Закон Украины Об основных принципах обеспечения кибербезопасности Украины

Настоящий Закон определяет правовые и организационные основы обеспечения защиты жизненно важных интересов человека и гражданина, общества и государства, национальных интересов Украины в киберпространстве, основные цели, направления и принципы государственной политики в сфере кибербезопасности, полномочия государственных органов, предприятий, учреждений, организаций, лиц и граждан в этой сфере, основные принципы координации их деятельности по обеспечению кибербезопасности.

Статья 1. Определение терминов
В этом Законе нижеприведенные термины употребляются в таком значении:

1) индикаторы киберугроз - показатели (технические данные), используемые для выявления и реагирования на киберугрозы;

2) информация об инциденте кибербезопасности - сведения об обстоятельствах киберинциденту, в частности о том, какие объекты киберзащиты и при каких условиях подверглись кибератаке, из них успешно обнаружены, нейтрализованы предотвращенных с помощью каких средств киберзащиты, в том числе с использованием которых индикаторов киберугроз;

3) инцидент кибербезопасности (далее - киберинцидент) - событие или ряд неблагоприятных событий случайного характера (природного, технического, технологического, ложного, в том числе в результате действия человеческого фактора) и / или имеющих признаки возможной (потенциальной) кибератаки, которые составляют угрозу безопасности систем электронных коммуникаций, систем управления технологическими процессами, создают вероятность нарушения штатного режима функционирования таких систем (в том числе срыва и / или блокировки работы системы, и / или несанкционированного управления ее ресурсами), ставят под угрозу безопасность (защищенность) электронных информационных ресурсов ;

4) кибератака - направлены (умышленные) действия в киберпространстве, которые осуществляются с помощью средств электронных коммуникаций (включая информационно-коммуникационные технологии, программные, программно-аппаратные средства, другие технические и технологические средства и оборудования) и направлены на достижение одной или совокупности таких целей : нарушение конфиденциальности, целостности, доступности

электронных информационных ресурсов, обрабатываемых (передаются, хранятся) в коммуникационных и / или технологических системах, получение несанкционированного доступа к таким ресурсам; нарушения безопасности, устойчивого, надежного и штатного режима функционирования коммуникационных и / или технологических систем; использование коммуникационной системы, ее ресурсов и средств электронных коммуникаций для осуществления кибератак на другие объекты киберзащиты;

5) кибербезопасность - защищенность жизненно важных интересов человека и гражданина, общества и государства при использовании киберпространства, при которой обеспечиваются устойчивое развитие информационного общества и цифровой коммуникационной среды, своевременное выявление, предотвращение и нейтрализация реальных и потенциальных угроз национальной безопасности Украины в киберпространстве;

6) киберугроз - имеющиеся и потенциально возможные явления и факторы, создающие опасность жизненно важным национальным интересам Украины в киберпространстве, оказывают негативное влияние на состояние кибербезопасности государства, кибербезопасность и киберзащита ее объектов;

7) киберзащита - совокупность организационных, правовых, инженерно-технических мероприятий, а также мероприятий криптографической и технической защиты информации, направленных на предотвращение киберинцидентам, выявление и защиту от кибератак, ликвидации их последствий, восстановление устойчивости и надежности функционирования коммуникационных, технологических систем;

8) киберпреступлений (компьютерное преступление) - общественно опасное виновное деяние в киберпространстве и / или с его использованием, ответственность за которое предусмотрена законом Украины об уголовной ответственности и / или которое признано преступлением международными договорами Украины;

9) киберпреступность - совокупность киберпреступлений;

10) кибероборона - совокупность политических, экономических, социальных, военных, научных, научно-технических, информационных, правовых, организационных и других мероприятий, которые осуществляются в киберпространстве и направлены на обеспечение защиты суверенитета и обороноспособности государства, предотвращение возникновения вооруженного конфликта и отпор вооруженной агрессии ;

11) киберпространство - среда (виртуальное пространство), которое предоставляет возможности для осуществления коммуникаций и / или реализации общественных отношений, образованное в результате функционирования совместных (объединенных) коммуникационных систем и обеспечение электронных коммуникаций с использованием сети Интернет и / или других глобальных сетей передачи данных;

12) кибербразведку - деятельность, осуществляемая разведывательными органами в киберпространстве или с его использованием;

13) кибертерроризм - террористическая деятельность, осуществляемая в киберпространстве или с его использованием;

14) кибершпионажем - шпионаж, осуществляемой в киберпространстве или с его использованием;

15) критическая информационная инфраструктура - совокупность объектов критической информационной инфраструктуры;

16) критически важные объекты инфраструктуры (далее - объекты критической инфраструктуры) - предприятия, учреждения и организации независимо от формы собственности, деятельность которых непосредственно связана с технологическими процессами и / или предоставлением услуг, имеющих большое значение для экономики и промышленности, функционирования общества и безопасности населения, вывод из строя или нарушение функционирования которых может оказать негативное влияние на состояние национальной безопасности и обороны Украины, окружающей природной среды, причинить имущественный вред и / или представлять угрозу для жизни и здоровья людей;

17) Национальная телекоммуникационная сеть - совокупность специальных телекоммуникационных систем (сетей), систем специальной связи, других коммуникационных систем, используемых в интересах органов государственной власти и органов местного самоуправления, правоохранительных органов и воинских формирований, образованных в соответствии с законом, предназначена для обращения (передача, прием, создание, обработка, хранение) и защиты национальных информационных ресурсов, обеспечение защищенных электронных коммуникаций, предоставление спектра современных защищенных информационно-коммуникационных (мультисервисных) услуг в интересах осуществления управления государством в мирное время, в условиях чрезвычайного положения и в особый период и которая является сетью (системой) двойного назначения с использованием части ее ресурса для предоставления услуг, в частности с киберзащиты, другим потребителям;

