КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ

Проект www.aztech.com.ua

Настоящая Концепция обосновывает необходимость и своевременность разработки Стратегии кибербезопасности Украины (далее – Стратегии), определяет ее принципы и направления, а также ее место в системе нормативных актов государства.

I. Актуальность разработки Стратегии

Информационные и коммуникационные технологии (ИКТ) стремительно развиваются, усиливая свое влияние на все ключевые сферы деятельности гражданина, организаций и государства в Украины. Сеть Интернет и другие составные элементы киберпространства утвердились в качестве системообразующего фактора украинского экономического развития и модернизации. Внедрение ИКТ в процессы государственного управления является основой построения эффективного и социально ответственного демократического государства в XXI веке. В связи с этим требуется целенаправленная и системная государственная политика развития национального сектора применения информационных технологий.

В то же время вместе со значительным ростом возможностей проникновение ИКТ во все сферы жизни вызывает возникновение ряда новых и развитие некоторых существующих угроз личности, обществу и государству.

Трансграничный характер киберпространства, его зависимость от сложных информационных технологий, активное использование площадок и сервисов киберпространства всеми группами граждан Украины определяют новые возможности, но при этом и развивают новые угрозы для:

нанесения урона правам, интересам и жизнедеятельности личности, организации, государственных органов;

проведения кибератак против защищаемых информационных ресурсов со стороны киберпреступников и кибертеррористов;

использования кибероружия в рамках специальных операций и кибервойн, в том числе сопровождающих традиционные боевые действия.

В настоящее время в Украины принят ряд документов, направленных на обеспечение различных аспектов национальной информационной безопасности. Среди них Доктрина информационной безопасности Украины, Стратегия развития информационного общества в Украины и другие документы. Однако существующее регулирование не охватывает в необходимой мере систему отношений, возникающих в рамках киберпространства как элемента информационного пространства.

В целях реализации связанных с использованием функционала киберпространства возможностей и установления контроля над возникающими рисками остро встает вопрос о необходимости подготовки специального документа в данной области. Принимая во внимание комплексный характер

проблемы, ее масштаб, перспективу долговременного развития, накопленный международный опыт, обоснованным представляется выбор стратегии как формы документа.

II. Место кибербезопасности в структуре информационной безопасности

Разработка Стратегии как документа, направленного на получение планируемого результата с учетом долговременного развития, требует четкого обозначения круга проблем, которые будут решены в рамках работы по обозначенным в Стратегии направлениям. Поэтому особое значение имеет определение понятия «кибербезопасность».

В Стратегии киберпространство должно рассматриваться как определенный, имеющий четкие границы элемент информационного пространства. Такой подход согласуется с положениями международных стандартов, которые дают определения терминам из сферы информационной безопасности и устанавливают их соотношение. «Кибербезопасность» понимается, таким образом, как более узкое по смыслу понятие, чем «информационная безопасность».

Стратегия должна базироваться на следующей системе понятий:

1) информационное пространство – сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

2) информационная безопасность – состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

3) киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства);

4) кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Анализ показывает, что в официальных украинских документах в области информационной безопасности термин «кибербезопасность» не выделяется из объема понятия «информационная безопасность» и не используется отдельно. В то же время в большинстве зарубежных стран он выделен в самостоятельную дефиницию. Необходимо учитывать, что регулирование киберпространства исключительно на национальном уровне невозможно в силу его трансграничности. В связи с этим существует необходимость обозначения в украинских документах, посвященных информационной безопасности, термина «кибербезопасность», что позволит установить соответствие между украинскими

и иностранными нормативными актами, а также даст возможность участвовать в международной нормотворческой работе в сфере кибербезопасности.

III. Место Стратегии в системе действующего законодательства

Стратегия имеет свой предмет регулирования, не вступает в противоречие с действующими нормативными актами и не создает избыточного регулирования.

Стратегия призвана:

1) устранить имеющиеся пробелы в регулировании обеспечения кибербезопасности Украины;

2) создать основания для включения в процесс обеспечения кибербезопасности Украины в качестве действующих лиц наравне с государственными органами структуры гражданского общества и бизнес-организации;

3) систематизировать действия всех заинтересованных сторон в целях повышения уровня кибербезопасностиУкраины ;

4) сформулировать модель угроз кибербезопасности Украины, а также направления и меры для противостояния им.

