



**ДЕПАРТАМЕНТ ИНФОРМАТИЗАЦИИ И СВЯЗИ
КРАСНОДАРСКОГО КРАЯ**

П Р И К А З

от 03.04.2018

№ 42

г. Краснодар

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

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Законом Краснодарского края от 1 июля 2008 года № 1517-КЗ «Об информационных системах и информатизации Краснодарского края», Положением о департаменте информатизации и связи Краснодарского края, утвержденным постановлением главы администрации (губернатора) Краснодарского края от 13 января 2011 года № 5, в целях реализации региональной политики в области информационной безопасности п р и к а з ы в а ю:

1. Утвердить Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Краснодарского края (далее – Перечень) согласно приложению к настоящему приказу.

2. Управлению связи департамента информатизации и связи Краснодарского края (Бугрий) обеспечить направление настоящего приказа в исполнительные органы государственной власти Краснодарского края, органы местного самоуправления муниципальных образований Краснодарского края для руководства данным Перечнем при выполнении мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

3. Отделу юридического обеспечения департамента информатизации и связи Краснодарского края (Лемонджава) обеспечить размещение (опубликование) настоящего приказа на официальном сайте администрации Краснодарского края в информационно-телекоммуникационной сети «Интернет» и направление настоящего приказа в департамент информационной политики Краснодарского края в целях размещения на «Официальном интернет-портал правовой информации» (www.pravo.gov.ru), управлению информатизации департамента информатизации и связи Краснодарского края

(Головченко) обеспечить размещение настоящего приказа на официальном сайте департамента информатизации и связи Краснодарского края в информационно-телекоммуникационной сети «Интернет» (<https://dis.krasnodar.ru>) в разделе «Департамент», подразделе «Нормотворческая деятельность департамента», подразделе «Приказы».

4. Контроль за исполнением настоящего приказа оставляю за собой.

5. Приказ вступает в силу на следующий день после его официального опубликования.

Руководитель департамента



Е.В. Юшков

ПРИЛОЖЕНИЕ

УТВЕРЖДЕН

приказом департамента информатизации
и связи Краснодарского края
от 03.04.2013 № 42

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Краснодарского края

1. В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 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.

2. Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Краснодарского края, сформирован на основе модели угроз безопасности информации информационных систем исполнительных органов государственной власти Краснодарского края и модели нарушителя безопасности информации информационных систем исполнительных органов государственной власти Краснодарского края, утвержденных 24 ноября 2016 года руководителем департамента информатизации и связи Краснодарского края.

3. В общем случае, угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных Краснодарского края, являются:

- угроза стихийных бедствий и природных явлений;
- угрозы социально-политического характера;
- угроза отказа электропитания серверного и телекоммуникационного оборудования;
- угроза отказа электропитания автоматизированных рабочих мест пользователей;

угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования;

угроза разглашения конфиденциальной информации пользователями информационной системы;

угроза разглашения конфиденциальной информации сотрудниками подрядных организаций;

угроза утраты мобильных технических средств пользователями информационной системы или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации;

угроза передачи носителей информации лицам, не имеющих права доступа к хранимой на них информации;

угроза утраты носителей информации;

угроза физического устаревания аппаратных компонентов информационной системы и (или) недостаточности вычислительных мощностей для решаемых задач;

угроза некорректной настройки программного обеспечения;

угроза использования информации идентификации/аутентификации, заданной по умолчанию;

угроза незащищённого удалённого администрирования информационной системы;

угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу);

угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом);

угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей);

угроза агрегирования данных, обрабатываемых с помощью мобильного устройства;

угроза утечки видовой информации;

угроза преодоления физической защиты;

угроза физического выведения из строя автоматизированных рабочих мест, обрабатывающих защищаемую информацию;

угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию;

угроза физического выведения из строя средств передачи информации;

угроза хищения автоматизированных рабочих мест, обрабатывающих защищаемую информацию;

угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию;

угроза хищения средств передачи информации;

угроза хищения носителей информации и мобильных технических средств;

- угроза изменения компонентов системы (аппаратной конфигурации) автоматизированных рабочих мест;
- угроза изменения компонентов системы (аппаратной конфигурации) серверов;
- угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
- угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам;
- угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;
- угроза подбора пароля;
- угроза использования уязвимостей используемого программного обеспечения;
- угроза установки уязвимых версий программного обеспечения;
- угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию;
- угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений;
- угроза подмены программного обеспечения;
- угроза внедрения вредоносного кода или данных на автоматизированных рабочих местах;
- угроза внедрения вредоносного кода или данных на серверах;
- угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет
- угроза нарушения функционирования веб-приложений;
- угроза получения сведений об информационной системе;
- угроза исследования работы приложения;
- угроза несанкционированного копирования защищаемой информации;
- угроза несанкционированного восстановления удалённой защищаемой информации;
- угроза использования технологий беспроводного доступа;
- угроза несанкционированного доступа к компонентам среды виртуализации;
- угроза приведения системы в состояние «отказ в обслуживании»;
- угроза реализации атаки «человек посередине» при передаче информации за пределы контролируемой зоны;
- угроза реализации атаки «человек посередине» при передаче информации за пределы контролируемой зоны;
- угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;
- угроза наличия ошибок в ходе проектирования, разработки и отладки системы;
- угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования;

- угроза слабости механизмов контроля входных данных;
- угроза слабости или некорректной настройки механизмов контроля целостности и резервирования данных;
- угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика;
- угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации;
- угроза анализа криптографических алгоритмов и их реализации;
- угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации;
- угроза несанкционированного воздействия на средство защиты информации;
- угроза несанкционированного изменения параметров настройки средств защиты информации;
- угроза проникновения из смежных информационных систем с более низким уровнем защищенности.

4. Возможности потенциальных нарушителей по подготовке и проведению атак на средства криптографической защиты информации (далее – СКЗИ), используемые для обеспечения безопасности персональных данных, включают:

- создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;
- создание способов, подготовка и проведение атак на этапе эксплуатации СКЗИ;
- проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств;
- внесение на этапе ввода в эксплуатацию СКЗИ 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 на этапе ввода в эксплуатацию СКЗИ несанкционированных изменений в документацию на СКЗИ и компоненты СФ;
- проведение атак на этапе эксплуатации СКЗИ на следующие объекты:
 - защищаемую информацию;
 - ключевую, аутентифицирующую и парольную информацию СКЗИ;
 - программные компоненты СКЗИ;
 - аппаратные компоненты СКЗИ;
 - программные компоненты СФ;
 - аппаратные компоненты СФ (аппаратные средства, входящие в СФ, включая микросхемы с записанным микрокодом BIOS, осуществляющей инициализацию этих средств);

- 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;

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, автоматизированных системах, программном обеспечении, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, автоматизированные системы, программное обеспечение, используемые в информационной системе совместно с 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;

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

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

- сведения обо всех проявляющихся в каналах связи, не защищённых 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;

применение находящихся в свободном доступе и/или специально разработанных используемых за пределами контролируемой зоны аппаратных средств и программного обеспечения, включая аппаратные и программные компоненты СКЗИ и СФ;

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 внутренних каналов связи и распространения сигналов:

- не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

- сопровождающих функционирование СКЗИ и СФ;

проведение на этапе эксплуатации СКЗИ атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеет выход в эти сети;

использование на этапе эксплуатации находящихся за пределами контролируемой зоны аппаратных средств и программного обеспечения из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства);

- проведение атаки при нахождении в пределах контролируемой зоны;

- проведение атак на этапе эксплуатации СКЗИ на документацию на СКЗИ и компоненты СФ;

- проведение атак на этапе эксплуатации СКЗИ на помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ;

- получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по разграничению доступа в помещения, в которых находятся программные и технические элементы систем обработки данных, способные функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ;

- использование штатных средств информационных систем персональных данных, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

- физический доступ к программным и техническим элементам систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ;

- воздействие на аппаратные компоненты СКЗИ и СФ, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

5. Актуальность угроз безопасности персональных данных для конкретных информационных систем (в том числе угрозы наличия недекларированных возможностей в системном и прикладном программном обеспечении) должна определяться при разработке частных моделей угроз безопасности персональных данных с учетом архитектуры, структуры (топологии), назначения информационных систем, состава и критичности обрабатываемой информации, реализованных мер защиты информации. Разработка частных моделей угроз безопасности персональных данных должна осуществляться с учетом положений модели угроз безопасности информации информационных систем исполнительных органов государственной власти Краснодарского края и модели нарушителя безопасности информации информационных систем исполнительных органов государственной власти Краснодарского края, утвержденных 18 декабря 2017 года руководителем департамента информатизации и связи Краснодарского края.

Руководитель департамента



Е.В. Юшков