**Сертификация по требованиям информационной безопасности
– надежный механизм киберзащиты.**

По мере развития информационного общества возрастает опасность и значимость угроз кибератак для безопасности функционирования государственных организаций и объектов хозяйственного и социально-культурного назначения.

Важность данной проблемы подчеркивает тот факт, что согласно принятому Закону Республики Узбекистан «О кибербезопасности» на государственные органы и организации возлагается обязанность по использованию сертифицированных аппаратных, аппаратно-программных и программных средств для киберзащиты своих информационных систем и ресурсов.

В обязательном порядке подлежат сертификации аппаратные, аппаратно-программные и программные средства, применяемые для обеспечения кибербезопасности информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры, функционирующих:

- в сфере государственного управления и оказания государственных услуг,

- обороны,

- обеспечения государственной безопасности, правопорядка,

- топливно-энергетического комплекса (атомной энергетики),

- химической, нефтехимической отраслях,

- металлургии,

- водопользования и водоснабжения,

- сельского хозяйства,

- здравоохранения,

- жилищно-коммунального обслуживания,

- банковско-финансовой системы,

- транспорта,

- информационно-коммуникационных технологий,

- экологии и охраны окружающей среды,

- добычи и переработки полезных ископаемых стратегического значения,

- производственной сфере,

- в других отраслях экономики и социальной сфере.

Основные обязательные требования, применяемые при сертификации, регламентируются государственными стандартами:

O‘z DSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;

O‘z DSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации»;

O‘z DSt 2816:2014 «Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей»;

O‘z DSt 2817:2014 «Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации».

Стандарт O‘z DSt 2814 устанавливает требования по защите информации в автоматизированных системах (АС) различных классов, при этом выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

Специалисты ГУП «Центр кибербезопасности» готовы оказать содействие по данному вопросу на любом этапе проектирования, разработки и внедрения АС.

Согласно стандарту O‘z DSt 2814 во всех АС, предназначенных для обработки или хранения информации, отнесенной к государственным секретам и конфиденциальной информации (независимо от класса защищенности), должны применяться:

- межсетевые экраны, сертифицированные по O‘z DSt 2815;

- программное обеспечение средств защиты информации (в том числе встроенных в общесистемное и прикладное ПО), сертифицированное
по O‘z DSt 2816 на отсутствие недекларированных возможностей;

- средства вычислительной техники, сертифицированные по O‘z DSt 2817.

Помимо указаний на необходимость применения при разработке АС других стандартов (O‘z DSt 2815 – O‘z DSt 2817), стандарт O‘z DSt 2814 содержит собственные проверяемые при сертификации требования к ряду подсистем комплекса программно-технических средств по защите информации от несанкционированного доступа:

- управления доступом;

- регистрации и учёта;

- криптографической защиты;

- обеспечения целостности программного обеспечения и данных.

Необходимо учитывать, что стандарт O‘z DSt 2814 имеет широкую область применения и содержит не только технические требования, проверяемые при сертификации, но и организационные решения, которые государственным организациям и собственникам объектов КИИ необходимо будет выполнять на этапах внедрения и обеспечения функционирования своих информационных систем.

Стандарт O‘z DSt 2815 устанавливает классификацию межсетевых экранов (файерволов, брандмауэров) по уровню защищенности от несанкционированного доступа к информации в соответствии с показателями защищенности, в частности определяемыми следующими их функциональными характеристиками:

- управление доступом (фильтрация данных и трансляция адресов);

- идентификация и аутентификация;

- регистрация;

- администрирование, восстановление и ряд других.

С учётом данного обстоятельства, основным методом сертификационных испытаний межсетевых экранов является тестирование их функциональных возможностей на соответствие установленным требованиям и технической документации разработчиков.

Требования стандарта O‘z DSt 2816 распространяются **на все виды средств защиты информации** (как отечественного, так и импортного производства) и регламентируют порядок контроля их программного обеспечения в части отсутствия в нем недекларированных возможностей. **Получение сертификата соответствия согласно стандарту O‘z DSt 2816 до ввода в эксплуатации средств защиты информации, является обязательным.**

Для выполнения такого контроля методика проведения сертификационных испытаний на соответствие требованиям стандарта O‘z DSt 2816 подразумевает предоставление в испытательную лабораторию исходного текста программного обеспечения с описанием всех реализуемых им функций, и его загрузочных кодов, для проведения их изучения и сопоставительного анализа.

Стандарт O‘z DSt 2817 устанавливает требования к операционным системам, на базе которых реализуется информационная система, обеспечивая контроль показателей их защищенности по ряду функциональных параметров:

- контроль доступом;

- идентификация и аутентификация;

- очистка памяти;

- маркировка документов;

- защита ввода и вывода информации на съемный носитель информации, и ряда других.

В целом, как видно из вышеизложенного, применяемые при сертификации в ГУП «Центр кибербезопасности» государственные стандарты образуют единый комплекс требований, позволяющий всесторонне удостовериться в надежности киберзащиты информационных систем.

ГУП «Центр кибербезопасности» располагает современными испытательными средствами и высококвалифицированными специалистами в области сертификации, оказывающими содействие государственным организациям, собственникам объектов критической информационной инфраструктуры, разработчикам и поставщикам ПО в реализации требований Закона Республики Узбекистан «О кибербезопасности» для обеспечения надежной защиты информации от киберугроз.