# ПРАВИТЕЛЬСТВО ТУЛЬСКОЙ ОБЛАСТИ

# ПОСТАНОВЛЕНИЕ

от 29.10.2015 № 504

**Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях**

С целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях, в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Концепцией защиты информации в Тульской области, одобренной решением Комиссии по информационной безопасности Тульской области от 22 мая 2014 года, на основании статьи 48 Устава (Основного Закона) Тульской области правительство Тульской области ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях (приложение).

2. Рекомендовать органам местного самоуправления Тульской области и подведомственным им учреждениям, организациям:

определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в используемых ими информационных системах персональных данных;

094682

при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться настоящим постановлением.

3. Постановление вступает в силу со дня официального опубликования.

**Первый заместитель Губернатора Тульской области – председатель правительства Тульской области** **Ю.М. Андрианов**

Приложение
к постановлению правительства
Тульской области

от 29.10.2015 № 504

# УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, актуальные при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях

## Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях (далее – Актуальные угрозы безопасности ИСПДн ТО), разработаны в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Актуальные угрозы безопасности ИСПДн ТО содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) органов исполнительной власти Тульской области и аппарата правительства Тульской области (далее – государственные органы).

3. При разработке Актуальных угроз безопасности ИСПДн ТО использованы методические документы, модели угроз безопасности персональных данных, утвержденные Федеральной службой по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) и Федеральной службой безопасности Российской Федерации (далее – ФСБ России).

4. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в Актуальных угрозах безопасности ИСПДн ТО, подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных.

При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик конкретной ИСПДн и применяемых в ней информационных технологий, особенностей её функционирования.

В частной модели угроз безопасности персональных данных указываются:

описание ИСПДн и её 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.

Типовая форма частной модели угроз безопасности персональных данных для государственных органов разрабатывается министерством по информатизации, связи и вопросам открытого управления Тульской области с учетом требований приказа Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и приказа Федеральной службы безопасности 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» (далее – Приказ ФСБ России).

5. Актуальные угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в Актуальных угрозах безопасности ИСПДн ТО, 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.

Информационные системы персональных данных в органах государственной власти Тульской области и подведомственных им учреждениях и организациях 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 осуществляется 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 с целью получения государственных и муниципальных услуг, а также:

в целях обеспечения деятельности Губернатора и правительства Тульской области;

в целях обеспечения кадровой работы, в том числе в целях содействия гражданским служащим, работникам в прохождении государственной гражданской службы Тульской области, выполнении работы, в обучении и должностном росте, обеспечения личной безопасности гражданских служащих, работников и членов их семей, обеспечения сохранности принадлежащего им имущества и имущества государственных органов, учета результатов исполнения ими должностных обязанностей, обеспечения установленных законодательством Российской Федерации условий осуществления служебной деятельности и труда, гарантий и компенсаций;

в целях формирования кадрового резерва на государственной гражданской службе Тульской области, резерва управленческих кадров Тульской области, противодействия коррупции;

в целях реализации процедур по представлению граждан к награждению;

в целях приема, обработки и распределения поступивших в адрес Губернатора Тульской области, первого заместителя Губернатора Тульской области – председателя правительства Тульской области, их заместителей, органов исполнительной власти и подразделений аппарата правительства Тульской области документов, обращений граждан и организаций, а также регистрация и отправка исходящей корреспонденции;

в целях ведения внутренней служебной переписки;

в целях формирования внутренних документов, регламентирующих деятельность аппарата правительства Тульской области и органов исполнительной власти Тульской области;

в целях предоставления жилых помещений специализированного жилищного фонда Тульской области;

в целях выдачи вкладышей в паспорт для прохода в здание правительства Тульской области и пропусков для парковки у здания правительства Тульской области автотранспортных средств;

в целях подготовки и проведения мероприятий с участием или по поручению Губернатора Тульской области, подготовки пресс-релизов о деятельности правительства Тульской области, взаимодействия со сторонними СМИ.

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 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.

## Угрозы безопасности информационных систем персональных данных

Учитывая особенности обработки персональных данных в государственных органах, 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 распространение 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.

Для ИСПДн государственных органов Тульской области актуальны угрозы безопасности третьего типа.

Исходя из состава обрабатываемых персональных данных и типа актуальных угроз, определяется, что для обеспечения безопасности персональных данных в ИСПДн государственных органов Тульской области необходимо обеспечение второго уровня защищенности персональных данных (УЗ 2).