В части включения Стратегии в систему действующих нормативных актов Украины следует обратить внимание на следующее:

1. Стратегия основывается на ключевых принципах закона о «Об информации, информационных технологиях и о защите информации», к которым можно отнести обеспечение безопасности Украины при создании информационных систем, их эксплуатации, неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

2. Стратегия согласуется с Доктриной информационной безопасности Украины (далее – Доктрина) и развивает ее отдельные положения. Одной из центральных задач в области информационной безопасности, согласно Доктрине, является разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности. Стратегия предусматривает действия по обеспечению безопасности государственных информационных ресурсов, такие как проведение регулярной оценки защищенности государственных информационных ресурсов и систем.

Задачей Стратегии является организация поддержки отечественных разработчиков программного обеспечения в соответствии с включенными в Доктрину положениями о необходимости развития современных информационных технологий и отечественной индустрии информации.

В соответствии с Доктриной, к организационно-техническим методам обеспечения информационной безопасности относится формирование системы отслеживания показателей и характеристик информационной безопасности Украины в наиболее важных сферах жизни и деятельности общества и государства. Стратегия, конкретизируя положения Доктрины,

предусматривает создание механизма мониторинга киберугроз и реагирования на них, а также открытие общедоступного интернет-портала, посвященного проблемам кибербезопасности, который будет, в том числе, содержать аналитическую и статистическую информацию. Доктрина предусматривает создание единой системы подготовки кадров в области информационной безопасности и информационных технологий. Стратегия, в свою очередь, предлагает набор необходимых мероприятий и действия в целях повышения компетентности специалистов различных сфер в вопросах кибербезопасности.

Отдельно необходимо отметить внимание, которое Стратегия, как и Доктрина, уделяет расширению международного сотрудничества. В этом сотрудничестве главенствующую роль играет, прежде всего, выработка совместных мер по нормативному ограничению распространения и применения информационного оружия.

3. Стратегия согласуется с положениями Стратегии развития информационного общества в Украины (далее – Стратегия развития информационного общества).

Одной из задач Стратегии развития информационного общества является сохранение культуры многонационального народа Украины, укрепление нравственных и патриотических принципов в общественном сознании, развитие системы культурного и гуманитарного просвещения. Стратегия предусматривает содействие формированию культуры информационной безопасности и повышения уровня цифровой грамотности гражданУкраины .

Согласно Стратегии развития информационного общества, общественное развитие базируется на следующих принципах: партнерство государства, бизнеса и гражданского общества, свобода и равенство доступа к информации и знаниям, поддержка отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий, содействие развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий, обеспечение национальной безопасности в информационной сфере. Стратегия построена на принципах включенного участия всех вовлеченных в систему отношений в рамках киберпространства сторон: гражданского общества, бизнеса и государства.

4. Стратегия постулирует ряд подходов, соответствующих «Основным направлениям государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Украины».

5. Стратегия согласуется с «Основными направлениями государственной политики в области формирования культуры информационной безопасности», предусматривая повышение уровня компетенций граждан Украины в части обеспечения кибербезопасности через разработку новых и расширение существующих образовательных программ, а также организацию просветительских информационных кампаний.

6. Стратегия поддерживает и развивает положения «Основ государственной политики Украины в области международной информационной безопасности на период до 2030 года»[5] как на уровне взаимодействия государственных институтов, предусматривая участие Украины в разработке и реализации мер по обеспечению кибербезопасности на международном уровне, так и на уровне взаимодействия организаций, в том числе в части расширения сотрудничества украинских коммерческих и корпоративных ситуационных центров с иностранными и международными ситуационными центрами в целях обмена информацией о киберугрозах, использовании защитных технологий, мерах и средствах обеспечения кибербезопасности.

IV. Цель Стратегии

Целью Стратегии является обеспечение кибербезопасности личности, организации и государства в Украины путем определения системы приоритетов, принципов и мер в области внутренней и внешней политики.

V. Принципы Стратегии

Стратегия кибербезопасности базируется на следующих основных принципах:

1) принцип гарантированности конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;

2) принцип максимальной защищенности личности, организаций, в том числе обеспечивающих функционирование критической информационной инфраструктуры, и государственных органов в части функционирования информационных ресурсов, информационных систем и информационно-телекоммуникационных сетей в киберпространстве;

3) принцип конструктивного сотрудничества всех субъектов информационного общества – личности, организаций и государства – в области обеспечения кибербезопасности;

Сферы ответственности действующих лиц:

государство – правовое регулирование сферы кибербезопасности и координация усилий стейкхолдеров;

бизнес – обеспечение кибербезопасности критической информационной инфраструктуры, находящейся в частной собственности, внедрение и соблюдение стандартов кибербезопасности;

общество – повышение уровня цифровой грамотности и обеспечение обратной связи в ответ на усилия государства и бизнеса.

