АДМИНИСТРАЦИЯ КОСТРОМСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ
от 3 апреля 2017 г. N 137-а

ОБ ОПРЕДЕЛЕНИИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫХ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ КОСТРОМСКОЙ ОБЛАСТИ

В соответствии с Федерального закона от 27 июля 2006 года N 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 исполнительных органов государственной власти Костромской области, взаимодействующих с информационными системами персональных данных администрации Костромской области, администрация Костромской области постановляет:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных администрации Костромской области, согласно приложению к настоящему постановлению.

2. Исполнительным органам государственной власти Костромской области:

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

2) руководствоваться настоящим постановлением при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, взаимодействующих с информационными системами персональных данных администрации Костромской области.

3. Управлению информатизации и связи администрации Костромской области разместить настоящее постановление:

на официальном сайте администрации Костромской области;

в информационно-телекоммуникационной сети "Интернет" в течение 10 дней со дня его принятия.

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

Губернатор
Костромской области
С.СИТНИКОВ

Приложение
к постановлению
администрации
Костромской области
от 3 апреля 2017 г. N 137-а

УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ КОСТРОМСКОЙ ОБЛАСТИ

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных администрации Костромской области (далее - Актуальные угрозы безопасности ИСПДн АКО), разработаны в соответствии с Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных".

2. Актуальные угрозы безопасности ИСПДн АКО содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) администрации Костромской области.

3. При разработке Актуальных угроз безопасности ИСПДн АКО использованы нормативные правовые акты:

1) Федеральный от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

2) Федеральный от 27 июля 2006 года N 152-ФЗ "О персональных данных";

3) Президента Российской Федерации от 17 марта 2008 года N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

4) Президента Российской Федерации от 22 мая 2015 года N 260 "О некоторых вопросах информационной безопасности Российской Федерации";

5) Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

6) Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 18 февраля 2013 года N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (далее - Приказ ФСТЭК России);

7) Федеральной службы безопасности Российской Федерации (далее - ФСБ России)

от 10 июля 2014 года N 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);

8) ФСБ России от 9 февраля 2005 года N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)";

9) 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, утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 года N 149/7/2/6-432 (далее - Методические рекомендации ФСБ России по разработке НПА);

10) определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России от 14 февраля 2008 года;

11) угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России от 15 февраля 2008 года (далее - Базовая модель угроз).

4. Угрозы безопасности персональных данных, обрабатываемые в ИСПДн администрации Костромской области, приведенные в Актуальных угрозах безопасности ИСПДн АКО, подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных.

5. Частная модель угроз безопасности персональных данных разрабатывается в соответствии с угроз и с учетом требований ФСТЭК России и ФСБ России.

6. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик конкретной ИСПДн и применяемых в ней информационных технологий, а также особенностей ее функционирования, в том числе с использованием банка данных угроз безопасности информации (www.bdu.fstec.ru).

7. В частной модели угроз безопасности персональных данных указываются:

1) описание ИСПДн и ее структурно-функциональных характеристик;

2) описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя);

3) описание возможных уязвимостей ИСПДн, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

8. Персональные данные субъектов персональных данных обрабатываются с целью обеспечения деятельности администрации Костромской области и исполнительных органов государственной власти Костромской области (далее - ИОГВ).

9. Актуальные угрозы безопасности персональных данных, обрабатываемые в ИСПДн, содержащиеся в Актуальных угрозах безопасности ИСПДн АКО, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн администрации Костромской области. Указанные изменения согласовываются с ФСТЭК России и ФСБ России в установленном порядке.

10. ИСПДн администрации Костромской области характеризуются тем, что в качестве объектов информатизации выступают распределенные ИСПДн, имеющие подключение к информационно-телекоммуникационным сетям общего пользования (далее - сети общего пользования) и (или) информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет").

11. ИСПДн ИОГВ характеризуются тем, что в качестве объектов информатизации выступают автоматизированные рабочие места, имеющие подключение к ИСПДн администрации Костромской области, а также подключение к сетям общего пользования и (или) сети "Интернет".

12. ИСПДн администрации Костромской области и ИСПДн ИОГВ имеют различную структуру, являются разноплановыми системами.

13. Ввод персональных данных в ИСПДн администрации Костромской области и ИСПДн ИОГВ, а также вывод данных из ИСПДн администрации Костромской области и ИСПДн ИОГВ осуществляется с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные носители информации, в том числе и компакт-диски.

