**Выступление заместителя начальника Государственной Службы Специальной Связи и Информационной Безопасности Азербайджанской Республики генерал-майора Аллахверана Исмайлова на мероприятии «TurkmenTEL-2023», которое пройдет 9-10 ноября 2023 года в городе Ашхабад, Туркменистан**

**Уважаемые участники конференции!**

**Дамы и господа!**

Рад приветствовать вас на конференции «TurkmenTEL-2023» и хочу выразить искреннюю благодарность Правительству Туркменистана и организаторам за приглашение и организацию столь масштабного мероприятия, а также за оказанный теплый прием и гостеприимство. Хотел бы выразить удовлетворение возможностью обсудить проблематику в области кибербезопасности, одной из важнейших и постоянно развивающихся тем современности, на данном мероприятии, -- где демонстрируются новые технологии, создаются интересные возможности, налаживается сотрудничество.

Позвольте мне сначала поделиться информацией об организации, которую я представляю. Государственная Служба Специальной Связи и Информационной Безопасности Азербайджанской Республики была образована Указом Президента Азербайджанской Республики от 16 марта 2020 года, выделившись в отдельную, самостоятельную структуру. Данная Служба была создана в целях организации, эксплуатации, и обеспечения безопасного развития специальных информационно-коммуникационных систем и сетей для государственных органов Азербайджанской Республики, а также для подключения государственных органов к сети Интернет, и размещения соответствующих информационных ресурсов в едином защищенном информационно-ресурсном центре.

Служба осуществляет свою деятельность по следующим направлениям:

- обеспечение безопасности критической информационной инфраструктуры государственных органов (учреждений) совместно с соответствующими государственными органами, в том числе борьба с киберугрозами;
- мониторинг параметров безопасности информационных ресурсов сети Интернет и информационных систем государственных органов (учреждений) с целью оказания соответствующей технической и методической помощи в целях повышения их кибербезопасности;

- обеспечение безопасности и защищенности системы межведомственного электронного документооборота между государственными органами (учреждениями) ;
- организация и совершенствование криптологической деятельности; предотвращение утечки информации из технических каналов;
- выделение защищенных каналов связи на основании запроса государственных органов (учреждений);
- сбор и анализ киберинцидентов в государственных органах (учреждениях) и информирование соответствующих органов об обнаруженных утечках информации;
- участие в разработке государственных стандартов и классификаций по информационной безопасности;

Хотел бы подчеркнуть, что Государственная Служба Специальной Связи и Информационной Безопасности Азербайджанской Республики сотрудничает с международными партнерами в сфере кибербезопасности, борьбы с киберугрозами и киберпреступностью. Наглядным примером тому является подписание Меморандумов о взаимопонимании между нашей Службой и соответствующими организациями ряда других стран о сотрудничестве в борьбе с киберугрозами, организации обмена информацией и опытом по обеспечению кибербезопасности. Один из таких Меморандумов был подписан и на этом мероприятии с братским государством Туркменистан. Не лишним будет отметить, что подобные соглашения имеют большое значение для развития международного сотрудничества в данной сфере.

В современную эпоху развитие и внедрение все более совершенных технологий, систем управления, и программных продуктов привело также к повышенному риску уязвимости данных систем, что, в свою очередь, сделало кибербезопасность решающим фактором. В целях продолжения развития этой сферы в Азербайджане 28 августа 2023 года была принята «Национальная стратегия Азербайджанской Республики по информационной безопасности и кибербезопасности на 2023-2027 годы», направленная на повышение уровня национальной информационной безопасности в целях обеспечения безопасного использования современных ИКТ государством, обществом и народом. Стоит отметить, что международные организации уделяют особое внимание наличию стратегии информационной безопасности или кибербезопасности, что также является одним из основных критериев, влияющих на рейтинг стран по кибербезопасности.

Согласно этой Стратегии, в сфере обеспечения информационной безопасности и кибербезопасности в Азербайджанской Республике планируется стратегическое планирование деятельности по определенным направлениям, которые указаны в Стратегии и поэтапная реализация.

При этом по следующим важным направлениям основным исполнительным органом назначена Государственная Служба Специальной связи и Информационной Безопасности :

- Выявление и классифицирование категорий угроз информационной безопасности и кибербезопасности в информационном пространстве
- Формирование культуры информационной безопасности и кибербезопасности в государственных органах (учреждениях), частных организациях – принятие мер по обеспечению кибергигиены
- Определение форм сотрудничества государственных органов (учреждений), частного сектора и институтов гражданского общества по обеспечению информационной безопасности и кибербезопасности, в том числе по принятию мер против инцидентов, и создание их правовой основы

Необходимо также отметить что обеспечение информационной безопасности и защиты данных требует не только соответствующего оборудования, но и соблюдения правил безопасности при использовании Интернета и данных. Цифровая трансформация и технологическое развитие требуют от сотрудников частного и, особенно, государственного сектора все более внимательного подхода к мерам кибербезопасности. При содействии Центра по борьбе с компьютерными инцидентами при Государственной Службе Специальной Связи и Информационной Безопасности Азербайджанской Республики в мае 2022 года была создана Платформа сотрудничества по кибергигиене, в рамках которой было запланировано проведение образовательных мероприятий и тренингов по кибербезопасности с целью защиты учреждений и компаний от существующих или потенциальных угроз, а также рисков.

Принимая во внимание вышесказанное, важно, чтобы сотрудники информационных инфраструктур повышали свои знания в области информационной безопасности и использовали выделенные для служебного использования информационные технологии только по прямому назначению, соблюдали политику информационной безопасности. Для решения подобной задачи 26-27 октября текущего года в Азербайджане, при совместной организации нашей Службы и Службы Государственной Безопасности

Азербайджанской Республики было успешно проведено мероприятие «Critical Infrastructure Defence Challenge (Задача Защиты Критической Инфраструктуры) (CIDC-2023)», включившее в себя конференции на злободневные темы, мастер-классы по современным технологиям и продуктам, а также впервые в нашей стране соревнование «Кибервойна», организованное для защиты критически важных инфраструктур, с моделированием кибератак, практически полностью идентичных реальным. Презентации и панельные дискуссии по информационной безопасности, викторины и тренинги в контексте данной сферы, выставка передовых продуктов и решений, которую проводили местные и иностранные ИТ-компании для государственного и частного сектора, студентов и специалистов, -- все это составные части данного Мероприятия. Не лишним будет отметить, что планируется продолжить подобные мероприятия в нашей стране в ближайшие годы, как в специализированной форме для локальных инфраструктур, так и в формате соревнований по кибервойне международного уровня.

Резюмируя, хочу напомнить, что в современную эпоху, когда киберугрозы развиваются и продолжают совершенствоваться, кибербезопасность остается постоянной проблемой. Поэтому для эффективной борьбы с непрерывно изменяющимся ландшафтом киберугроз необходимо постоянно развивать инновационные технологии и подходы в этой области, а особое внимание следует уделять применению таких технологий, как искусственный интеллект и приложений, которые могут анализировать большие объемы данных в реальном времени; а также быть в курсе последних достижений и передового опыта. В этом плане сегодняшнее мероприятие заслуживает отдельной похвалы.

Завершая свое выступление, я бы хотел еще раз поблагодарить Вас за проведение этого мероприятия в столь впечатляющем виде и пожелать успешного проведения Конференции. Полагаю, что дискуссии в рамках мероприятия будут эффективными с точки зрения изучения существующих проблем и поиска их решений, будут способствовать обмену опытом и расширению перспективного сотрудничества.

**Спасибо за внимание!**