ЗАКОНОДАТЕЛЬНОЕ СОБРАНИЕ ПЕРМСКОГО КРАЯ

Р А С П О Р Я Ж Е Н И Е

11.03.2019 **№ 10**

Об утверждении политики безопасности персональных данных, обрабатываемых в информационных системах персональных данных Законодательного Собрания Пермского края

В целях исполнения норм Федерального Закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Утвердить политику безопасности персональных данных, обрабатываемых в информационных системах персональных данных Законодательного Собрания Пермского края.

2. Разместить политику безопасности персональных данных на сайте Законодательного Собрания Пермского края в общедоступном разделе в пределах одного ссылочного перехода.

3. Контроль за исполнением распоряжения возложить на руководителя аппарата Законодательного Собрания Пермского края Новиченкова В.Е.

Председатель
Законодательного Собрания В.А.Сухих

752-19

Приложение
к распоряжению председателя
Законодательного Собрания
Пермского края
от 11.03.2019 № 10

ПОЛИТИКА
безопасности персональных данных, обрабатываемых в информационных системах персональных данных Законодательного Собрания Пермского края

1. Общие положения

Настоящая Политика безопасности персональных данных, обрабатываемых в информационных системах персональных данных Законодательного Собрания Пермского края (далее – Политика), является официальным документом и разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, защиты их от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных и минимизации ущерба от возможной реализации угроз.

Безопасность персональных данных достигается путем исключения 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.

Информация, содержащая персональные данные, и связанные с ней ресурсы должны быть доступны только для пользователей, прошедших идентификацию. В информационных системах персональных данных должно осуществляться своевременное обнаружение угроз и реагирование на угрозы безопасности персональных данных.

В информационных системах персональных данных необходимо исключить возможность преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

В настоящем документе используются следующие термины и их определения.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности персональных данных – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности персональных данных.

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

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

Нарушитель безопасности персональных данных – лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление доступа), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Оператор персональных данных – Законодательное Собрание Пермского края, государственный орган, самостоятельно или совместно с другими лицами организующие и осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия, совершаемые с персональными данными.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

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

Субъекты персональных данных – государственные гражданские служащие аппарата Законодательного Собрания, депутаты Законодательного Собрания, помощники депутатов, лица, заключающие контракты с Законодательным Собранием, лица, обращающиеся с запросами в Законодательное Собрание и другие лица.

Технический канал утечки информации – совокупность носителей информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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, применяемые в информационных системах.

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 иные несанкционированные действия при их обработке в информационной системе персональных данных.

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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Система защиты персональных данных

Система защиты персональных данных строится на основании:

а) перечня персональных данных, подлежащих защите;

б) перечня информационных систем персональных данных;

в) акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных;

г) частной модели угроз и нарушителя безопасности персональных данных;

д) положения о разграничении прав доступа к обрабатываемым персональным данным;

е) Федеральных законов от 27.07.2006 №152-ФЗ «О персональных данных», от 27.07 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

ж) Постановлений Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

з) руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определён необходимый уровень защищенности персональных данных в каждой информационной системе персональных данных Законодательного Собрания. Для каждой информационной системы персональных данных составлен список используемых технических средств, а также программного обеспечения, участвующего в обработке персональных данных, подлежащих защите.

Система защиты персональных данных включает следующие технические и программные средства:

а) антивирусные средства для объектов вычислительной техники;

б) средства межсетевого экранирования;

в) средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

Так же в список включены функции защиты, обеспечиваемые штатными средствами информационной системы персональных данных и операционных систем, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты. Список функций защиты включает:

а) управление доступом и разграничение доступа пользователей;

б) регистрацию и учет действий с информацией;

в) обеспечение целостности данных;

г) обнаружение вторжений;

д) оповещение.

3. Требования, предъявляемые к подсистемам системы защиты персональных данных

Система защиты персональных данных Законодательного Собрания включает в себя следующие подсистемы:

а) управления доступом, регистрации и учета;

б) обеспечения целостности и доступности;

в) антивирусной защиты;

г) межсетевого экранирования;

д) анализа защищенности;

е) обнаружения вторжений;

ж) криптографической защиты.

Подсистемы системы защиты персональных данных имеют различный функционал в зависимости от уровня защищенности персональных данных при их обработке в информационной системе персональных данных, определенного в Акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных.

3.1. Подсистема управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

а) идентификации и проверки подлинности субъектов доступа при входе в информационную систему персональных данных;

б) идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

в) идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

г) регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрации загрузки и инициализации операционной системы и ее останова;

д) регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

е) регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом, регистрации и учета реализуется с помощью штатных средств обработки персональных данных (операционных систем, приложений), а так же при помощи специальных технических средств и их комплексов.

3.2. Подсистема обеспечения целостности и доступности

Данная подсистема предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационных систем персональных данных Законодательного Собрания, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов информационных систем персональных данных.

