ПРАВИТЕЛЬСТВО КИРОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

24.08.2017 № 421-П

г. Киров

Об определении перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Кировской области, подведомственных им областных государственных предприятий, областных государственных учреждений, открытых акционерных обществ, 100 процентов акций которых находятся в государственной собственности области, Правительство Кировской области ПОСТАНОВЛЯЕТ:

1. Определить перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных (далее – ИСПДн), согласно приложению.

2. Органам исполнительной власти Кировской области, подведомственным им областным государственным предприятиям, областным государственным учреждениям, открытым акционерным обществам, 100 процентов акций которых находятся в государственной собственности Кировской области, при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими ИСПДн, руководствоваться настоящим постановлением.

3. Рекомендовать органам местного самоуправления Кировской области при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими ИСПДн, руководствоваться настоящим постановлением.

4. Контроль за выполнением постановления возложить на министерство информационных технологий и связи Кировской области.

Врио Губернатора –
Председателя Правительства
Кировской области И.В. Васильев

Приложение

к постановлению Правительства
Кировской области
от 24.08.2017 № 421-П

ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных

1. Общие положения

Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Кировской области (далее – Перечень актуальных угроз безопасности ИСПДн КО), разработан в соответствии с:

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной

Заместителем директора Федеральной службы по техническому и экспортному контролю 15.02.2008;

Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Заместителем директора Федеральной службы по техническому и экспортному контролю 14.02.2008;

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 Центра Федеральной службы безопасности Российской Федерации 31.03.2015 № 149/7/2/6-432 (далее – методические рекомендации ФСБ России № 149/7/2/6-432);

приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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»;

информацией об угрозах безопасности информации, содержащейся в Банке данных угроз безопасности информации (http://bdu.fstec.ru/), сформированном Федеральной службой по техническому и экспортному контролю.

2. Перечень актуальных угроз безопасности ИСПДн КО

2.1. Угрозы безопасности персональных данных рассмотрены в методических документах ФСТЭК России и ФСБ России. Основными

характеристиками безопасности персональных данных являются конфиденциальность, целостность и доступность.

Конфиденциальность – обязательное для соблюдения лицом, получившим доступ к персональным данным, 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 или сбоев в функционировании ИСПДн в процессе обработки или хранения.

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

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность воздействия на ИСПДн и обрабатываемые в ней персональные данные, результатом которого может стать нарушение характеристик безопасности персональных данных.

2.2. Перечень актуальных угроз безопасности ИСПДн КО содержит угрозы безопасности персональных данных, актуальные при их обработке в ИСПДн органов исполнительной власти Кировской области, подведомственных им областных государственных предприятий, областных государственных учреждений, а также открытых акционерных обществ, 100 процентов акций которых находятся в государственной собственности Кировской области (далее – ОИВ и организации).

2.3. Актуальные угрозы безопасности ИСПДн КО в зависимости от условий, характерных для конкретных ИСПДн, сгруппированы в разделы:

актуальные угрозы, характерные для всех ИСПДн (пункт 2.4 настоящего Перечня актуальных угроз безопасности ИСПДн КО);

актуальные угрозы в зависимости от архитектуры ИСПДн (пункт 2.5 настоящего Перечня актуальных угроз безопасности ИСПДн КО);

актуальные угрозы в зависимости от особенностей ИСПДн (пункт 2.6 настоящего Перечня актуальных угроз безопасности ИСПДн КО).

Для конкретной ИСПДн согласно пунктам 2.4 – 2.6 настоящего Перечня актуальных угроз безопасности ИСПДн КО определяется архитектура и особенности этой ИСПДн и выбирается соответствующий перечень актуальных угроз.