18) национальные электронные информационные ресурсы (далее - национальные информационные ресурсы) - систематизированы электронные информационные ресурсы, содержащие информацию независимо от вида, содержания, формы, времени и места ее создания (включая публичную информацию, государственные информационные ресурсы и другую информацию), предназначенную для удовлетворение жизненно важных общественных потребностей гражданина, личности, общества и государства. Под электронными информационными ресурсами понимается любая информация, созданная, записанная, обработанная или сохранена в цифровой или иной нематериальной форме с помощью электронных, магнитных, электромагнитных, оптических, технических, программных или других средств;

18-1) Национальный центр резервирования государственных информационных ресурсов – организованная совокупность объектов, созданных с целью обеспечения надежности и бесперебойности работы государственных информационных ресурсов, киберзащиты, хранения национальных электронных информационных ресурсов, резервного копирования информации и сведений национальных электронных информационных ресурсов государственных органов, военных формирований, образованных в соответствии с законами, предприятиями, учреждениями и организациями;

19) объект критической информационной инфраструктуры - коммуникационная или технологическая система объекта критической инфраструктуры, кибератака на которую непосредственно повлияет на устойчивое функционирование такого объекта критической инфраструктуры;

20) система управления технологическими процессами (далее - технологическая система) - автоматизированная или автоматическая система, которая представляет собой совокупность оборудования, средств, комплексов и систем обработки, передачи и приема, предназначена для организационного управления и / или управления технологическими процессами (включая промышленное, электронное, коммуникационное оборудование, другие технические и технологические средства) независимо от наличия доступа системы к сети Интернет и / или других глобальных сетей передачи данных;

21) системы электронных коммуникаций (далее - коммуникационные системы) - системы передачи, коммутации или маршрутизации, оборудование и другие ресурсы (включая пассивные сетевые элементы, которые позволяют передавать сигналы с помощью проводных, радио-, оптических или других электромагнитных средств, сети мобильной, спутниковой связи, электрические кабельные сети в части, в которой они используются для целей передачи сигналов), обеспечивают электронные коммуникации (передачу электронных

информационных ресурсов), в том числе средства и устройства связи, компьютеры, другая компьютерная техника, информационно-телекоммуникационные системы, имеющих доступ к сети Интернет и / или других глобальных сетей передачи данных.

Термины "национальная безопасность", "национальные интересы", "угрозы национальной безопасности" употребляются в настоящем Законе в значении, определенном Законом Украины "Об основах национальной безопасности Украины".

Термин "платежный рынок" употребляется в настоящем Законе в значении, приведенном в Законе Украины "О платежных услугах".

Статья 2. Принципы применения Закона

1. Настоящий Закон не распространяется на:

1) отношения и услуги, связанные с содержанием информации, обрабатываемой (передается, хранится) в коммуникационных и / или в технологических системах;

2) деятельность, связанную с защитой информации, составляющей государственную тайну, коммуникационные и технологические системы, предназначенные для ее обработки;

3) социальные сети, частные электронные информационные ресурсы в сети Интернет (включая блог-платформы, видеохостинги, другие веб-ресурсы), если такие информационные ресурсы не содержат информацию, необходимость защиты которой установлено законом, отношения и услуги, связанные с функционированием таких сетей и ресурсов;

4) коммуникационные системы, которые не взаимодействуют с публичными сетями электронных коммуникаций (электронными сетями общего пользования), не подключены к сети Интернет и / или других глобальных сетей передачи данных (кроме технологических систем).

2. Применение законодательства в сфере кибербезопасности и принятия субъектами властных полномочий решений во исполнение норм этого Закона осуществляются с соблюдением принципов:

1) минимально необходимого регулирования, согласно которому решения (мероприятия) субъектов властных полномочий должны быть необходимыми и минимально достаточными для достижения целей и задач, определенных настоящим Законом;

2) объективности и правовой определенности, максимально возможного применения национального и международного права относительно полномочий и обязанностей государственных органов, предприятий, учреждений, организаций, граждан в сфере кибербезопасности;

3) обеспечение защиты прав пользователей коммуникационных систем и / или потребителей услуг электронных коммуникаций, и / или услуг по защите информации, киберзащиты, в том числе прав на невмешательство в частную жизнь и защиты персональных данных;

4) прозрачности, согласно которому решения (мероприятия) субъектов властных полномочий должны быть должным образом обоснованы и сообщены субъектам, которых они касаются, до вступления в силу (их применение)

5) сбалансированности требований и ответственности, согласно которому должно быть обеспечен баланс между установлением ответственности за невыполнение требований кибербезопасности и киберзащиты, а также за введение чрезмерных требований и ограничений;

6) недискриминации, согласно которому решения, действия и бездеятельность субъектов властных полномочий не могут приводить к юридическому или фактическому объему прав и обязанностей лица, являются:

отличным от объема прав и обязанностей других лиц в подобных ситуациях, если только такое различие не является необходимой и минимально достаточной для удовлетворения общественного интереса;

таким, как и объем прав и обязанностей других лиц в неподобных ситуациях, если такое единообразие не является необходимой и минимально достаточной для удовлетворения общественного интереса;

7) эквивалентности требований к обеспечению кибербезопасности объектов критической инфраструктуры, согласно которым применение правовых норм должно быть как можно более равнозначным по киберзащиты коммуникационных и технологических систем объектов критической инфраструктуры, принадлежащих к одному сектору экономики и / или осуществляющих аналогичные функции.

Указанные принципы применяются без преобладания какого-либо из них с учетом целей и задач этого Закона.

