РЕСПУБЛИКАНСКОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«БАСКЕТБОЛЬНАЯ ШКОЛА ВЫСШЕГО МАСТЕРСТВА»
(РГБУ «БШВМ»)

УТВЕРЖДЕНЫ
приказом РГБУ «БШВМ»
от 26.12.2019 № 53

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных

г. Черкесск
2019

Республиканское государственное бюджетное учреждение „Баскетбольная школа высшего мастерства" с 10 января 2020 года переименовано в Республиканское государственное бюджетное учреждение „Спортивная школа по баскетболу" на основании Постановления Правительства Карачаево-Черкесской Республики от 23 декабря 2019 года „О переименовании государственных бюджетных учреждений Карачаево-Черкесской Республики, подведомственных Министерству физической культуры и спорта Карачаево-Черкесской Республики".

1. К угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных в РГБУ «БШВМ» (далее - информационные системы), относятся:

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 воздействия на лиц, обладающих 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.

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 нарушителем, находясь вне пространства, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных 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:

3.4.1. 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;

3.4.2. внесение несанкционированных изменений в технические и организационно-распорядительные документы на СКЗИ и компоненты СФ;

3.5. проведение атак на этапе эксплуатации СКЗИ на:

3.5.1. персональные данные;

3.5.2. ключевую, аутентифицирующую и парольную информацию СКЗИ;

3.5.3. программные компоненты СКЗИ;

3.5.4. аппаратные компоненты СКЗИ;

3.5.5. программные компоненты СФ, включая программное обеспечение базовых систем ввода (вывода);

3.5.6. аппаратные компоненты СФ;

3.5.7. данные, передаваемые по каналам связи;

3.5.8. 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") следующей информации об информационной системе, в которой используется СКЗИ:

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

3.6.2. 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;

3.6.3. содержание конструкторской документации на СКЗИ;

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

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

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

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

3.6.8. сведения о нарушениях правил эксплуатации СКЗИ и СФ в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

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

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

3.7. применение:

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

3.7.2. 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:

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

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

3.11. проведение атаки при нахождении в пределах контролируемой зоны;

3.12. на этапе эксплуатации СКЗИ возможное уничтожение и несанкционированный доступ к:

3.12.1. документации на СКЗИ и компоненты СФ;

3.12.2. помещениям, 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;

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

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

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

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

3.14. использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

3.15. физический доступ к СВТ, на которых реализованы СКЗИ и СФ;

3.16. наличие у нарушителя аппаратных компонентов СКЗИ и СФ, реализованных в информационной системе, в которой используется СКЗИ.