2.4. Актуальными угрозами безопасности персональных данных, общими для всех ИСПДн, являются угрозы:

утечки акустической (речевой) информации;

утечки информации по каналам побочных электромагнитных излучений и наводок;

утечки видовой информации;

связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении (далее – ПО), используемом в ИСПДн;

связанные с наличием недокументированных (недекларированных) возможностей в прикладном ПО, используемом в ИСПДн;

несанкционированного отключения или обхода функций средств защиты информации;

выявления паролей, в том числе связанные с использованием стандартных паролей;

обхода возможности ведения или уничтожения журнала операций пользователя с персональными данными;

связанные с необеспечением доверенной загрузки средств вычислительной техники, используемых в ИСПДн;

связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн;

связанные с преднамеренными действиями лиц, не имеющих доступа к ИСПДн;

связанные с преднамеренными или непреднамеренными действиями лиц, имевших доступ к ИСПДн;

связанные с недостаточностью принимаемых организационных мер и программно-технических средств обеспечения информационной безопасности, определенных в результате проведения оценки защищенности ИСПДн;

нарушения целостности и доступности данных вследствие выхода из строя или сбоя в работе вычислительных средств, периферийного оборудования, средств хранения данных, коммуникационного оборудования, системной инфраструктуры, средств виртуализации, ПО и средств защиты информации и других программно-технических средств ИСПДн;

связанные со сбоями системы электроснабжения;

связанные с нарушением климатического режима и других условий эксплуатации оборудования.

2.5. Актуальные угрозы безопасности персональных данных в зависимости от архитектуры ИСПДн.

Выбор архитектуры прикладного ПО и средств доступа к ИСПДн значительным образом влияет на уровень опасности угроз, которые могут быть реализованы в отношении рабочих мест пользователей ИСПДн.

Уровень опасности угрозы в данном разделе определяется объемом персональных данных, в отношении которых в случае реализации угрозы будет нарушена их конфиденциальность, целостность или доступность.

Архитектуры ИСПДн подразделяются на следующие виды: автономная, файл-серверная, клиент-серверная, трехзвенная. Помимо этого, выделяется технология терминального доступа к ИСПДн.

2.5.1. Автономная ИСПДн.

Автономная ИСПДн представляет собой компьютер, на котором в полном объеме хранятся и обрабатываются персональные данные.

Актуальными угрозами безопасности персональных данных являются угрозы несанкционированного доступа ко всем персональным данным ИСПДн.

2.5.2. Файл-серверная ИСПДн.

В файл-серверных ИСПДн применяется несколько компьютеров, объединенных локальной вычислительной сетью. При этом данные хранятся в общей папке на одном из компьютеров (или сервере) и пользователи имеют доступ к файлам на запись и чтение.

Актуальными угрозами безопасности персональных данных являются угрозы несанкционированного доступа ко всем персональным данным ИСПДн.

2.5.3. Клиент-серверная ИСПДн.

В клиент-серверной архитектуре база данных ИСПДн обрабатывается на сервере специальным приложением – сервером баз данных, а данные запрашиваются с использованием структурированных запросов, сильно ограничивающих объем передаваемых данных.

Актуальными угрозами безопасности персональных данных являются угрозы:

несанкционированного доступа к персональным данным в объеме, который позволяет запросить, обработать и отобразить ПО пользователя (для рабочих мест пользователей ИСПДн и каналов их связи с сервером);

несанкционированного доступа ко всем персональным данным ИСПДн, хранящимся на сервере.

В случаях если клиент-серверная ИСПДн запрашивает и обрабатывает на рабочем месте пользователя полный объем данных, то угрозы в таких ИСПДн аналогичны угрозам, характерным для файл-серверной ИСПДн.

2.5.4. Трехзвенная ИСПДн.

В трехзвенной архитектуре ИСПДн между пользователем и сервером базы данных применяется сервер приложений, в задачу которого входит обработка и минимизация объема отображаемых данных на рабочем месте пользователя. При этом функции рабочего места пользователя, как правило, ограничены до просмотра набора данных или модификации набора данных.

Актуальными угрозами безопасности персональных данных являются угрозы:

несанкционированного доступа к персональным данным в объеме, который позволяет передать или получить от рабочего места пользователя сервер приложений (для рабочих мест пользователей, сервера приложений и каналов их связи);

несанкционированного доступа ко всем персональным данным ИСПДн, хранящимся на сервере.

2.5.5. Терминальный доступ к ИСПДн.

Терминальный режим доступа пользователя к ИСПДн функционирует на основе сервера терминалов, устанавливаемого между пользователем и сервером приложений или пользователем и сервером баз данных. Такой режим доступа может быть применен в комплексе с любой архитектурой ИСПДн. При этом на таком рабочем месте пользователя обрабатывается только изображение, полученное с сервера, и используются клавиатура и мышь.