Статья 3. Правовые основы обеспечения кибербезопасности Украины

1. Правовую основу обеспечения кибербезопасности Украины составляют Конституция Украины, законы Украины относительно основ национальной безопасности, основ внутренней и внешней политики, электронных коммуникаций, защиты государственных информационных ресурсов и информации, требование относительно защиты которой установлено законом, этот и другие законы Украины, Конвенция о киберпреступности , другие международные договоры, согласие на обязательность которых предоставлено Верховной Радой Украины, указы Президента Украины, акты Кабинета Министров Украины, а также другие нормативно-правовые акты, принимаемые во исполнение законов Украины.

2. Если международным договором Украины, согласие на обязательность которого предоставлено Верховной Радой Украины, предусмотрены иные правила, чем установленные настоящим Законом, применяются положения международного договора Украины.

Статья 4. Объекты кибербезопасности и киберзащиты

1. Объектами кибербезопасности являются:

1) конституционные права и свободы человека и гражданина;

2) общество, устойчивое развитие информационного общества и цифровой коммуникационной среды;

3) государство, его конституционный строй, суверенитет, территориальная целостность и неприкосновенность;

4) национальные интересы во всех сферах жизнедеятельности личности, общества и государства;

5) объекты критической инфраструктуры.

2. Объектами киберзащиты является:

1) коммуникационные системы всех форм собственности, в которых обрабатываются национальные информационные ресурсы и / или используемых в интересах органов государственной власти, органов местного самоуправления, правоохранительных органов и воинских формирований, образованных в соответствии с законом;

2) объекты критической информационной инфраструктуры;

3) коммуникационные системы, которые используются для удовлетворения общественных потребностей и / или реализации правоотношений в сферах

электронного управления, электронных государственных услуг, электронной коммерции, электронного документооборота.

3. Порядок формирования перечня объектов критической информационной инфраструктуры, перечень таких объектов и порядок их внесения в государственный реестр объектов критической информационной инфраструктуры, а также порядок формирования и обеспечения функционирования государственного реестра объектов критической информационной инфраструктуры утверждаются Кабинетом Министров Украины.

Полномочия по формированию и обеспечению функционирования реестра объектов критической информационной инфраструктуры в банковской системе Украины возлагаются на Национальный банк Украины.

Статья 5. Субъекты обеспечения кибербезопасности

1. Координация деятельности в сфере кибербезопасности как составляющей национальной безопасности Украины осуществляется Президентом Украины через возглавляемую им Совет национальной безопасности и обороны Украины.

2. Национальный координационный центр кибербезопасности как рабочий орган Совета национальной безопасности и обороны Украины осуществляет координацию и контроль за деятельностью субъектов сектора безопасности и обороны, которые обеспечивают кибербезопасность, вносит Президенту Украины предложения по формированию и уточнению Стратегии кибербезопасности Украины.

3. Кабинет Министров Украины обеспечивает формирование и реализацию государственной политики в сфере кибербезопасности, защиту прав и свобод человека и гражданина, национальных интересов Украины в киберпространстве, борьбу с киберпреступностью; организует и обеспечивает необходимыми силами, средствами и ресурсами функционирования национальной системы кибербезопасности; формирует требования и обеспечивает функционирование системы аудита информационной безопасности на объектах критической инфраструктуры (кроме объектов критической инфраструктуры в банковской системе Украины).

4. Субъектами, непосредственно осуществляющих в пределах своей компетенции меры по обеспечению кибербезопасности, являются:

1) министерства и другие центральные органы исполнительной власти;

2) местные государственные администрации;

3) органы местного самоуправления;

4) правоохранительные, разведывательные и контрразведывательные органы, субъекты оперативно-розыскной деятельности;

5) Вооруженные Силы Украины, другие военные формирования, образованные в соответствии с законом;

6) Национальный банк Украины;

7) предприятия, учреждения и организации, отнесенные к объектам критической инфраструктуры;

8) субъекты хозяйствования, граждане Украины и объединения граждан, другие лица, осуществляющие деятельность и / или предоставляют услуги, связанные с национальными информационными ресурсами, информационными электронными услугами, осуществлением электронных сделок, электронными коммуникациями, защитой информации и киберзащиты .

5. Субъекты обеспечения кибербезопасности в пределах своей компетенции:

1) осуществляют меры по предотвращению использования киберпространства в военных, разведывательно-подрывных, террористических и других противоправных и преступных целях;

2) осуществляют выявление и реагирование на киберинциденты и кибератаки, устранения их последствий;

3) осуществляют информационный обмен о реализованных и потенциальных киберугроз;

4) разрабатывают и реализуют меры, организационные, образовательные и другие мероприятия в сфере кибербезопасности, кибероборони и киберзащиты;

5) обеспечивают проведение аудита информационной безопасности, в том числе на подчиненных объектах и объектах, которые принадлежат к сфере их управления;

6) осуществляют другие меры по обеспечению развития и безопасности киберпространства.

Статья 6. Объекты критической инфраструктуры

1. К объектам критической инфраструктуры могут быть отнесены предприятия, учреждения и организации независимо от формы собственности, которые:

1) осуществляют деятельность и предоставляющих услуги в области энергетики, химической промышленности, транспорта, информационно-коммуникационных технологий, электронных коммуникаций, в банковском и финансовом секторах, а также на платежном рынке;

2) предоставляют услуги в сферах жизнеобеспечения населения, в частности в сферах централизованного водоснабжения, водоотведения, снабжения электрической энергии и газа, производства продуктов питания, сельского хозяйства, здравоохранения,

3) являются коммунальными, аварийными и спасательными службами, службами экстренной помощи населению;

4) включены в перечень предприятий, имеющих стратегическое значение для экономики и безопасности государства;

5) являются объектами потенциально опасных технологий и производств.