4) принцип баланса между установлением ответственности за несоблюдение требований кибербезопасности с одной стороны и введением избыточных ограничений - с другой;

5) принцип приоритезации рисков кибербезопасности в соответствии с вероятностями реализации киберугроз и размерами негативных последствий от инцидентов кибербезопасности;

6) принцип систематической актуализации средств и методов обеспечения кибербезопасности в целях противостояния изменяющимся киберугрозам.

VI. Приоритеты Стратегии в обеспечении кибербезопасности

Стратегия предусматривает первоочередную реализацию следующих действий:

1) развитие национальной системы защиты от кибератак и предупреждения киберугроз, поощрение создания и развития частных защитных систем в данной области;

2) развитие и обновление в соответствии с требованиями времени механизмов повышения надежности критической информационной инфраструктуры;

3) совершенствование мер обеспечения безопасности государственных информационных ресурсов в киберпространстве;

4) разработку механизмов партнерства государства, бизнеса и гражданского общества в сфере кибербезопасности;

5) развитие цифровой грамотности граждан и культуры безопасного поведения в киберпространстве;

6) наращивание международного сотрудничества в целях выработки и развития договоренностей и механизмов для повышения глобального уровня кибербезопасности.

VII. Направления деятельности по обеспечению кибербезопасности, которые должны быть отражены и уточнены в Стратегии

Обеспечение кибербезопасности Украины должно осуществляться по следующим направлениям.

1. Принятие общесистемных мер по обеспечению кибербезопасности, в частности:

организация проведения регулярной оценки и анализа защищенности государственных и муниципальных информационных систем и информационно-телекоммуникационных сетей, критической информационной инфраструктуры от киберугроз;

принятие стандартов кибербезопасности и определение механизма проверки их соблюдения;

гармонизация национальных стандартов Украины и международных стандартов информационной безопасности, обеспечение перевода на украинский язык действующих и подготавливаемых иностранных стандартов в целях информирования специалистов в области информационной безопасности и использования в нормотворческой работе;

развитие государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Украины, в том числе создание и развитие сети государственных и корпоративных ситуационных центров и центров реагирования на инциденты кибербезопасности;

разработка, утверждение и подготовка к использованию антикризисного плана пресечения попыток реализации или непосредственной реализации киберугроз национального масштаба, в том числе во взаимодействии с иностранными государствами, организациями и гражданами.

2. Совершенствование нормативно-правовой базы и правовых мер обеспечения кибербезопасности, в частности:

проведение аудита и создание механизма обновления требований и рекомендаций по кибербезопасности в отношении государственных и муниципальных информационных систем, информационно-телекоммуникационных сетей, критической информационной инфраструктуры организаций с частным и государственным участием;

системное совершенствование законодательства Украины в сфере кибербезопасности, в том числе на основе адаптации правовых норм из законодательств зарубежных государств, и приведение законодательства Украины в сфере кибербезопасности в соответствие с ратифицированными международными соглашениями;

расширение практики привлечения экспертного сообщества, научных и некоммерческих организаций к подготовке ключевых проектов нормативных документов в сфере кибербезопасности;

ужесточение административной и уголовной ответственности за преступления, совершенные в киберпространстве, введение норм уголовной и административной ответственности за традиционные правонарушения, совершенные с применением информационно-коммуникационных технологий;

упрощение взаимодействия правоохранительных органов с иностранными уполномоченными органами при расследовании инцидентов кибербезопасности;

подготовка нормативно-правовой базы для совершенствования и применения технологий облачных вычислений, а также разработки и функционирования «облачных» сервисов.

3. Проведение научных исследований в области кибербезопасности, в частности:

реализация научно-технических программ и исследований в соответствии с «Основными направлениями научных исследований в области обеспечения информационной безопасности Украины»

определение передовых научно-технических центров в области кибербезопасности и оказание им адресной государственной поддержки в проведении прикладных и фундаментальных исследований и конструкторских работ.

4. Создание условий для разработки, производства и применения средств обеспечения кибербезопасности, в частности:

государственная поддержка отечественных производителей средств обеспечения кибербезопасности, в том числе введение налоговых льгот, поддержка продвижения продукции на глобальном рынке;

содействие разработке отечественных программных и технических средств обеспечения кибербезопасности, в том числе реализуемых как свободно распространяемое программное обеспечение;

разработка системных мер по внедрению и применению отечественных программных и аппаратных средств, в том числе средств обеспечения кибербезопасности, вместо аналогов иностранного производства в государственных и муниципальных информационных системах, информационно-телекоммуникационных сетях, информационных системах критически важных объектов инфраструктуры и обеспечивающих их взаимодействие информационно-телекоммуникационных сетях.

