ЗАКОНОДАТЕЛЬНОЕ СОБРАНИЕ КЕМЕРОВСКОЙ ОБЛАСТИ – КУЗБАССА

ПОСТАНОВЛЕНИЕ

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Законодательном Собрании Кемеровской области – Кузбасса

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» и статьей 22 Закона Кемеровской области – Кузбасса «О Законодательном Собрании Кемеровской области – Кузбасса и законодательной деятельности в Кемеровской области – Кузбассе» Законодательное Собрание Кемеровской области – Кузбасса

п о с т а н о в л я е т:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Законодательном Собрании Кемеровской области – Кузбасса, согласно приложению к настоящему Постановлению.

2. Опубликовать настоящее Постановление на сайте «Законодательный вестник Кузбасса».

3. Контроль за исполнением настоящего Постановления возложить на заместителя председателя Законодательного Собрания Кемеровской области – Кузбасса Репину Д.Я.

4. Настоящее Постановление вступает в силу со дня его официального опубликования.

Председатель А.А. Зеленин

Законодательное Собрание Кемеровской области – Кузбасса * Для постановлений

г. Кемерово
22 апреля 2025 года
№ 930

Приложение
к постановлению Законодательного
Собрания Кемеровской области – Кузбасса
«Об определении угроз безопасности
персональных данных, актуальных при
обработке персональных данных в
информационных системах персональных
данных в Законодательном Собрании
Кемеровской области – Кузбасса»

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Законодательном Собрании Кемеровской области – Кузбасса

I. Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных (далее – ИСПДн) в Законодательном Собрании Кемеровской области – Кузбасса, разработаны в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных», постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России «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», Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021, Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденными руководством 8-го Центра ФСБ России, Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной

заместителем директора ФСТЭК России 15.02.2008, и Банком данных угроз безопасности информации, размещенным на официальном сайте ФСТЭК России.

2. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн в Законодательном Собрании Кемеровской области – Кузбасса (далее – актуальные угрозы безопасности персональных данных в ИСПДн), содержат перечень актуальных угроз безопасности персональных данных при их обработке в ИСПДн в Законодательном Собрании Кемеровской области – Кузбасса (далее – Законодательное Собрание).

3. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в актуальных угрозах безопасности персональных данных в ИСПДн, подлежат адаптации в ходе разработки Законодательным Собранием частных моделей угроз безопасности персональных данных для каждой информационной системы.

4. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик информационной системы, эксплуатируемой при осуществлении Законодательным Собранием функций и полномочий, а также применяемых в ней информационных технологий и особенностей ее функционирования.

В частной модели угроз безопасности персональных данных указываются:

описание ИСПДн и ее структурно-функциональных характеристик;

описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

описание возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Частная модель угроз безопасности персональных данных для государственных органов разрабатывается с учетом требований приказа ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и приказа ФСБ России «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».

5. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в актуальных угрозах безопасности персональных данных в ИСПДн, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз

безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с ФСТЭК России и ФСБ России в установленном порядке.

В Законодательном Собрании функционируют информационные системы, обрабатывающие специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора, общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора, и персональные данные менее чем 100 000 субъектов персональных данных, являющихся сотрудниками оператора.

ИСПДн в Законодательном Собрании имеют сходную структуру, однотипны, характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы, имеющие подключение к единому центру обработки данных, а также подключение к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных в ИСПДн и вывод данных из ИСПДн осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и компакт-диски.

Персональные данные субъектов персональных данных обрабатываются в целях:

ведения финансово-экономической деятельности в соответствии с требованиями законодательства Российской Федерации;

проведения конкурсного отбора на государственную гражданскую службу Кемеровской области – Кузбасса в Законодательном Собрании;

ведения кадрового резерва на государственной гражданской службе Кемеровской области – Кузбасса в Законодательном Собрании;

формирования и ведения Реестра государственных гражданских служащих Кемеровской области – Кузбасса в Законодательном Собрании;

обеспечения деятельности сенатора Российской Федерации от Законодательного Собрания;

награждения наградами Законодательного Собрания;

рассмотрения запросов, обращений граждан, объединений граждан, в том числе юридических лиц.

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты информации (далее – СКЗИ).

Контролируемой зоной ИСПДн являются административные здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

В административных зданиях осуществляется пропускной и внутриобъектовый режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники запрещено. Помещения оборудованы запирающимися дверями. В коридорах, вестибюлях и холлах ведется видеонаблюдение.

II. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

Учитывая особенности обработки персональных данных в Законодательном Собрании, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

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

Целостность – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Основной целью применения в ИСПДн в Законодательном Собрании СКЗИ является защита персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

Объектами защиты являются:

персональные данные;

СКЗИ;

среда функционирования СКЗИ (далее – СФ СКЗИ);

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на

технические и программные компоненты СФ СКЗИ;

носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

используемые информационной системой каналы (линии) связи, включая кабельные системы;

помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

Основными актуальными угрозами безопасности персональных данных в ИСПДн в Законодательном Собрании согласно требованиям ФСТЭК России являются:

угрозы воздействия на программы с высокими привилегиями;

угрозы восстановления и (или) повторного использования аутентификационной информации;

угрозы деструктивного изменения конфигурации/среды окружения программ;

угрозы длительного удержания вычислительных ресурсов пользователями;

угрозы доступа к защищаемым файлам с использованием обходного пути;

угрозы доступа к локальным файлам сервера при помощи URL;

угрозы доступа/перехвата/изменения HTTP cookies;

угрозы избыточного выделения оперативной памяти;

угрозы изменения системных и глобальных переменных;

угрозы использования вычислительных ресурсов суперкомпьютера «паразитными» процессами;

угрозы использования информации идентификации/аутентификации, заданной по умолчанию;

угрозы использования механизмов авторизации для повышения привилегий;

угрозы использования слабостей протоколов сетевого/локального обмена данными;

угрозы некорректного использования прозрачного прокси-сервера за счет плагинов браузера;

угрозы неправомерного ознакомления с защищаемой информацией;

угрозы несанкционированного восстановления удаленной защищаемой информации;

угрозы несанкционированного доступа к аутентификационной информации;

угрозы несанкционированного доступа к сегментам вычислительного поля;

угрозы несанкционированного доступа к системе по беспроводным каналам;

угрозы несанкционированного изменения аутентификационной информации;

угрозы несанкционированного копирования защищаемой информации;

угрозы обнаружения открытых портов и идентификации привязанных к ним сетевых служб;

угрозы обнаружения хостов;

угрозы обхода некорректно настроенных механизмов аутентификации;

угрозы определения типов объектов защиты;

угрозы определения топологии вычислительной сети;

угрозы перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;

угрозы переполнения целочисленных переменных;

угрозы перехвата данных, передаваемых по вычислительной сети;

угрозы повышения привилегий;

угрозы подключения к беспроводной сети в обход процедуры аутентификации;

угрозы подмены беспроводного клиента или точки доступа;

угрозы подмены действия пользователя путем обмана;

угрозы подмены доверенного пользователя;

угрозы подмены содержимого сетевых ресурсов;

угрозы подмены субъекта сетевого доступа;

угрозы получения предварительной информации об объекте защиты;

угрозы получения сведений о владельце беспроводного устройства;

угрозы приведения системы в состояние «отказ в обслуживании»;

угрозы сканирования веб-сервисов, разработанных на основе языка описания WSDL;

угрозы удаления аутентификационной информации;

угрозы усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

угрозы утраты носителей информации;

угрозы физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

угрозы форматирования носителей информации;

угрозы «форсированного веб-браузинга»;

угрозы хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

угрозы заражения компьютера при посещении неблагонадежных сайтов;

угрозы «кражи» учетной записи доступа к сетевым сервисам;

угрозы наличия механизмов разработчика;

угрозы распространения «почтовых червей»;

угрозы «спама» веб-сервера;

угрозы «фарминга»;

угрозы «фишинга»;

угрозы несанкционированной модификации защищаемой информации;

угрозы несанкционированного изменения параметров настройки средств защиты информации;

угрозы внедрения вредоносного кода через рекламу, сервисы и контент;

угрозы несанкционированного воздействия на средство защиты информации;

угрозы подмены программного обеспечения;

угрозы маскирования действий вредоносного кода;

угрозы внедрения вредоносного кода за счет посещения зараженных сайтов в сети «Интернет»;

угрозы внедрения вредоносного кода в дистрибутив программного обеспечения;

угрозы использования уязвимых версий программного обеспечения;

угрозы утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;

угрозы удаленного запуска вредоносного кода в обход механизмов защиты операционной системы;

угрозы хищения аутентификационной информации из временных файлов cookie;

угрозы скрытной регистрации вредоносной программой учетных записей администраторов;

угрозы утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;

угрозы несанкционированного доступа к системе при помощи сторонних сервисов;

угрозы использования скомпрометированного доверенного источника обновлений программного обеспечения.