

29 августа 2017 года

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных

1. Термины, определения, сокращения

1.1. Автоматизированная информационная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.2. Безопасность персональных данных - состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

1.3. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

1.4. Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

1.5. Вредоносная программа (ВП) - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

1.6. Доступ к персональным данным - возможность получения персональных данных и их использования.

1.7. Защита от несанкционированного доступа - предотвращение или существенное затруднение несанкционированного доступа.

1.8. Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

1.9. Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

1.11. Информационная система персональных данных ИСПДн (далее ИС) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

1.12. Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

1.13. Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

1.14. Контролируемая зона (КЗ) - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

1.15. Межсетевой экран - локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

1.16. Недекларированные возможности (НДВ) - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

1.17. Несанкционированный доступ к персональным данным (несанкционированные действия) (НСД) - доступ к персональным данным или действия с персональными данными, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

1.18. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

1.19. Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

1.20. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

1.21. Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

1.22. Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.23. Побочные электромагнитные излучения и наводки (ПЭМИН) - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

1.24. Пользователь ИСПДн - лицо, участвующее в функционировании ИСПДн или использующее результаты ее функционирования.

1.25. Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

1.26. Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить персональные данные или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

1.27. Программное (программно-математическое) воздействие (ПМВ) - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

1.28. Ресурс информационной системы персональных данных - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы персональных данных.

1.29. Средства вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки персональных данных, способных функционировать самостоятельно или в составе других систем.

1.30. Санкционированный доступ к персональным данным - доступ к персональным данным, не нарушающий правила разграничения доступа.

1.31. Система защиты персональных данных (СЗПДн) - комплекс организационных мер и программно-технических средств обеспечения безопасности ПДн в ИСПДн.

1.32. Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1.33. Технический канал утечки информации - совокупность носителя персональных данных (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается информация, содержащая персональные данные.

1.34. Технические средства информационной системы персональных данных (ТС) - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

1.35. Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

1.36. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

1.37. Утечка (защищаемой) информации, содержащей персональные данные, по техническим каналам - неконтролируемое распространение персональных данных от носителя персональных данных через физическую среду до технического средства, осуществляющего перехват информации, содержащей персональные данные.

1.38. Целостность информации, содержащей персональные данные, - способность средства вычислительной техники или информационной системы персональных данных обеспечивать неизменность информации, содержащей персональные данные, в условиях случайного и/или преднамеренного искажения (разрушения).

2. Общие положения

2.1. Настоящее положение определяет цели, задачи, содержание, порядок организации и выполнения мероприятий по защите персональных данных в ходе их обработки в информационных системах структурного подразделения (или территориального органа) администрации города Нижнего Новгорода.

Положение является документом, обязательным для выполнения всеми должностными лицами при проведении работ, требующих защиты информации или информационных процессов, связанных с хранением, обработкой персональных данных в информационных системах персональных данных, эксплуатируемых в образовательном учреждении.

Положение разработано в соответствии с Федеральным законом от 27.07.06 № 152-ФЗ «О персональных данных», приказом Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю и Мининформсвязи РФ от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», руководящими документами ФСТЭК России в области защиты персональных данных.

2.2. Защита персональных данных, обрабатываемых в информационных системах, является составной частью работ по созданию и эксплуатации информационных систем персональных данных (далее – ИСПДн) и должна осуществляться в установленном настоящим Положением порядке во взаимосвязи с другими мерами по защите информации.

2.3. Должностные лица, осуществляющие обработку персональных данных, а также организующие эксплуатацию (разработку) информационных систем персональных данных, несут персональную ответственность за соблюдение требований настоящего Положения.

2.4. Технические и программные средства, применяемые в целях закрытия технических каналов утечки персональных данных в ходе их автоматизированной обработки, защиты от несанкционированного доступа, должны иметь сертификат соответствия требованиям безопасности информации, выданный уполномоченным в области безопасности органом.

2.5. Требования Настоящего Положения не распространяются на ИСПДн, обрабатывающие персональные данные, отнесенные в установленном порядке к сведениям, составляющим государственную тайну.

2.6. Изменения в текст настоящего Положения вносятся порядком, предусмотренным для его утверждения.

3.Замысел обеспечения безопасности персональных данных

3.1. Персональные данные – информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, хранимая, обрабатываемая и циркулирующая на объектах информатизации, являются критичным ресурсом и требуют постоянного поддержания таких свойств, как конфиденциальность, целостность и доступность, вследствие чего необходимо принятие адекватных мер по обеспечению их безопасности.

3.2. Основной целью мероприятий по защите персональных данных, обрабатываемых в информационных системах, является снижение риска получения ущерба в условиях действия преднамеренных и непреднамеренных угроз информационной безопасности, а также возможного ущерба а случае утечки информации, содержащей персональные данные, и ожидаемых затрат на достижение поставленной цели. Достижение требуемого уровня безопасности персональных данных, должно быть обеспечено системным применением организационных, организационно-технических, технических и программно-технических мер на всех этапах разработки, испытаний, внедрения и эксплуатации информационных систем персональных данных в структурном подразделении (территориальном органе) администрации города Нижнего Новгорода.

3.3. В качестве основных угроз безопасности персональных данных в ходе их обработки в информационных системах необходимо рассматривать:

3.3.1. Хищение, модификация или блокирование информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств.