2. Критерии и порядок отнесения объектов к объектам критической инфраструктуры, перечень таких объектов, общие требования к их киберзащиты, в том числе по применению индикаторов киберугроз, и требования к проведению независимого аудита информационной безопасности утверждаются Кабинетом Министров Украины, а относительно банков, других лиц, осуществляющих деятельность на рынках финансовых услуг, государственное регулирование и надзор за деятельностью которых осуществляет Национальный банк Украины, операторов платежных систем и / или участников платежных систем, технологических операторов платежных услуг - Национальным банком Украины.

3. Требования и порядок проведения независимого аудита информационной безопасности на объектах критической инфраструктуры устанавливаются соответствующими нормативно-правовыми актами по аудиту информационной безопасности, утверждаются Кабинетом Министров Украины.

Разработка нормативно-правовых актов по независимому аудиту информационной безопасности на объектах критической инфраструктуры осуществляется на основе международных стандартов, стандартов Европейского Союза и НАТО с обязательным привлечением представителей основных субъектов национальной системы кибербезопасности, научных учреждений, независимых аудиторов и экспертов в области кибербезопасности, общественных организаций.

4. Ответственность за обеспечение киберзащиты коммуникационных и технологических систем объектов критической инфраструктуры, защиты

технологической информации в соответствии с требованиями законодательства, за безотлагательное информирование правительственной команды реагирования на компьютерные чрезвычайные события Украины CERT-UA об инцидентах кибербезопасности, за организацию проведения независимого аудита информационной безопасности на таких объектах возлагается на владельцев и / или руководителей предприятий, учреждений и организаций, отнесенных к объектам критической инфраструктуры.

5. Обмен информацией об инцидентах кибербезопасности, содержащий персональные данные, осуществляется с соблюдением требований Закона Украины "О защите персональных данных".

Статья 7. Принципы обеспечения кибербезопасности

1. Обеспечение кибербезопасности в Украине основывается на принципах:

1) верховенства права, законности, уважения прав человека и основных свобод и их защиты в порядке, определенном законом;

2) обеспечение национальных интересов Украины;

3) открытости, доступности, стабильности и защищенности киберпространства, развития сети Интернет и ответственных действий в киберпространстве;

4) государственно-частной взаимодействия, широкого сотрудничества с гражданским обществом в сфере кибербезопасности и киберзащиты, в частности путем обмена информацией об инцидентах кибербезопасности, реализации совместных научных и исследовательских проектов, обучения и повышения квалификации кадров в этой сфере;

5) пропорциональности и адекватности мер киберзащиты реальным и потенциальным рискам, реализации неотъемлемого права государства на самозащиту в соответствии с нормами международного права в случае совершения агрессивных действий в киберпространстве;

6) приоритетности мер;

7) неотвратимости наказания за совершение киберпреступлений;

8) приоритетного развития и поддержки отечественного научного, научно-технического и производственного потенциала;

9) международного сотрудничества с целью укрепления взаимного доверия в сфере кибербезопасности и выработки совместных подходов в противодействии киберугрозами, консолидации усилий в расследовании и предотвращении

киберпреступлений, недопущения использования киберпространства в террористических, военных, других противоправных целях;

10) обеспечение демократического гражданского контроля за образованными в соответствии с законами Украины военными формированиями и правоохранительными органами, которые осуществляют деятельность в сфере кибербезопасности.

Статья 8. Национальная система кибербезопасности

1. Национальная система кибербезопасности является совокупностью субъектов обеспечения кибербезопасности и взаимосвязанных мероприятий политического, научно-технического, информационного, образовательного характера, организационных, правовых, оперативно-розыскных, разведывательных, контрразведывательных, оборонных, инженерно-технических мероприятий, а также мероприятий криптографической и технической защиты информационных ресурсов, киберзащиты объектов критической информационной инфраструктуры.

2. Основными субъектами национальной системы кибербезопасности является Государственная служба специальной связи и защиты информации Украины, Национальная полиция Украина, Служба безопасности Украины, Министерство обороны Украины и Генеральный штаб Вооруженных Сил Украины, разведывательные органы, Национальный банк Украины, в соответствии с Конституцией и законов Украины выполняют в установленном порядке следующие основные задачи:

1) Государственная служба специальной связи и защиты информации Украины обеспечивает формирование и реализацию государственной политики по защите в киберпространстве государственных информационных ресурсов и информации, требование относительно защиты которой установлено законом, киберзащиты объектов критической информационной инфраструктуры, осуществляет государственный контроль в этих сферах; координирует деятельность других субъектов обеспечения кибербезопасности по киберзащиты; обеспечивает создание и функционирование Национальной телекоммуникационной сети, внедрение организационно-технической модели киберзащиты; осуществляет организационно-технические мероприятия по предупреждению, выявлению и реагированию на киберинциденты и кибератаки и устранения их последствий; информирует о киберугрозы и соответствующие методы защиты от них; обеспечивает внедрение аудита информационной безопасности на объектах критической инфраструктуры, устанавливает требования к аудиторам информационной безопасности, определяет порядок их аттестации (переаттестации) координирует, организует и проводит аудит

защищенности коммуникационных и технологических систем объектов критической инфраструктуры уязвимость; обеспечивает функционирование Государственного центра киберзащиты, правительственной команды реагирования на компьютерные чрезвычайные события Украины CERT-UA;

2) Национальная полиция Украина обеспечивает защиту прав и свобод человека и гражданина, интересов общества и государства от уголовно противоправных посягательств в киберпространстве; осуществляет мероприятия по предупреждению, выявлению, пресечению и раскрытию киберпреступлений, повышение осведомленности граждан о безопасности в киберпространстве;

3) Служба безопасности Украины осуществляет предотвращения, выявления, пресечения и раскрытия уголовных преступлений против мира и безопасности человечества, совершаемых в киберпространстве; осуществляет контрразведывательные и оперативно-розыскные мероприятия, направленные на борьбу с кибертерроризмом и кибершпионажем, негласно проверяет готовность объектов критической инфраструктуры к возможным кибератак и киберинцидентив; противодействует киберпреступности, последствия которой могут создать угрозу жизненно важным интересам государства; расследует киберинциденты и кибератаки по государственным электронным информационным ресурсам, информации, требование относительно защиты которой установлено законом, критической информационной инфраструктуры; обеспечивает реагирование на киберинциденты в сфере государственной безопасности;