14. Информационный обмен персональными данными по сетям общего пользования и (или) сети "Интернет" осуществляется с использованием сертифицированных шифровальных (криптографических) средств защиты информации (далее - СКЗИ).

15. Технические средства ИСПДн администрации Костромской области и ИСПДн ИОГВ размещаются на территории Российской Федерации.

16. Базы данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, находятся на территории Российской Федерации.

17. Контролируемой зоной ИСПДн администрации Костромской области и ИСПДн ИОГВ являются административные здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн администрации Костромской области и ИСПДн ИОГВ. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям общего пользования и (или) сети "Интернет".

18. 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.

19. Защита персональных данных в ИСПДн администрации Костромской области и ИСПДн ИОГВ и сетях общего пользования, подключаемых к сети "Интернет",

обеспечивается средствами защиты информации (далее - СЗИ):

1) средствами антивирусной защиты, сертифицированными ФСТЭК России, не ниже 4 класса;

2) межсетевыми экранами, сертифицированными ФСТЭК России, не ниже 3 класса;

3) СКЗИ, формирующими виртуальные частные сети (VPN), сертифицированными ФСБ России по классу КС1 и выше;

4) средством государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Глава 2. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

20. Учитывая особенности обработки персональных данных в администрации Костромской области, а также категорию и объем обрабатываемых в ИСПДн администрации Костромской области 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 ИСПДн администрации Костромской области обеспечивать сохранность и неизменность персональных данных при попытках несанкционированных воздействий на них в процессе обработки или хранения.

Доступность - состояние персональных данных, при котором субъекты, имеющие право доступа, могут реализовать его беспрепятственно.

21. Под 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 ИСПДн администрации Костромской области, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

22. Для ИСПДн администрации Костромской области актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием недокументированных (недекларированных) возможностей (далее - НДВ) в системном и прикладном программном обеспечении (далее - ПО), используемом в ИСПДн администрации Костромской области.

23. ИСПДн администрации Костромской области обрабатывают персональные данные сотрудников администрации Костромской области и (или) иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками администрации Костромской области.

24. Исходя из состава обрабатываемых персональных данных и типа актуальных

угроз определяется, что для обеспечения безопасности персональных данных в ИСПДн администрации Костромской области необходимо обеспечение четвертого уровня защищенности персональных данных (УЗ 4).

25. Основной целью применения СКЗИ в ИСПДн администрации Костромской области является защита персональных данных, в том числе при информационном обмене по сетям общего пользования и (или) сети "Интернет".

26. Объектами защиты являются:

1) персональные данные;

2) СКЗИ;

3) среда функционирования СКЗИ (далее - СФ);

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

5) документы, дела, журналы, картотеки, издания, технические документы, рабочие материалы, в которых отражена защищаемая информация, относящаяся к ИСПДн администрации Костромской области и их криптографической защите, включая документацию на СКЗИ и технические и программные компоненты СФ;

6) носители защищаемой информации, используемые в ИСПДн администрации Костромской области в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

7) используемые ИСПДн администрации Костромской области каналы (линии) связи, включая кабельные системы;

8) помещения, в которых находятся ресурсы ИСПДн администрации Костромской области, имеющие отношение к криптографической защите персональных данных.

27. Основными видами угроз безопасности для персональных данных в ИСПДн администрации Костромской области являются:

1) угрозы утечки информации по техническим каналам:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналам побочного электромагнитного излучения и наводки;

2) угрозы несанкционированного доступа (далее - НСД) к информации:

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

кража персональной электронно-вычислительной машины (далее - ПЭВМ);

кража носителей информации;

кража ключей доступа;

кража, модификация, уничтожение информации;

вывод из строя узлов ПЭВМ, каналов связи;

несанкционированное отключение СЗИ;

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

действия вредоносных программ (вирусов);

установка ПО, не связанного с исполнением служебных обязанностей;

угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты персональных данных в ее составе из-за сбоев в ПО, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного характера (ударов молний, пожаров, наводнений):

утрата ключей и атрибутов доступа;

непреднамеренная модификация (уничтожение) информации сотрудниками;

непреднамеренное отключение СЗИ;

выход из строя аппаратно-программных средств;

сбой системы электроснабжения;

стихийное бедствие;

угрозы преднамеренных действий внутренних нарушителей:

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

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

угрозы НСД по каналам связи:

угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

перехват за пределами с 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.

