O‘ZBEKISTON RESPUBLIKASI PREZIDENTINING
FARMONI

2026 yil «10» марта № УП–38

Об определении Стратегии кибербезопасности Республики Узбекистан и совершенствовании системы предупреждения киберпреступности

В целях эффективной защиты интересов личности, общества и государства в киберпространстве, обеспечения стабильности информационной инфраструктуры, определения приоритетных направлений дальнейшего усиления кибербезопасности в отраслях цифровой экономики, совершенствования системы предупреждения киберпреступности, а также формирования и укрепления культуры кибербезопасности граждан **постановляю**:

1. Определить основными **стратегическими целями и задачами Республики Узбекистан в сфере кибербезопасности**:

(a) цели:

(i) укрепление национальной **киберустойчивости**, защита критической информационной и государственной цифровой **инфраструктуры**;

(ii) системное снижение киберрисков и повышение уровня цифровой безопасности граждан, частного сектора и государства;

(iii) активное **противодействие** киберпреступности;

(iv) развитие цифровых инноваций, технологий искусственного интеллекта и укрепление технологической независимости в сфере кибербезопасности;

(v) развитие **международного сотрудничества** и участие в процессах **глобального** регулирования киберпространства;

(б) задачи:

(i) создание национальных центров реагирования на киберугрозы и систем их **раннего обнаружения**, а также **оперативного обмена** данными о киберугрозах;

(ii) развитие национальной инфраструктуры цифровой идентификации, аутентификации и управления доступами, а также отечественных программных и аппаратных решений;

(iii) совершенствование законодательства и **внедрение стандартов** в области защиты данных, повышения ответственности частного сектора и реагирования на киберинциденты;

(iv) повышение возможностей цифровой криминалистики и потенциала специализированных подразделений правоохранительных органов;

(v) участие в международных киберучениях, соглашениях и совместных расследованиях киберинцидентов.

2. Утвердить:

(а) Стратегию кибербезопасности Республики Узбекистана 2026–2030 годы (далее – Стратегия) согласно **приложению № 1**;

(б) «Дорожную карту» по реализации Стратегии кибербезопасности Республики Узбекистан на 2026–2030 годы (далее – «Дорожная карта») согласно **приложению № 2**.

3. Руководители государственных органов и организаций несут **персональную ответственность** за своевременную и эффективную реализацию мер, определенных в Стратегии и «Дорожной карте».

4. Создать с **1 апреля 2026 года**:

(а) на базе соответствующих структурных подразделений в Министерства юстиции, Министерства энергетики и Налогового комитета в рамках действующих штатных единиц **Отдел по обеспечению кибербезопасности** в количестве не менее 4 штатных единиц;

(б) в нижеследующих государственных органах и организациях в рамках *действующих штатных единиц, а также в пределах фонда оплаты* труда **структурные подразделения**, ответственные за обеспечение кибербезопасности в:

(i) Комитете промышленной, радиационной и ядерной безопасности при Кабинете Министров;

(ii) Агентстве миграции при Кабинете Министров;

(iii) Национальном агентстве по энергоэффективности при Кабинете Министров;

(iv) Департаменте миграции и персонализации при Министерстве внутренних дел;

(v) Агентстве по оборонной промышленности при Министерстве обороны;

(vi) Агентстве гражданской авиации при Министерстве транспорта;

(vii) Агентстве инновационного развития при Министерстве высшего образования, науки и инноваций;

(viii) Агентстве «Узархив» при Министерстве юстиции;

(ix) Комитете по развитию конкуренции и защите прав потребителей;

(x) Агентстве по делам молодежи;

(xi) АО «Узбекгидроэнерго».

5. Государственные органы и организации, предусмотренные в пункте 4 настоящего Указа, представить **до конца 2026 года** в секретариат Совета безопасности при Президенте Республики Узбекистан информацию о результатах деятельности созданных подразделений.

6. Под председательством секретаря Совета безопасности при Президенте Республики Узбекистан создать **Национальный координационный совет по обеспечению кибербезопасности и борьбе с киберпреступностью.**

7. Секретариату Совета безопасности при Президенте Республики Узбекистан **в недельный срок** утвердить положение и состав Национального координационного совета.