3.3. Подсистема антивирусной защиты

Данная подсистема предназначена для обеспечения антивирусной защиты объектов вычислительной техники Законодательного Собрания. Средства антивирусной защиты предназначены для реализации следующих функций:

а) резидентный антивирусный мониторинг;

б) антивирусное сканирование;

в) скрипт-блокирование;

г) централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчетов и статистической информации по работе продукта;

д) автоматизированное обновление антивирусных баз;

е) ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

ж) автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения во все элементы информационных систем персональных данных.

3.4. Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

а) фильтрации открытого и закрытого (зашифрованного) IP-трафика;

б) фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

в) идентификации и аутентификации администратора информационной безопасности или администратора информационной системы персональных данных при его локальных запросах на доступ;

г) контроля целостности своей программной и информационной части;

д) фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

е) фильтрации трафика с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

ж) регистрации и учета запрашиваемых сервисов прикладного уровня;

з) блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

и) контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе сети.

3.5. Подсистема анализа защищенности

Регулярный анализ защищенности информационных систем персональных данных обеспечивает выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы персональных данных, которые могут быть использованы нарушителем для реализации атаки на систему.

Подсистема реализуется с помощью организации аудита программно-аппаратных комплексов систем обработки персональных данных.

3.6. Подсистема обнаружения вторжений

Подсистема обнаружения вторжений обеспечивает выявление сетевых атак на элементы информационной системы персональных данных, подключенных к сетям общего пользования и международного обмена.

Функционал подсистемы реализуется программно-аппаратными средствами.

3.7. Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в информационных системах персональных данных Законодательного Собрания при ее передаче по каналам связи сетей общего пользования и международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

4. Пользователи информационных систем персональных данных

В информационных системах персональных данных Законодательного Собрания выделены следующие группы пользователей, участвующих в обработке персональных данных:
администраторы информационных систем персональных данных;
операторы информационных систем персональных данных.

4.1. Администраторы информационных систем персональных данных

Администраторы информационных систем персональных данных являются ответственными за настройку, внедрение и сопровождение информационных систем персональных данных. Обеспечивают функционирование подсистем управления доступом информационных систем персональных данных и уполномочены осуществлять предоставление и разграничение доступа конечных пользователей (операторов информационных систем персональных данных) к элементам, хранящим персональные данные.

Администраторы информационных систем персональных данных обладают следующим уровнем доступа и знаний:

а) обладают полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных;

б) обладают полной информацией о технических средствах и конфигурации информационных систем персональных данных;

в) обладают возможностями внесения изменений в программное обеспечение информационных систем персональных данных на стадии ее разработки, внедрения и/или сопровождения.

4.2. Операторы информационной системы персональных данных

Операторы информационных систем персональных данных – сотрудники Законодательного Собрания, осуществляющие обработку персональных данных. Обработка персональных данных включает: возможность просмотра персональных данных, ручной ввод персональных данных в информационную систему персональных данных, формирование справок и отчетов по информации, полученной из информационной системы персональных данных.

Оператор информационной системы персональных данных обладает всеми необходимыми атрибутами, обеспечивающими доступ к персональным данным.

5. Администратор информационной безопасности

Администратор информационной безопасности, ответственный за функционирование системы защиты персональных данных, включая

обслуживание и настройку административной, серверной и клиентской компонент.

Администратор информационной безопасности обладает следующим уровнем доступа и знаний:

а) обладает полной информацией об информационных системах персональных данных;

б) имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационной системы персональных данных;

в) не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор информационной безопасности уполномочен:

а) реализовывать политики безопасности в части настройки средств защиты информации, межсетевых экранов и систем обнаружения вторжений, в соответствии с которыми пользователь (операторы информационных систем персональных данных) получает возможность работать с элементами информационных систем персональных данных;

б) осуществлять аудит средств защиты информации;

в) осуществлять контроль действий пользователей информационных систем персональных данных при их работе с персональными данными.

6. Требования к пользователям по обеспечению защиты персональных данных

Пользователи информационных систем персональных данных должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению установленного режима безопасности персональных данных.

Сотрудник, допущенный к обработке персональных данных, должен быть ознакомлен администратором информационной безопасности с настоящей Политикой, установленными процедурами работы с элементами информационной системы персональных данных и системой защиты персональных данных.

Сотрудники Законодательного Собрания, использующие технические средства аутентификации, должны обеспечивать сохранность персональных идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а также возможность их утери или использования третьими лицами. Сотрудники несут персональную ответственность за сохранность идентификаторов.

Сотрудники Законодательного Собрания должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи информационной системы персональных данных должны знать требования по безопасности персональных данных и процедуры защиты оборудования,

оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

При работе с техническими средствами обработки персональных данных сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна в силу выполнения ими своих должностных обязанностей.

При работе с персональными данными в информационной системе персональных данных сотрудники Законодательного Собрания обязаны исключить возможность просмотра персональных данных третьими лицами с мониторов объектов вычислительной техники.

При завершении работы с информационной системой персональных данных сотрудники обязаны защитить объекты вычислительной техники с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационной системы персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству и администратору информационной безопасности.

7. Ответственность пользователей информационной системы персональных данных

В соответствии со ст. 24 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную или иную предусмотренную законодательством Российской Федерации ответственность.

Пользователи информационных систем персональных данных несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.