4) Министерство обороны Украины, Генеральный штаб Вооруженных Сил Украины в соответствии с компетенцией осуществляют мероприятия по подготовке государства к отражению военной агрессии в киберпространстве (кибероборонь) осуществляют военное сотрудничество с НАТО и другими субъектами оборонной сферы по обеспечению безопасности киберпространства и совместной защиты от киберугроз; внедряют мероприятия по обеспечению киберзащиты критической информационной инфраструктуры в условиях чрезвычайного и военного положения;

5) разведывательные органы Украины осуществляют разведывательную деятельность относительно угроз национальной безопасности Украины в киберпространстве, других событий и обстоятельств, касающихся сферы кибербезопасности;

6) Национальный банк Украины определяет порядок, требования и меры по обеспечению киберзащиты и информационной безопасности банками, другими лицами, осуществляющими деятельность на рынках финансовых услуг, государственное регулирование и надзор за деятельностью которых

осуществляет Национальный банк Украины, операторами платежных систем и / или участниками платежных систем, технологическими операторами платежных услуг, осуществляет контроль за их выполнением; создает центр киберзащиты Национального банка Украины, обеспечивает функционирование системы киберзащиты для банков, других лиц, осуществляющих деятельность на рынках финансовых услуг, государственное регулирование и надзор за деятельностью которых осуществляет Национальный банк Украины, операторов платежных систем и / или участников платежных систем, технологических операторов платежных услуг; обеспечивает проведение оценки состояния киберзащиты и аудита информационной безопасности на объектах критической инфраструктуры в банках, других лицах, осуществляющих деятельность на рынках финансовых услуг, государственное регулирование и надзор за деятельностью которых осуществляет Национальный банк Украины, операторах платежных систем и / или участникам платежных систем технологических операторах платежных услуг.

3. Функционирование национальной системы кибербезопасности обеспечивается путем:

1) выработка и оперативной адаптации государственной политики в сфере кибербезопасности, направленной на развитие киберпространства, достижения совместимости с соответствующими стандартами Европейского Союза и НАТО,

2) создание нормативно-правовой и терминологической базы в сфере кибербезопасности, гармонизации нормативных документов в области электронных коммуникаций, защиты информации, информационной безопасности и кибербезопасности в соответствии с международными стандартами, в частности стандартов Европейского Союза и НАТО,

3) установление обязательных требований информационной безопасности объектов критической информационной инфраструктуры, в том числе при их создании, ввод в эксплуатацию, эксплуатации и модернизации с учетом международных стандартов и специфики отрасли, в которую входят соответствующие объекты критической информационной инфраструктуры;

4) формирование конкурентной среды в сфере электронных коммуникаций, предоставление услуг по защите информации и киберзащиты;

5) привлечение экспертного потенциала научных учреждений, профессиональных и общественных объединений к подготовке проектов концептуальных документов в сфере кибербезопасности;

6) проведение учений по действиям в случае чрезвычайных ситуаций и инцидентов в киберпространстве;

7) функционирования системы аудита информационной безопасности, внедрение лучших мировых практик и международных стандартов по вопросам кибербезопасности и киберзащиты;

8) развития сети команд реагирования на компьютерные чрезвычайные события;

9) развития и совершенствования системы технической и криптографической защиты информации;

10) обеспечение соблюдения требований законодательства по защите государственных информационных ресурсов и информации;

11) создание и обеспечение функционирования Национальной телекоммуникационной сети;

12) обмена информацией об инцидентах кибербезопасности между субъектами обеспечения кибербезопасности в порядке, определенном законодательством;

13) внедрение единой (универсальной) системы индикаторов киберугроз с учетом международных стандартов по вопросам кибербезопасности и киберзащиты;

14) подготовки специалистов образовательно-квалификационных уровней бакалавра и магистра по государственному заказу в объеме, необходимом для удовлетворения потребностей государственного сектора экономики, а также за небюджетные средства, в том числе для повышения квалификации и проведения обязательной периодической аттестации (переаттестации) персонала, ответственного за обеспечение кибербезопасности объектов критической инфраструктуры, с учетом международных стандартов;

15) внедрение организационно-технической модели национальной системы кибербезопасности как комплекса мер, сил и средств киберзащиты, направленных на оперативное (кризисное) реагирования на кибератаки и киберинциденты, внедрения контрмер, направленных на минимизацию уязвимости коммуникационных систем;

16) установление требований (правил, установок) по безопасному использованию сети Интернет и предоставления электронных услуг государственными органами;

17) государственно-частной взаимодействия в предотвращении киберугрозами объектам критической инфраструктуры, реагировании на кибератаки и

киберинциденты, устранении их последствий, в частности в условиях кризисных ситуаций, чрезвычайного и военного положения, в период;

18) периодического проведения обзора национальной системы кибербезопасности, разработка индикаторов состояния кибербезопасности;

19) стратегического планирования и программно-целевого обеспечения в сфере развития электронных коммуникаций, информационных технологий, защиты информации и киберзащиты;

20) развития международного сотрудничества в области кибербезопасности, поддержки международных инициатив в сфере кибербезопасности, которые отвечают национальным интересам Украины, углубление сотрудничества Украины с Европейским Союзом и НАТО с целью усиления способности Украины в сфере кибербезопасности, участия в мероприятиях по укреплению доверия при использовании киберпространства, что проводятся под эгидой Организации по безопасности и сотрудничеству в Европе;