28. Основные целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных в ИСПДн администрации Костромской области или создания условий для этого (далее - атака), при создании способов, подготовке и проведении которых используются возможности из числа следующих:

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

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

3) проведение атаки, находясь вне контролируемой зоны;

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

внесение несанкционированных изменений в СКЗИ и (или) в СФ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ (вирусов);

внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

5) 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 ПО BIOS;

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

иные объекты, которые установлены при формировании совокупности предложений 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;

6) получение из находящихся в свободном доступе источников (включая сети общего пользования и (или) сеть "Интернет") информации об ИСПДн, в которой используется СКЗИ. При этом может быть получена следующая информация:

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

сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИСПДн совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в ИСПДн 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 НСД к информации организационными и техническими мерами;

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

сведения обо всех проявляющихся в каналах связи, не защищенных от НСД 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;

7) применение:

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

специально разработанных АС и ПО;

8) 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 НСД к информации организационными и техническими мерами;

каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

9) проведение на этапе эксплуатации атаки из сетей общего пользования и (или) сети "Интернет", если ИСПДн, в которых используются СКЗИ, имеют выход в эти сети;

10) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств ИСПДн, применяемых на местах эксплуатации СКЗИ (далее - штатные средства);

11) проведение атаки при нахождении в пределах контролируемой зоны;

12) проведение атак на этапе эксплуатации СКЗИ на следующие объекты:

документацию на СКЗИ и компоненты СФ;

помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;

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

сведений о физических мерах защиты объектов, в которых размещены ресурсы ИСПДн;

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИСПДн;

сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

14) использование штатных средств, ограниченное мерами, реализованными в ИСПДн, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

15) физический доступ к СВТ, на которых реализованы СКЗИ и СФ;

16) возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в ИСПДн, в которой используется СКЗИ, и направленными на предотвращение и пресечение НСД;

17) создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак НДВ прикладного ПО;

18) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в ИСПДн, в которой используется СКЗИ, и направленными на предотвращение и пресечение НСД;

19) проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и

СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ;

20) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ системного ПО;

21) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ;

22) возможность располагать всеми аппаратными компонентами СКЗИ и СФ.

29. Угрозы, перечисленные в пункте 28 Актуальных угроз безопасности ИСПДн АКО, которые могут быть нейтрализованы только с помощью СКЗИ, учитываются при разработке частных моделей угроз безопасности персональных данных в соответствии с Методических рекомендаций ФСБ России по разработке НПА.

Глава 3. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИСПДН АКО

30. Актуальными угрозами безопасности ИСПДн АКО являются угрозы НСД к персональным данным:

1) действия вредоносных программ (вирусов);

2) утрата ключей и атрибутов доступа;

3) перехват передаваемой из ИСПДн и принимаемой из внешних сетей информации за пределами контролируемой зоны;

4) НСД через сеть "Интернет";

5) НСД через локальную вычислительную сеть организации;

6) утечка атрибутов доступа;

7) 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.;

8) угрозы выявления паролей по сети;

9) угрозы подмены доверенного объекта в сети;

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

11) угрозы типа "Отказ в обслуживании";

12) угрозы удаленного запуска приложений;

13) угрозы внедрения по сети вредоносных программ.

31. Актуальными угрозами безопасности ИСПДн АКО со СКЗИ являются атаки, при создании способов, подготовке и проведении которых используются возможности из числа следующих:

1) создание способов, подготовка и проведение атак без привлечения специалистов в

области разработки и анализа СКЗИ;

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

3) проведение атаки, находясь вне контролируемой зоны;

4) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) атаки по внесению несанкционированных изменений в СКЗИ и (или) в СФ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ (вирусов);

5) 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 ПО BIOS;

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

6) получение из находящихся в свободном доступе источников (включая сети общего пользования и (или) сеть "Интернет") информации об ИСПДн, в которой используется СКЗИ. При этом может быть получена следующая информация:

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

сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИСПДн совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в ИСПДн 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;

7) применение находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

8) применение специально разработанных АС и ПО;

9) проведение на этапе эксплуатации атаки из сетей общего пользования и (или) сети "Интернет", если ИСПДн, в которых используются СКЗИ, имеют выход в эти сети;

10) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава штатных средств.