ПРАВИТЕЛЬСТВО КАЛУЖСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

26 апреля 2018 г. № 258

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Калужской области

В соответствии с частью 5 статьи 19 Федерального закона «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 Калужской области, Правительство Калужской области **ПОСТАНОВЛЯЕТ:**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Калужской области, согласно приложению к настоящему постановлению.

2. Рекомендовать государственным учреждениям, подведомственным органам исполнительной власти Калужской области, руководствоваться угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Калужской области, указанными в приложении к настоящему постановлению.

3. Настоящее постановление вступает в силу со дня его официального опубликования.

Губернатор Калужской области **А.Д. Артамонов**

Приложение к постановлению
Правительства Калужской области
от 26.04.2018 г. № 258

УГРОЗЫ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ КАЛУЖСКОЙ ОБЛАСТИ

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных (далее – (ИСПДн) органов исполнительной власти Калужской области, определены для ИСПДн органов исполнительной власти Калужской области, эксплуатируемых при осуществлении соответствующих видов деятельности, в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

1.2. При определении угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн органов исполнительной власти Калужской области, используются термины и понятия, установленные Федеральным законом «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» (далее – Требования к защите персональных данных), 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 России (далее – ФСТЭК России) 14 февраля 2008 года, 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 Федеральной службой безопасности России 31 марта 2015 года № 149/7/2/6-432.

1.3. Под актуальными угрозами безопасности персональных данных при их обработке в ИСПДн органов исполнительной власти Калужской области 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 с персональными данными.

1.4. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн органов исполнительной власти Калужской области, подлежат адаптации при определении операторами ИСПДн угроз безопасности персональных данных, актуальных для конкретных ИСПДн органов исполнительной власти Калужской области.

2. Информационные системы персональных данных органов исполнительной власти Калужской области

2.1. ИСПДн органов исполнительной власти Калужской области создаются в целях реализации функций и осуществления полномочий, возложенных на органы исполнительной власти Калужской области в соответствии с законодательством, и эксплуатируются при осуществлении следующих видов деятельности:

ведение кадрового учёта;

ведение бухгалтерского учета;

работа с обращениями граждан;

оказание государственных услуг и исполнение государственных функций по направлениям деятельности органов исполнительной власти Калужской области.

2.2. В ИСПДн органов исполнительной власти Калужской области обрабатываются специальные, биометрические, общедоступные и иные категории персональных данных государственных гражданских служащих и работников органов исполнительной власти Калужской области, а также иных субъектов персональных данных.

2.3. В соответствии с Требованиями к защите персональных данных для ИСПДн органов исполнительной власти Калужской области актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

2.4. В соответствии с Требованиями к защите персональных данных для ИСПДн органов исполнительной власти Калужской области определен уровень защищенности персональных данных для каждой ИСПДн. Органами исполнительной власти Калужской области эксплуатируются ИСПДн от четвертого до второго уровня защищенности персональных данных включительно.

2.5. ИСПДн органов исполнительной власти Калужской области, эксплуатируемые при осуществлении соответствующих видов деятельности, имеют сходные структуры, однотипны.

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

2.7. Контролируемой зоной ИСПДн органов исполнительной власти Калужской области являются административные здания или отдельные помещения, в которых размещаются органы исполнительной власти Калужской области и ведется обработка и хранение персональных данных (далее – контролируемая зона).

2.8. В пределах контролируемой зоны находятся рабочие места пользователей ИСПДн органов исполнительной власти Калужской области, серверы, сетевое и телекоммуникационное оборудование. 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.

3. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн органов исполнительной власти Калужской области

3.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн органов исполнительной власти Калужской области, определенные в соответствии с методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 14 февраля 2008 года:

угрозы утечки видовой информации;

угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения несанкционированного доступа программ;

угрозы внедрения вредоносных программ;

кража носителей информации;

утрата ключей и атрибутов доступа;

непреднамеренная модификация (уничтожение) информации сотрудниками;

угроза «Анализ сетевого трафика» с перехватом передаваемой в ИСПДн информации за пределами контролируемой зоны;

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 другого;

угрозы выявления паролей по сети;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ;

угрозы несанкционированного доступа к образам виртуальных машин;

угрозы внедрения вредоносных программ в виртуальной машине.