21) осуществление оперативно-розыскных, разведывательных, контрразведывательных и других мероприятий, направленных на предотвращение, выявление, пресечение и раскрытие уголовных преступлений против мира и безопасности человечества, совершаемых с использованием киберпространства, расследование, преследование, оперативного реагирования и противодействия киберпреступности, разведывательно-подрывной , террористической и иной деятельности в киберпространстве, что наносит ущерб интересам Украины, использованию сети Интернет в военных целях;

22) осуществление военно-политических, военно-технических и других мероприятий для расширения возможностей военной организации государства, сектора безопасности и обороны с использованием киберпространства, создания и развития сил, средств и инструментов возможного ответа на агрессию в киберпространстве, которая может применяться как средство сдерживания военных конфликтов и угроз с использованием киберпространства;

23) ограничения участия в мероприятиях по обеспечению информационной безопасности и кибербезопасности любых субъектов хозяйствования, находящихся под контролем государства, признанной Верховным Советом Украины государством-агрессором, или государств и лиц, в отношении которых действуют специальные экономические и другие ограничительные меры (санкции), принятые на национальном или международном уровне вследствие агрессии в отношении Украины, а также ограничения использования продукции, технологий и услуг таких субъектов для обеспечения технической и криптографической защиты государственных информационных ресурсов,

усиление государственного контроля в этой сфере;

24) развития системы контрразведывательного обеспечения кибербезопасности, предназначенной для предотвращения, своевременного выявления и противодействия внешним и внутренним угрозам безопасности Украины с использованием киберпространства; устранение условий, им способствующих, и причин их возникновения;

25) проведение разведывательных мероприятий по выявлению и противодействию угрозам национальной безопасности Украины в киберпространстве, выявления других событий и обстоятельств, касающихся сферы кибербезопасности.

4. Порядок функционирования Национальной телекоммуникационной сети, критерии, правила и требования о предоставлении услуг, их тарификации для пользователей бюджетной сферы, возмещение расходов государственного бюджета на содержание Национальной телекоммуникационной сети утверждаются Кабинетом Министров Украины.

5. Внедрение организационно-технической модели кибербезопасности как составляющей национальной системы кибербезопасности осуществляется Государственным центром киберзащиты, который обеспечивает создание и функционирование основных составляющих системы защищенного доступа государственных органов к сети Интернет, системы антивирусной защиты информационных ресурсов, аудита информационной безопасности и состояния киберзащиты объектов критической информационной инфраструктуры, системы обнаружения уязвимостей и реагирования на киберинциденты и кибератаки по объектам киберзащиты, системы взаимодействия команд реагирования на компьютерные чрезвычайные события, а также во взаимодействии с другими субъектами обеспечения кибербезопасности разрабатывает сценарии реагирования на киберугрозы, меры по противодействию таким угрозам, программы и методики проведения кибернавчань.

6. Органы государственной власти, военные формирования, образованные в соответствии с законами Украины, государственные предприятия, учреждения и организации с целью устранения возможных последствий киберинцидентов и кибератак создают резервные копии национальных электронных информационных ресурсов, которые находятся в их владении или распоряжении и являются критическими для их устойчивого функционирования и передают их на хранение в Национальный центр резервирования государственных информационных ресурсов, кроме тех, передача которых ограничена законодательством. Порядок передачи, хранения и доступа к указанным копиям определяется Кабинетом Министров Украины.

Национальный центр резервирования государственных информационных ресурсов обеспечивает:

1) непрерывность работы соответствующего национального электронного информационного ресурса, резервного копирования информации и сведений национального электронного информационного ресурса через единые основные и резервные защищенные центры обработки данных (дата-центры), предназначенные для обработки национальных электронных информационных ресурсов, резервного копирования национальных электронных информационных ресурсов;

2) надежное функционирование серверного оборудования, системы хранения данных, активного сетевого оборудования, архитектурно-технических решений по резервному копированию и дублированию информационных систем, постоянно работающей инженерной инфраструктуры;

3) осуществление обязательного контроля за статистическими данными работы по физической защите объектов, системы управления и мониторинга информационных систем, комплекса организационных мероприятий;

4) разработка, создание (построение), модернизацию, развитие, внедрение и сопровождение программного обеспечения информационной системы (платформы) для построения и ведения реестров.

Статья 9. Правительственная команда реагирования на компьютерные чрезвычайные события Украины CERT-UA

1. Задачами CERT-UA являются:

1) накопление и проведения анализа данных о киберинциденты, ведения государственного реестра киберинцидентив;

2) предоставление владельцам объектов киберзащиты практической помощи по вопросам предупреждения, выявления и устранения последствий киберинцидентив по этим объектам;

3) организация и проведение практических семинаров по вопросам киберзащиты для субъектов национальной системы кибербезопасности и владельцев объектов киберзащиты;

4) подготовка и размещение на своем официальном сайте рекомендаций по противодействию современным видам кибератак и киберугроз;

5) взаимодействие с правоохранительными органами, обеспечение их своевременного информирования о кибератаки;

6) взаимодействие с иностранными и международными организациями по вопросам реагирования на киберинциденты, в частности в рамках участия в Форуме команд реагирования на инциденты безопасности FIRST с уплатой членских взносов;

7) взаимодействие с украинскими командами реагирования на компьютерные чрезвычайные события, а также другими предприятиями, учреждениями и организациями независимо от формы собственности, осуществляющих деятельность, связанную с обеспечением безопасности киберпространства;

8) обработки полученной от граждан информации о киберинциденты по объектам киберзащиты;

9) содействие государственным органам, органам местного самоуправления, военным формированием, созданным в соответствии с законом, предприятиям, учреждениям и организациям независимо от формы собственности, а также гражданам Украины в решении вопросов киберзащиты и противодействия киберугрозами.

2. Обеспечение функционирования CERT-UA осуществляет Государственная служба специальной связи и защиты информации Украины в пределах штатной численности и выделенных объемов финансирования.

Статья 10. Государственно-частное взаимодействие в сфере кибербезопасности

1. Государственно-частное взаимодействие в сфере кибербезопасности осуществляется путем:

1) создание системы своевременного выявления, предупреждения и нейтрализации киберугроз, в том числе с привлечением волонтерских организаций;

2) повышение цифровой грамотности граждан и культуры безопасности поведения в киберпространстве, комплексных знаний, навыков и умений, необходимых для поддержания целей кибербезопасности, реализации государственных и общественных проектов по повышению уровня осведомленности общества о киберугроз и киберзащиты;

3) обмена информацией между государственными органами, частным сектором и гражданами по киберугроз объектам критической инфраструктуры, других киберугроз, кибератак и киберинцидентив;

4) партнерства и координации команд реагирования на компьютерные чрезвычайные события;

5) привлечение экспертного потенциала, научных учреждений, профессиональных объединений и общественных организаций к подготовке ключевых отраслевых проектов и нормативных документов в области кибербезопасности;

6) оказание консультативной и практической помощи по вопросам реагирования на кибератаки;

7) формирование инициатив и создание авторитетных консультационных пунктов для граждан, представителей промышленности и бизнеса с целью обеспечения безопасности в сети Интернет;

8) внедрение механизма общественного контроля эффективности мер по обеспечению кибербезопасности;

9) периодического проведения национального саммита с профессиональными поставщиками бизнес-услуг, включая страховщиков, аудиторов, юристов, определение их роли в содействии лучшему управлению рисками в сфере кибербезопасности;

10) создание системы подготовки кадров и повышения компетентности специалистов различных сфер деятельности по вопросам кибербезопасности;

11) тесного взаимодействия с физическими лицами, общественными и волонтерскими организациями, ИТ-компаниями в целях выполнения мероприятий кибероборонь в киберпространстве.

2. Государственно-частное взаимодействие в сфере кибербезопасности применяется с учетом установленных законодательством особенностей правового режима в отношении отдельных объектов и отдельных видов деятельности.

Статья 11. Содействие субъектам обеспечения кибербезопасности Украины

Государственные органы и органы местного самоуправления, их должностные лица, предприятия, учреждения и организации независимо от формы собственности, лица, граждане и объединения граждан обязаны содействовать субъектам обеспечения кибербезопасности, сообщать известные им данные об угрозах национальной безопасности с использованием киберпространства или любых других киберугроз объектам кибербезопасности, кибератак и / или

обстоятельств, информация о которых может способствовать предотвращению, выявлению и пресечению таких угроз, противодействия киберпреступности, кибератакам и минимизации их последствий.

Статья 12. Ответственность за нарушение законодательства в сфере кибербезопасности

Лица, виновные в нарушении законодательства в сферах национальной безопасности, электронных коммуникаций и защиты информации, если киберпространство является местом и / или способом осуществления уголовного преступления другого виновного деяния, ответственность за которое предусмотрена гражданским, административным, уголовным законодательством, несут ответственность согласно закону.

Статья 13. Финансовое обеспечение мероприятий кибербезопасности

Источниками финансирования работ и мероприятий по обеспечению кибербезопасности и киберзащиты есть средства государственного и местных бюджетов, собственных средств субъектов хозяйствования, кредиты банков, средства международной технической помощи и другие источники, не запрещенные законодательством.

Статья 14. Международное сотрудничество в сфере кибербезопасности

1. Украина в соответствии с заключенными ею международными договорами осуществляет сотрудничество в сфере кибербезопасности с иностранными государствами, их правоохранительными органами и специальными службами, а также с международными организациями, осуществляющими борьбу с международной киберпреступностью.

2. Украина в соответствии с международными договорами, согласие на обязательность которых предоставлено Верховной Радой Украины, может принимать участие в совместных мероприятиях по обеспечению кибербезопасности, в частности в проведении совместных учений субъектов сектора безопасности и обороны в рамках мероприятий коллективной обороны с соблюдением требований законов Украины "О порядке направления подразделений Вооруженных сил Украины в другие государства" и "О порядке допуска и условиях пребывания подразделений вооруженных сил других государств на территории Украины".

3. В соответствии с законодательством Украины в сфере внешних сношений субъекты обеспечения кибербезопасности в пределах своих полномочий могут осуществлять международное сотрудничество в сфере кибербезопасности непосредственно на двусторонней или многосторонней основе.

4. Информацию по вопросам, связанным с борьбой с международной киберпреступностью, Украина предоставляет иностранному государству на основании запроса, соблюдая требования законодательства Украины и ее международно-правовых обязательств. Такая информация может быть предоставлена без предварительного запроса иностранного государства, если это не препятствует проведению предварительного расследования или судебного рассмотрения дела и может способствовать компетентным органам иностранного государства в прекращении кибератаки, своевременном выявлении и пресечении уголовного преступления с использованием киберпространства.

Статья 15. Контроль за законностью мер по обеспечению кибербезопасности Украины

1. Контроль за соблюдением законодательства при осуществлении мероприятий по обеспечению кибербезопасности осуществляется Верховной Радой Украины в порядке, определенном Конституцией Украины.

Парламентский контроль за соблюдением законодательства о защите персональных данных и доступ к публичной информации в сфере кибербезопасности осуществляется Уполномоченным Верховной Рады Украины по правам человека.

2. Контроль за деятельностью по обеспечению кибербезопасности субъектов сектора безопасности и обороны, других государственных органов осуществляется Президентом Украины и Кабинетом Министров Украины в порядке, определенном Конституцией и законами Украины.

3. Независимый аудит деятельности основных субъектов национальной кибербезопасности, определенных частью второй статьи 8 настоящего Закона, об эффективности системы обеспечения кибербезопасности государства проводится ежегодно в соответствии с международными стандартами аудита.

