать и контролировать процедуры принятия мер по предотвращению несанкционированного доступа к ПДн; инцидентов, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к

снижению уровня защищенности ПДн.
3.3. Администратор ИБ ИСПДн обязан:
3.3.1. осуществлять установку, настройку и сопровождение технических средств защиты;
3.3.2. участвовать в приемке новых программных средств;
3.3.3. обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения;
3.3.4. уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты;
3.3.5. вести контроль над процессом осуществления резервного копирования объектов защиты;
3.3.6. анализировать состояние защиты ИСПДн и ее отдельных подсистем;
3.3.7. контролировать неизменность состояния средств защиты их параметров и режимов защиты;
3.3.8. контролировать физическую сохранность средств и оборудования ИСПДн;
3.3.9. контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты;
3.3.10. контролировать исполнение пользователями парольной политики;
3.3.11. не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;
3.3.12. не допускать к работе на элементах ИСПДн посторонних лиц;
3.3.13. осуществлять периодические контрольные проверки носителей ПДн, рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;
3.3.14. оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты;
3.3.15. периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации;
3.3.16. в случае отказа работоспособности технических средств и программного обеспечения средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;
3.3.17. принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.
3.4. Администратор по обработке ПДн в ИСПДн обязан:
3.4.1. поддерживать текущий порядок обеспечения безопасности ПДн;
3.4.2.организовывать доведение до сведения работников образовательного учреждения положений законодательства РФ и локальных нормативных документов по обеспечению безопасности ПДн;
3.4.3. определять перечень работников образовательного учреждения, которым доступ к ПДн необходим для выполнения служебных обязанностей;
3.4.4. участвовать в реализации планов и программ поддержки осведомленности (обучения) в области обеспечения ИБ;
3.4.5. в случае отказа работоспособности технических средств и программного обеспечения ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;
3.4.6. принимать меры по реагированию, в случае возникновения непредвиденных и аварийных ситуаций, с целью ликвидации их последствий.
3.5. Необходимые технические меры для обеспечения безопасности ПДн реализуются в рамках системы защиты персональных данных (далее – СЗПДн).
3.6. СЗПДн обеспечивает защиту информации, содержащей ПДн, обрабатываемой с применением средств вычислительной техники, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно- оптической и иной основе.

3.7. Мероприятия по обеспечению безопасности ПДн, реализуемые в рамках СЗПДн, включают:
3.7.1. определение уровня защищенности ИСПДн;
3.7.2. создание моделей угроз и нарушителя для каждой ИСПДн;
3.7.3. применение организационных и технических мер по обеспечению безопасности ПДн для поддержания установленного уровня защищенности ПДн и нейтрализации актуальных угроз безопасности ПДн;
3.7.4. определение во внутренних нормативных документах порядка применения мер защиты, применяемых для обеспечения безопасности ПДн;
3.7.5. ознакомление работников образовательного учреждения, непосредственно осуществляющих обработку ПДн, с требованиями законодательных и нормативных актов, локальных нормативных документов, устанавливающих порядок обеспечения безопасности ПДн;
3.7.6. организацию внутреннего контроля и (или) аудита соответствия порядка обеспечения безопасности ПДн требованиям законодательных и нормативных актов, локальных нормативных документов;
3.7.7. организацию обучения, инструктажей и повышения осведомленности работников, осуществляющих обработку ПДн, по вопросам обеспечения безопасности ПДн;
3.7.8. совершенствование СЗПДн в соответствии с изменяемыми внутренними и внешними условиями и факторами, в том числе изменениями требований законодательства РФ.

4. Требования к системе защиты персональных данных

4.1. Требования к СЗПДн устанавливаются исходя из уровня защищенности ПДн и состава актуальных угроз безопасности ПДн.
4.2. Определение уровней защищенности ИСПДн производится в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4.3. Определение угроз безопасности ПДн производится в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России от 14.02.2008) на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России от 15.02.2008).

5. Описание системы защиты персональных данных

5.1. В число мер по обеспечению безопасности ПДн, реализованных в образовательном учреждении, входят:
5.1.1. определение порядка доступа в помещения, в которых осуществляется обработки ПДн;
5.1.2. размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;
5.1.3. ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн (в том числе серверное помещение), а также хранятся носители информации;
5.1.4. реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным активам, информационной системе и связанным с ее использованием работам, документам только для выполнения функциональных обязанностей;
5.1.5.установление правил доступа пользователей и обслуживающего персонала к

информационным активам, программным средствам обработки (передачи) и защиты информации на основе принципа минимально необходимых полномочий для выполнения своих функциональных обязанностей и поставленными перед ним задачами в объеме, необходимом для их исполнения;
5.1.6. учет и контроль лиц, допущенных к работе с ПДн;
5.1.7. регистрация и учет действий пользователей с ПДн, контроль несанкционированного доступа к ПДн;
5.1.8. размещение технических средства обработки графической, видео и буквенно-цифровой информации, содержащей ПДн, таким образом, чтобы исключить возможность просмотра посторонними лицами текстовой и графической, видовой информации, содержащей ПДн;
5.1.9. использование средств вычислительной техники, удовлетворяющих требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видео- дисплейным терминалам средств вычислительной техники;
5.1.10. учет и хранение съемных носителей, содержащих ПДн, и их обращение, исключающее хищение, подмену и уничтожение;
5.1.11. предотвращение внедрения в ИСПДн вредоносного программного обеспечения;
5.1.12. применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
5.1.13. оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
5.1.14. организация контроля за принимаемыми мерами по обеспечению безопасности ПДн и установленного уровня защищенности ПДн.
5.2. Для реализации указанных мер в составе СЗПДн реализованы следующие функциональные подсистемы:
5.2.1. идентификация и аутентификация субъектов доступа и объектов доступа;
5.2.2. управление доступом субъектов доступа к объектам доступа;
5.2.3. ограничение программной среды;
5.2.4. обеспечение целостности информационной системы и ПДн;
5.2.5. обеспечение доступности ПДн;
5.2.6. регистрация событий безопасности;
5.2.7. антивирусная защита;
5.2.8. защита технических средств;
5.2.9. защита информационной системы, ее средств, систем связи и передачи данных;
5.3. Технические средства защиты информации, используемые для нейтрализации актуальных угроз безопасности ПДн, применяемые в образовательном учреждении, проходят в установленном порядке процедуру оценки соответствия. Для выбора и реализации мер защиты ПДн в образовательном учреждении могут привлекаться на договорной основе сторонние организации, имеющие оформленную в установленном порядке лицензию на соответствующий вид деятельности в области защиты информации.

6. Контроль выполнения требований

6.1. Контроль и надзор за выполнением требований по обработке ПДн осуществляется уполномоченным органом по защите прав субъектов ПДн (Роскомнадзор).
6.2. Федеральные органы исполнительной власти (ФСБ России и ФСТЭК России) могут осуществлять контроль за выполнением организационных и технических мер по обеспечению безопасности ПДн без права ознакомления с ПДн, обрабатываемыми в ИСПДн.
6.3. Для проведения аудита соответствия порядка обеспечения безопасности ПДн

требованиям законодательства РФ могут привлекаться внешние организации, имеющие оформленную в установленном порядке лицензию на соответствующий вид деятельности в области защиты информации.

7. Ответственность

7.1. Обязанности за контроль выполнения положений настоящего положения, его пересмотр и составление рекомендаций по изменению возлагаются на ответственного за организацию обработки ПДн.

7.2. Ответственный за обработку ПДн, администратор ИБ и администратор ИСПДн несут персональную ответственность за соблюдение требований настоящего положения.