Угрозы безопасности информации (далее – УБИ) из состава банка данных угроз безопасности информации (www.bdu.fstec.ru), актуальные в информационных системах персональных данных органов исполнительной власти Калужской области:

УБИ.003: Угроза анализа криптографических алгоритмов и их реализации;

УБИ.006: Угроза внедрения кода или данных;

УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию;

УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ.076: Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети;

УБИ.078: Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;

УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

УБИ.127: Угроза подмены действия пользователя путём обмана;

УБИ.170: Угроза неправомерного шифрования информации;

УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети;

УБИ.172: Угроза распространения «почтовых червей»;

УБИ.186: Угроза внедрения вредоносного кода через рекламу, сервисы и контент.

3.2. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для нарушения безопасности.

3.2.1. Реализация угроз безопасности персональных данных, обрабатываемых в ИСПДн, определяется возможностями источников атак.

В ИСПДн органов исполнительной власти Калужской области актуальной является возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны.

3.2.2. При выборе класса СКЗИ для защиты персональных данных, обрабатываемых в ИСПДн органов исполнительной власти Калужской области, в качестве актуальных рассматриваются следующие возможности создания способов подготовки и проведения атак:

а) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

б) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;

в) проведение атаки при нахождении вне контролируемой зоны;

г) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и на этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, и в совокупности представляющие среду функционирования СКЗИ (далее – СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ,

внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

д) проведение атак на этапе эксплуатации СКЗИ на:

персональные данные,

ключевую, аутентифицирующую и парольную информацию СКЗИ,

программные компоненты СКЗИ,

аппаратные компоненты СКЗИ,

программные компоненты СФ, включая программное обеспечение BIOS,

аппаратные компоненты СФ,

данные, передаваемые по каналам связи,

иные объекты, которые установлены 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 и программного обеспечения (далее – ПО);

е) получение 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 используется СКЗИ. При этом может быть получена следующая информация:

общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

сведения об информационных технологиях, базах данных, аппаратных средствах, ПО, используемых в ИСПДн совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, аппаратные средства, ПО, используемые в информационной системе совместно с СКЗИ;

содержание конструкторской документации на СКЗИ;

содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее – канал связи);

все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;

сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;

сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;

ж) применение:

находящихся в свободном доступе или используемых за пределами контролируемой зоны аппаратных средств и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

специально разработанных аппаратных средств и ПО;

з) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и(или) проведении атаки:

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

каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

и) проведение на этапе эксплуатации 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;

к) использование на этапе эксплуатации находящихся за пределами контролируемой зоны аппаратных средств и ПО из состава средств ИСПДн, применяемых на местах эксплуатации СКЗИ.

4. Меры по обеспечению безопасности информации при эксплуатации ИСПДн органов исполнительной власти Калужской области

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн органов исполнительной власти Калужской области, определены с учетом следующих мер обеспечения безопасности информации, которые в обязательном порядке принимаются при обработке персональных данных в органах исполнительной власти Калужской области:

4.1. Доступ к каждой ИСПДн осуществляется согласно утвержденному оператором ИСПДн в соответствии с законодательством перечню лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

4.2. В административных зданиях, в которых размещаются органы исполнительной власти Калужской области, установлен пропускной режим. Проход в здания и перемещение (вынос за пределы здания) компьютеров, коммуникационного оборудования и оргтехники производится по пропускам.

4.3. В органах исполнительной власти Калужской области обеспечивается защита ключевой информации СКЗИ от несанкционированного доступа потенциального нарушителя, при эксплуатации СКЗИ соблюдаются требования эксплуатационно-технической документации на СКЗИ и требования действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ.

4.4. Для обеспечения безопасности персональных данных при их обработке в ИСПДн органов исполнительной власти Калужской области используются СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Операторами ИСПДн принимаются дополнительные меры по обеспечению безопасности персональных данных в зависимости от угроз безопасности персональных данных, признанных актуальными для конкретных информационных систем.