Для терминального доступа к ИСПДн актуальными являются угрозы несанкционированного доступа к персональным данным в объеме, который отображается пользователю на экране (для рабочих мест пользователей, для каналов связи рабочих мест пользователей с сервером терминалов).

2.6. Актуальные угрозы в зависимости от особенностей ИСПДн.

2.6.1. При функционировании ИСПДн в вычислительной сети любого типа актуальными являются угрозы:

внедрения ложного объекта;

подмены доверенных объектов;

навязывания ложного маршрута;

удаленного запуска вредоносных приложений, в том числе путем использования уязвимостей;

сканирования, направленные на выявление конфигурации вычислительной сети.

2.6.2. При использовании в ИСПДн технологий виртуализации актуальными являются угрозы:

выхода процесса за пределы виртуальной машины;

нарушения изоляции пользовательских данных внутри виртуальной машины;

нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин;

неконтролируемого роста числа виртуальных машин;

несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной среды;

несанкционированного доступа к виртуальным каналам передачи информации;

несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети;

несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение;

несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;

несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин;

несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети;

несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;

несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;

перехвата управления средой виртуализации.

К технологиям виртуализации могут относиться виртуализация серверов, рабочих станций, хранилищ данных, приложений и сетей.

2.6.3. Для ИСПДн, в которых пользователям предоставлен неограниченный доступ к открытым ресурсам сети международного информационного обмена, актуальными являются угрозы:

внедрения вредоносных программ;

несанкционированной рассылки информации;

выведывания информации с использованием приемов социальной инженерии при осуществлении информационного обмена.

2.6.4. Для ИСПДн, элементы которых осуществляют публикацию общедоступной информации или обмен общедоступной информацией с сетью международного информационного обмена, актуальными являются угрозы:

сканирования, направленные на выявление конфигурации опубликованных сервисов;

удаленного запуска приложений путем использования уязвимостей в ПО и конфигурации опубликованных сервисов;

типа «отказ в обслуживании».

2.6.5. При осуществлении удаленного доступа к конфиденциальным ресурсам ИСПДн с использованием каналов и сетей связи, выходящих за пределы контролируемой зоны, или информационно-телекоммуникационных сетей международного информационного обмена актуальными являются угрозы:

сканирования, направленные на выявление конфигурации инфраструктуры удаленного доступа;

удаленного запуска приложений путем использования уязвимостей в ПО и конфигурации опубликованных сервисов;

анализа сетевого трафика с перехватом передаваемой информации в каналах, выходящих за пределы контролируемой зоны;

типа «отказ в обслуживании».

2.6.6. При использовании съемных носителей информации актуальными являются угрозы:

внедрения вредоносных программ;

кражи (утраты) съемных носителей и их попадания к посторонним лицам;

повреждения информации на носителе;

утечки информации при выводе носителя из эксплуатации;

использования копий данных на неучтенных носителях.

2.6.7. При осуществлении доступа к ИСПДн с персональных мобильных средств актуальными являются угрозы:

внедрения вредоносных программ на мобильные средства;

кражи (утраты) мобильных средств и их попадания к посторонним лицам;

утечки информации при выводе мобильного средства из эксплуатации.

2.6.8. При использовании беспроводных технологий связи актуальной является угроза анализа сетевого трафика с перехватом передаваемой по беспроводным каналам связи информации за пределами контролируемой зоны.

