Приложение №1
к приказу ФГБУ СПбНИИФК
от 07.12.2018 № 5 о/д

УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФГБУ СПбНИИФК

№ п/п	Наименование угрозы
1	**Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных (далее – информационные системы) ФГБУ СПбНИИФК**
1.1	угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее - СКЗИ);
1.2.	угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого.
2	**Угрозы безопасности персональных данных, защищаемых без использования СКЗИ, включают:**
2.1.	угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации
2.2.	угрозы несанкционированного доступа (воздействия) к персональным данным лицами, обладающими полномочиями в информационных системах, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационных систем
2.3	угрозы воздействия вредоносного кода, вредоносной программы, внешних по отношению к информационным системам
2.4	угрозы использования методов социального инжиниринга к лицам, обладающим полномочиями в информационных системах
2.5	угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем

2.6	угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных
2.7	угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в системном и прикладном программном обеспечении информационных систем
2.8	угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных, в том числе с использованием протоколов межсетевого взаимодействия
2.9	угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем
2.10	угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации
2.11	угрозы, связанные с возможностью использования новых информационных технологий (технологии виртуализации, беспроводные технологии, облачные технологии, технологии удаленного доступа и иные новые технологии)
3	**Угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого включают:**
3.1.	создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ
3.2	создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ
3.3	проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона)
3.4	проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

а)	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
б)	внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ
3.5.	проведение атак на этапе эксплуатации СКЗИ на:
а)	персональные данные
б)	программные компоненты СКЗИ
в)	аппаратные компоненты СКЗИ
г)	программные компоненты СФ, включая программное обеспечение BIOS
д)	аппаратные компоненты СФ
е)	ключевую, аутентифицирующую и парольную информацию СКЗИ
ж)	данные, передаваемые по каналам связи
з)	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 (далее - АС) и программного обеспечения (далее - ПО)
3.6.	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:
а)	общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы)
б)	сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ

в)	содержание конструкторской документации на СКЗИ
г)	содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ
д)	общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ
е)	сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи)
ж)	все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами
з)	сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ
и)	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
к)	сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ
3.7	Применение:
а)	находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ
б)	специально разработанных АС и ПО
3.8	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:
а)	каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;
б)	каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;
3.9	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

3.10	проведение атаки при нахождении в пределах контролируемой зоны
3.11	проведение атак на этапе эксплуатации СКЗИ на следующие объекты
а)	документацию на СКЗИ и компоненты СФ;
б)	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
3.12	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:
а)	сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы
б)	сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы
в)	сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ
3.13	использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий
3.14	физический доступ к СВТ, на которых реализованы СКЗИ и СФ
3.15	возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий