УТВЕРЖДАЮ

И.о. директора МБУ ДО МУК г. Азова
_____ З.Ю. Гриценко
Приказ от 06.02.2020г. № 12

УГРОЗЫ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ МЕЖШКОЛЬНЫЙ УЧЕБНЫЙ КОМБИНАТ г. АЗОВА

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных работников МБУ ДО МУК г. Азова являются:
- угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее - СКЗИ);
- угрозы реализации 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 лиц, обладающих полномочиями в информационных системах, в том числе в ходе создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации информационных систем и дальнейшего хранения содержащейся в их базах данных информации;
2.3 угрозы воздействия вредоносного кода и (или) вредоносной программы, внешних по отношению к информационным системам;
2.4 угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем;
2.5 угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных, в том числе с использованием протоколов межсетевого взаимодействия;

2.6 угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем;
2.7 угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации лицами, обладающими административными полномочиями в информационных системах;
2.8 угрозы, связанные с возможностью использования новых информационных технологий.

3. Угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого (далее - атака) включают:

1) угрозы проведения атаки вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);

2) угрозы проведения на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ атаки путем внесения несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и которые в совокупности представляют среду функционирования СКЗИ (далее - СФ), а также которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

3) угрозы проведения атак на этапе эксплуатации СКЗИ на:

а) ключевую, аутентифицирующую и парольную информацию СКЗИ;
б) программные компоненты СКЗИ;
в) аппаратные компоненты СКЗИ;
г) программные компоненты СФ, включая базовую систему ввода (вывода);
д) аппаратные компоненты СФ;
е) данные, передаваемые по каналам связи;

4) угрозы получения 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 информационных системах, в которых используются СКЗИ:

а) общих сведений об информационных системах, в которых используются СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационных систем);

б) сведений об информационных технологиях, базах данных, аппаратных средствах (далее - АС), программном обеспечении (далее - ПО), используемых в информационных системах совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационных системах совместно с СКЗИ;
в) содержания конструкторской документации и эксплуатационных документов на аппаратные и программные компоненты СКЗИ и СФ, включающих сведения о составе, характеристиках, устройстве, условиях и правилах эксплуатации конкретных технических средств и систем обработки и защиты информации;
г) общих сведений о защищаемой информации, используемой в процессе эксплуатации СКЗИ;
д) сведений о каналах связи, по которым передаются защищаемые СКЗИ персональные данные;
е) сведений, получаемых в результате анализа любых доступных для перехвата сигналов от аппаратных компонентов СКЗИ и СФ;

5) угрозы применения специально разработанных АС и ПО;

6) угрозы использования 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 распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

7) угрозы проведения атаки при нахождении в пределах контролируемой зоны;

8) угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений:

а) сведений о физических мерах защиты объектов, в которых размещены ресурсы информационных систем;
б) сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационных систем;
в) сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы СКЗИ и СФ;

9) угрозы физического доступа к средствам вычислительной техники, на которых реализованы СКЗИ и СФ.