Основной целью применения в ИСПДн государственных органов Тульской области 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 (ПДн);

средства криптографической защиты информации (СКЗИ);

среда функционирования СКЗИ (далее – СФ);

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 информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;

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 видами угроз безопасности персональным данным в ИСПДн являются:

угрозы утечки информации по техническим каналам;

угрозы утечки акустической информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналам ПЭМИН;

угрозы несанкционированного доступа к информации;

угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;

кража ПЭВМ;

кража носителей информации;

кража ключей и атрибутов доступа;

кража, модификация, уничтожение информации;

вывод из строя узлов ПЭВМ, каналов связи;

несанкционированное отключение средств защиты;

угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (далее – НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

действия вредоносных программ (вирусов);

использование не декларированных возможностей системного программного обеспечения (далее – ПО) и ПО для обработки персональных данных;

установка ПО, не связанного с исполнением служебных обязанностей;

угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты персональных данных (далее – СЗПДн) в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного характера (ударов молний, пожаров, наводнений и т.п.);

утрата ключей и атрибутов доступа;

непреднамеренная модификация (уничтожение) информации сотрудниками;

непреднамеренное отключение средств защиты;

выход из строя аппаратно-программных средств;

сбой системы электроснабжения;

стихийное бедствие;

угрозы преднамеренных действий внутренних нарушителей;

доступ к информации, модификация, уничтожение информации лицами, не допущенными к ее обработке;

разглашение информации, её модификация или уничтожение сотрудниками, допущенными к ее обработке;

угрозы несанкционированного доступа по сети и каналам связи;

угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

перехват за переделами контролируемой зоны;

перехват в пределах контролируемой зоны внешними нарушителями;

перехват в пределах контролируемой зоны внутренними нарушителями;

угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

угрозы выявления паролей по сети;

угрозы навязывания ложного маршрута сети;

угрозы подмены доверенного объекта в сети;

угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ;

угрозы несанкционированного доступа при использовании технологий виртуализации;

угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

нарушение работоспособности информационных систем, построенных на основе технологий виртуализации, за счет несанкционированного доступа к средствам виртуализации;

атака на виртуальные каналы передачи данных;

несанкционированный доступ к образам виртуальных машин;

нарушение изоляции пользовательских данных внутри виртуальных машин;

атака на гипервизор с виртуальной машины;

атака на гипервизор из физической сети;

атака на защищаемые виртуальные машины из физической сети;

неконтролируемый рост числа виртуальных машин;

атака на сеть репликации виртуальных машин;

перехват управления в среде виртуализации;

выход процесса за пределы виртуальной среды.

При определении актуальных угроз безопасности персональных данных используются следующие положения:

единый подход к созданию, развитию (модернизации) и эксплуатации государственных информационных систем Тульской области, основанный на согласовании технологий обработки информации с министерством по информатизации, связи и вопросам открытого управления Тульской области;

реализация единого порядка согласования технических заданий и технических проектов на создание информационных систем и входящих в их состав систем защиты информации с использованием некриптографических средств защиты информации (далее – СЗИ) и (или) с использованием средств криптографической защиты информации (СКЗИ).

**Актуальные угрозы безопасности ИСПДн ТО:**

действия вредоносных программ (вирусов);

утрата ключей и атрибутов доступа;

перехват передаваемой из ИСПДн и принимаемой из внешних сетей информации за переделами контролируемой зоны;

несанкционированный доступ через сети международного обмена;

несанкционированный доступ через ЛВС организации;

утечка атрибутов доступа;

угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

угрозы выявления паролей по сети;

угрозы подмены доверенного объекта в сети;

угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ;

угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

нарушение работоспособности информационных систем, построенных на основе технологий виртуализации, за счет несанкционированного доступа к средствам виртуализации;

атака на виртуальные каналы передачи данных;

несанкционированный доступ к образам виртуальных машин;

нарушение изоляции пользовательских данных внутри виртуальных машин;

атака на гипервизор с виртуальной машины;

атака на гипервизор из физической сети;

атака на защищаемые виртуальные машины из физической сети;

неконтролируемый рост числа виртуальных машин;

атака на сеть репликации виртуальных машин;

перехват управления в среде виртуализации;

выход процесса за пределы виртуальной среды.