Отчеты о результатах проведения независимого аудита деятельности основных субъектов национальной кибербезопасности, определенных частью второй статьи 8 настоящего Закона, об эффективности системы обеспечения кибербезопасности государства за предыдущий год подаются Президенту Украины, Верховной Раде Украины и Кабинета Министров Украины в сорокапятидневный срок после окончания календарного года.

Комитет Верховной Рады Украины, к предмету ведения которого относятся вопросы национальной безопасности и обороны, и комитет Верховной Рады Украины, к предмету ведения которого относятся вопросы информатизации и

связи, на своих заседаниях рассматривают отчеты основных субъектов национальной кибербезопасности, определенных частью второй статьи 8 этого Закона, о результатах независимого аудита их деятельности по эффективности системы обеспечения кибербезопасности государства.

Основные субъекты национальной кибербезопасности, определенные частью второй статьи 8 настоящего Закона, представляют один раз в год отчеты о состоянии выполнения ими мероприятий по вопросам обеспечения кибербезопасности государства, отнесенных к их компетенции, должны содержать, в частности, информацию о результатах проведения независимого аудита их деятельности.

По результатам рассмотрения отчетов основных субъектов национальной кибербезопасности Комитет Верховной Рады Украины, к предмету ведения которого относятся вопросы информатизации и связи, может поставить вопрос о рассмотрении этих вопросов Верховной Радой Украины.

ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

1. Настоящий Закон вступает в силу через шесть месяцев со дня его опубликования.

2. Внести изменения в следующие законы Украины:

1) статью 7 Закона Украины "О Национальном банке Украины" (Ведомости Верховной Рады Украины, 1999 г.., № 29, ст. 238 с последующими изменениями) дополнить пунктами 32 и 33 следующего содержания:

"32) определяет порядок, требования и меры по обеспечению киберзащиты и информационной безопасности в банковской системе Украины и для субъектов перевода средств, осуществляет контроль за их выполнением; образует центр киберзащиты Национального банка Украины, обеспечивает функционирование системы киберзащиты в банковской системе Украины;

33) обеспечивает формирование и ведение перечня объектов критической инфраструктуры, а также реестра объектов критической информационной инфраструктуры в банковской системе Украины, определяет критерии и порядок отнесения объектов в банковской системе Украины к объектам критической инфраструктуры и объектов критической информационной инфраструктуры, обеспечивает проведение оценки состояния киберзащиты и аудита информационной безопасности в банковской системе Украины ";

2) в Законе Украины "Об обороне Украины" (Ведомости Верховной Рады Украины, 2000 г.., № 49, ст. 420; 2011, № 4, ст. 27; 2015, № 16, ст. 110; 2016 г., № 33, ст.

564):

а) статью 3 после абзаца девятнадцатого дополнить новым абзацем следующего содержания:

"Осуществление мер по кибероборонe (активного киберзащиты) для защиты суверенитета государства и обеспечения ее обороноспособности, предотвращения вооруженного конфликта и отпора вооруженной агрессии".

В связи с этим абзац двадцатый считать абзацем двадцать первого;

б) второе предложение части второй статьи 4 дополнить словами "в том числе проведение специальных операций (разведывательных, информационно-психологических и т.д.) в киберпространстве";

{Подпункт 3 пункта 2 раздела утратил силу на основании Закона № 912-IX от 17.09.2020}

{Подпункт 4 пункта 2 раздела утратил силу на основании Закона № 2469-VIII от 21.06.2018}

5) абзац шестой статьи 3 Закона Украины "О Службе внешней разведки Украины" (Ведомости Верховной Рады Украины, 2006г., № 8, ст. 94) после слов "национальной безопасности Украины" дополнить словами "в том числе в киберпространстве";

6) в Законе Украины "О Государственной службе специальной связи и защиты информации Украины" (Ведомости Верховной Рады Украины, 2014, № 25, ст. 890, № 29, ст. 946):

а) часть первую статьи 2 и абзац второй части первой статьи 3 после слов "криптографической и технической защиты информации" дополнить словом "киберзащиты";

б) в части первой статьи 14:

пункт 39 после слов "обеспечение функционирования" дополнить словом "правительственной";

дополнить пунктами 85-92 следующего содержания:

"85) формирование и реализация государственной политики по защите в киберпространстве государственных информационных ресурсов и информации, требование относительно защиты которой установлено законом, киберзащиты критической информационной инфраструктуры, осуществление

государственного контроля в этих сферах;

86) координация деятельности субъектов обеспечения кибербезопасности по киберзащиты;

87) обеспечение создания и функционирования Национальной телекоммуникационной сети;

88) внедрение организационно-технической модели киберзащиты, осуществления организационно-технических мероприятий по предупреждению, выявлению и реагированию на киберинциденты и кибератаки и устранения их последствий;

89) информирование о киберугрозы и соответствующие методы защиты от них;

90) обеспечение внедрения системы аудита информационной безопасности на объектах критической инфраструктуры, установление требований к аудиторам информационной безопасности, их аттестации (переаттестации)

91) координация, организация и проведение аудита защищенности коммуникационных и технологических систем объектов критической инфраструктуры уязвимость;

92) обеспечение функционирования Государственного центра киберзащиты ".

3. Кабинету Министров Украины в трехмесячный срок со дня вступления в силу настоящего Закона:

обеспечить принятие нормативно-правовых актов, необходимых для реализации настоящего Закона;

привести свои нормативно-правовые акты в соответствие с настоящим Законом;

обеспечить пересмотр и отмену министерствами и другими центральными органами исполнительной власти их нормативно-правовых актов, противоречащих настоящему Закону.

Президент Украины

П. Порошенко

г. Киев

5 октября 2017

№ 2163-VIII

Закон действующий. Актуальность проверена 10.02.2021