3.3.2. Уничтожение, хищение аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн.

3.3.3. Просмотр информации с экранов дисплеев и других средств ее отображения.

3.3.4. Непреднамеренные действия персонала и нарушение безопасности функционирования ИСПДн и средств защиты персональных данных в их составе из-за сбоев в программном обеспечении, а также угроз антропогенного и стихийного характера.

4. Организации и проведение работ по обеспечению безопасности персональных данных

4.1. Обязанности должностных лиц

4.1.1. Ответственность за безопасность информации

Оперативное руководство организацией работ и координацию деятельности по защите персональных данных возлагается на ответственных за обеспечение безопасности информации на АРМ, назначаемых приказами руководителей образовательных учреждений из числа своих заместителей.

4.1.2. Ответственность за правильную организацию работ по защите информации и соблюдение требований по защите информации при работе в информационных системах персональных данных возлагается на руководителей подразделений, использующих в своей деятельности обработку персональных данных на средствах вычислительной техники.

4.1.3. Должностные лица, осуществляющие обработку персональных данных в соответствующих ИСПДн (в том числе пользователи ИСПДн), несут персональную ответственность за выполнение установленных правил и требований по обеспечению безопасности персональных данных. Обязанности и права пользователей ИСПДн приводятся в «Инструкции пользователям».

4.1.4. Обязанности должностных лиц, осуществляющие обработку, защиту и контроль эффективности обработки персональных данных в ИСПДн должны быть регламентированы в их должностных инструкциях.

4.2. Порядок допуска сотрудников к обработке персональных данных

4.2.1. Перечень лиц, имеющих самостоятельный доступ к ИСПДн (ее элементам), а также перечень лиц, допущенных к техническому обслуживанию аппаратных и программных средств ИСПДн, утверждается руководителями образовательных учреждений.

4.3. Требования к размещению аппаратных средств информационных систем персональных данных.

4.3.1. Входные двери помещений, в которых располагаются аппаратные средства информационной системы, а также машинные носители информации должны оборудоваться замками, гарантирующими надежное закрытие помещений в нерабочее время, в них также могут устанавливаться кодовые и электронные замки.

4.3.2. Должен быть определен порядок постановки и снятия с охраны помещений, где осуществляется обработка персональных данных.

4.3.3. При проведении технического обслуживания и ремонта аппаратных средств ИСПДн запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения персональных данных.

4.3.4. Машинные носители информации, содержащие персональные данные, подлежат учету путем их маркировки с занесением учетных данных в журнал регистрации их выдачи и приема.

4.3.5. Журнал регистрации выдачи и приема носителей информации (компакт-диски, USB-устройства и т.п.) ведется в подразделениях, в которых производится обработка персональных данных.

4.3.6. Хранение машинных носителей информации осуществляется в условиях, исключающих их хищение либо несанкционированное копирование или уничтожение содержащейся на них информации.

4.3.7. Машинные носители информации, пришедшие в негодность, подлежат уничтожению с составлением Акта об уничтожении.

4.4. Обеспечение безопасности в ходе обмена информацией со сторонними организациями

4.4.1. Допускается передача персональных данных в указанные органы с использованием учетных в журнале регистрации машинных носителей информации.

4.4.2. Передача персональных данных в иные органы (ведомства) структурными подразделениями или территориальными органами администрации города Нижнего Новгорода должна осуществляться с письменного разрешения их руководителей с соблюдением требований законодательства на основании Соглашений, одним из обязательных пунктов которого должен быть пункт об обязательном соблюдении условия конфиденциальности сведений, содержащих персональные данные.

5. Контроль состояния защиты персональных данных

5.1. Контроль состояния защиты персональных данных - комплекс организационных и технических мероприятий которые организуются и осуществляются в целях выявления и предотвращения утечки информации по техническим каналам; исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации; предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации и работоспособности аппаратных средств ИСПДн.

5.2. Основными задачами контроля являются:

- проверка выполнения установленных норм и требований по защите персональных данных, учета требований по их защите в разрабатываемых документах;
- уточнение возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на аппаратные и программные элементы ИСПДн;
- оценка достаточности и эффективности принимаемых мер по защите персональных данных;
- проверка надлежащего использования средств защиты персональных данных;
- проверка выполнения требований по антивирусной защите ИСПДн;
- оперативное принятие мер по пресечению нарушений требований защиты персональных данных в структурных подразделениях и территориальных органах администрации;
- разработка предложений по устранению (ослаблению) угроз безопасности персональных данных, обрабатываемых в информационных системах.

5.3. В ходе контроля проверяются:

- соответствие принятых мер установленным нормам и требованиям безопасности информации;
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по защите персональных данных;
- полнота выявления возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на ИСПДн (ее элементы);
- эффективность применения организационных и технических мероприятий по защите персональных данных;
- устранение ранее выявленных недостатков.

5.4. Контроль за соблюдением установленных требований безопасности персональных данных осуществляется путем обследования ИСПДн. Обследование ИСПДн проводится комиссией по классификации ИСПДн при участии представителя управления образования, осуществляющего обработку персональных данных. Обследование ИСПДн проводится не реже одного раза в год (при неизменности условий ее эксплуатации).

5.5. В ходе обследования проверяется:

- выполнение требований по защите персональных данных от несанкционированного доступа;
- выполнение требований по антивирусной защите ИСПДн