5. Совершенствование кадрового обеспечения и организационных мер обеспечения кибербезопасности, в частности:

доработка, согласование и введение в действие образовательных стандартов подготовки и переподготовки специалистов в области кибербезопасности;

разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности, включающего модули по обеспечению кибербезопасности, либо дополнение имеющихся курсов упомянутыми модулями;

доработка квалификационных требований к государственным служащим, занятым в области информационных технологий и информационной безопасности, с учетом современных тенденций в целом и кибербезопасности в частности, а также закрепление для них проведения обязательной периодической аттестации на предмет проверки соответствия требованиям;

разработка и введение актуальных периодически обновляемых учебных курсов повышения квалификации в области кибербезопасности для преподавательских кадров и государственных служащих, вовлеченных в процессы обеспечения кибербезопасности государства, организаций и граждан;

подготовка мер стимулирования частно-государственного партнерства в области дополнительного профессионального образования по направлению кибербезопасности;

обеспечение содействия в создании новых и развитии функционирующих отечественных центров компетенций по вопросам кибербезопасности;

разработка рекомендаций по обеспечению безопасного использования аппаратных и программных продуктов и сервисов иностранного производства для граждан Украины, чья деятельность связана со сведениями, составляющими государственную тайну, защищаемой информацией или обеспечением кибербезопасности организаций и государственных органов.

6. Организация внутреннего и международного взаимодействия действующих лиц по обеспечению кибербезопасности, в частности:

расширение сотрудничества государства и государственных ситуационных центров с коммерческими и некоммерческим организациями, корпоративными и международными ситуационными центрами в целях обмена информацией о киберугрозах, об использовании технологий, применении мер и средств

обеспечения кибербезопасности, а также популяризация и внедрение практики безопасного поведения в киберпространстве;

установление порядка подготовки государством и организациями отчетности по вопросам кибербезопасности, в том числе в целях проведения последующего анализа и корректировки деятельности по обеспечению кибербезопасности;

усовершенствование механизмов инициирования государственными органами, организациями и гражданами расследований киберпреступлений, а также механизмов оказания помощи в ликвидации их последствий;

разработка совместно со страховыми и аудиторскими организациями мер по страхованию рисков от киберугроз, юридической поддержке обеспечения кибербезопасности, аудиту государственных органов и организаций по направлению «кибербезопасность»;

обеспечение участия Украины в разработке и реализации мер по обеспечению кибербезопасности на международном уровне;

создание механизмов государственного консультирования и оказания методической помощи в части обеспечения кибербезопасности критически важных объектов инфраструктуры;

разработка механизмов поощрения граждан, оказывающих помощь в борьбе с киберугрозами, в том числе в части поиска специалистами по информационной безопасности разного профиля уязвимостей защищаемых информационных ресурсов и формирования предложений по их устранению.

7. Формирование и развитие культуры безопасного поведения в киберпространстве и безопасного использования его сервисами, в частности:

организация комплексной информационной кампании в целях повышения уровня информированности граждан, организаций и государственных органов об актуальных киберугрозах, уязвимостях защищаемых ресурсов в киберпространстве и способах их компенсации, популяризация доступных технологий, мер и средств обеспечения кибербезопасности;

создание и проведение кампании по популяризации общедоступного государственного веб-портала о киберугрозах, проблемах кибербезопасности и путях их решения;

обеспечение информационной поддержки проводимым в Украины семинарам, выставкам, форумам по вопросам информационной безопасности в целом и кибербезопасности в частности.

VIII. Разработка и принятие Стратегии

После утверждения настоящей Концепции Правительство Украины создает рабочую группу по разработке Стратегии с участием представителей СБУ Украины, органа исполнительной власти, уполномоченного в области обеспечения безопасности, иных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, органов государственного надзора и контроля, коммерческих компаний, компаний с государственным участием и государственных организаций, в том числе научных

и академических учреждений, некоммерческих организаций, ведущих деятельность в связанных с кибербезопасностью сферах.

Рабочая группа обеспечивает разработку Стратегии в соответствии с положениями настоящей Концепции, которая впоследствии утверждается нормативным актом Правительства Украины. Неотъемлемой частью Стратегии является план мероприятий по ее реализации.

Необходимые бюджетные средства на реализацию мероприятий Стратегии предусматриваются в бюджетных ассигнованиях государственных органов, ответственных за их реализацию.