2.6.9. При использовании средств криптографической защиты информации (далее – СКЗИ) актуальными являются угрозы:

получения несанкционированного доступа к средствам криптографической защиты информации и средствам изготовления ключей шифрования и ключевых носителей;

кражи (утраты) и компрометации ключевой, аутентифицирующей и парольной информации СКЗИ;

кражи (утраты) экземпляра средства шифрования;

кражи (утраты), подмены документации на СКЗИ, а также внесения в нее несанкционированных изменений;

связанные с несоблюдением указанных в эксплуатационной документации к СКЗИ условий эксплуатации;

связанные с использованием стандартных паролей на носителях ключевой информации;

создания способов, подготовки и проведения атак на этапах разработки, производства и хранения СКЗИ;

создания способов, подготовки и проведения атак на этапе транспортировки СКЗИ;

создания способов, подготовки и проведения атак на этапе ввода СКЗИ в эксплуатацию (пусконаладочные работы);

создания способов, подготовки и проведения атак на этапе эксплуатации СКЗИ, в том числе:

проведения атак на персональные данные,

проведения атак на программные компоненты СКЗИ,

проведения атак на аппаратные компоненты СКЗИ,

проведения атак на программные компоненты, совместно с которыми штатно функционируют СКЗИ и в совокупности представляют среду функционирования СКЗИ (далее – СФ), включая ПО BIOS,

проведения атак на аппаратные компоненты СФ,

проведения атак на данные, передаваемые по каналам связи,

проведения атак на иные объекты, установленные при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее – АС) и ПО,

получения из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используются СКЗИ,

использования каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами,

использования каналов распространения сигналов, сопровождающих функционирование СКЗИ,

проведения атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети,

создания способов, подготовки и проведения атак без привлечения специалистов в области разработки и анализа СКЗИ,

проведения атаки за пределами контролируемой зоны,

проведения атаки путем применения находящихся в свободном доступе АС и ПО,

проведения атаки путем применения специально разработанных АС и ПО.

2.7. Перечень актуальных угроз безопасности ИСПДн КО уточняется и дополняется по мере выявления новых источников угроз безопасности, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Изменения Перечня актуальных угроз безопасности ИСПДн КО согласовываются министерством информационных технологий и связи Кировской области с ФСТЭК России и ФСБ России.

2.8. С целью обеспечения эффективного функционирования в Кировской области системы защиты информации ОИВ и организации согласовывают с министерством информационных технологий и связи Кировской области технические задания и проекты на создание ИСПДн.

3. Частные модели угроз ИСПДн

3.1. Частная модель угроз безопасности персональных данных при их обработке в ИСПДн или в сегменте ИСПДн разрабатывается организацией, на которую возложена обязанность по определению требований к обеспечению безопасности персональных данных в данной ИСПДн или в сегменте ИСПДн.

3.2. Частная модель угроз безопасности персональных данных при их обработке в ИСПДн разрабатывается на основе Перечня актуальных угроз безопасности ИСПДн КО с учетом особенностей, не определенных в настоящем Перечне актуальных угроз безопасности ИСПДн КО.

В рамках данной работы проводится подробный анализ структурно-функциональных характеристик конкретной ИСПДн, применяемых в ней информационных технологий, способов доступа к ИСПДн, особенностей ее функционирования и обслуживания, категорий обрабатываемой информации и пользователей ИСПДн.

Частная модель угроз безопасности персональных данных при их обработке в ИСПДн оформляется в форме документа и должна содержать:

описание ИСПДн и ее структурно-функциональных характеристик;

перечень угроз безопасности персональных данных и их описание, включающее описание возможностей нарушителя (модель нарушителя), возможных уязвимостей ИСПДн, способов реализации угроз безопасности и последствий от нарушения свойств безопасности персональных данных в зависимости от архитектуры и способов доступа к ИСПДн.

В случае если для обеспечения безопасности персональных данных, обрабатываемых в ИСПДн, необходимо использование СКЗИ, операторами ИСПДн при разработке частных моделей угроз в дополнение к угрозам безопасности персональных данных, определенным в соответсвии с пунктом 2.4 и подпунктом 2.6.9 пункта 2.6 настоящего Перечня актуальных угроз безопасности ИСПДн КО, также должны быть учтены угрозы, изложенные в методических рекомендациях ФСБ России № 149/7/2/6-432. При этом в частных моделях угроз необходимо привести обоснования признания угроз безопасности персональных данных неактуальными в виде перечня организационно-технических мер, реализация которых позволяет нейтрализовать такие угрозы, или перечня особенностей функционирования и организации эксплуатации информационной системы, делающих такие угрозы неактуальными. Типовой перечнь организационно-

технических мер приведен в приложении № 1 к методическим рекомендациям ФСБ России № 149/7/2/6-432.