8. Сформировать **с 1 апреля 2026 года** рабочие группы из специалистов Министерства энергетики, Министерства здравоохранения, Министерства дошкольного и школьного образования, высшего образования, науки и инноваций, Министерства юстиции, Министерства внутренних дел, Министерства обороны, Центрального банка, а также организаций, ответственных за оценку состояния обеспечения кибербезопасности в информационных системах в области цифрового правительства и банковско-финансовой сфере, а также в срок **до 1 июля 2026 года** представить информацию о результатах оценки в секретариат Совета безопасности при Президенте Республики Узбекистан.

9. Одобрить предложение Министерства цифровых технологий и Службы государственной безопасности о разрешении государственным органам и организациям, не имеющим соответствующего структурного подразделения (ответственного работника) по обеспечению кибербезопасности, либо достаточных сил и средств, пользоваться услугами организаций, оказывающих **аутсорсинговые услуги** по обеспечению кибербезопасности.

10. Установить порядок, в соответствии с которым государственные органы и организации могут пользоваться исключительно услугами **юридических лиц, включенных в реестр** организаций, оказывающих аутсорсинговые услуги по обеспечению кибербезопасности, в установленном порядке.

11. Службе государственной безопасности:

(а) в срок **до 1 августа 2026 года** совместно с Министерством цифровых технологий внести в Кабинет Министров проект постановления, предусматривающий порядок регистрации организаций, оказывающих аутсорсинговые услуги по обеспечению кибербезопасности, а также порядок пользования данной услугой;

(б) вести реестр организаций, оказывающих аутсорсинговые услуги по обеспечению кибербезопасности.

12. Установить порядок, в соответствии с которым начиная **с 1 апреля 2026 года** государственными органами и организациями (за исключением силовых структур и правоохранительных органов) **за счет средств внебюджетного фонда** и в **пределах бюджетных параметров направляются необходимые средства на вопросы обеспечения кибербезопасности**.

13. Одобрить предложение Службы государственной безопасности о проведении конкурсов с участием **независимых экспертов по выявлению уязвимых сторон и недостатков** национальных информационных систем и ресурсов в сфере кибербезопасности с целью **повышения уровня их устойчивости к современным кибератакам** на основе передового зарубежного опыта.

14. Определить, что **конкурсы** по выявлению связанных **с кибербезопасностью уязвимых сторон и недостатков** информационных систем и ресурсов государственных органов и организаций, а также субъектов критической информационной инфраструктуры проводятся на **специальной электронной платформе**, определяемой Службой государственной безопасности.

15. Службе государственной безопасности:

(а) в срок **до 1 августа 2026 года** совместно с Министерством юстиции разработать и внести в Кабинет Министров **порядок** проведения конкурса с участием независимых экспертов по выявлению **уязвимых сторон и недостатков** информационных систем и ресурсов в сфере кибербезопасности;

(б) в срок **до 1 октября 2026 года** создать специальную электронную платформу для проведения конкурса по выявлению связанных с кибербезопасностью уязвимых сторон и недостатков в информационных системах и ресурсах государственных органов и организаций, а также субъектов критической информационной инфраструктуры.

16. Министерству внутренних дел в срок **до 1 июля 2026 года** разработать и внести в Кабинет Министров проект постановления о создании киберлаборатории, предназначенной для информационно-технической поддержки оперативной деятельности.

17. Службе государственной безопасности совместно с Министерством цифровых технологий, Министерством высшего образования, науки и инноваций, Министерством дошкольного и школьного образования в целях повышения знаний молодежи по безопасному пользованию интернетом **до конца 2026 года**:

(а) организовать для учащихся старших классов в рамках воспитательных часов **занятий по киберкультуре**;

(б) разработать платформы, предоставляющие **бесплатные онлайн-курсы** по основам кибербезопасности, и социальные ролики по тематике для студентов и учащихся школ.

18. Секретариату Совета безопасности при Президенте Республики Узбекистан:

(а) эффективно организовать и скоординировать деятельность министерств, ведомств и организаций, ответственных за реализацию мер, определенных в «Дорожной карте»;

(б) провести контрольные мероприятия по своевременной, полной и качественной реализации «Дорожной карты» ответственными исполнителями, в том числе в разрезе регионов;

(в) координировать деятельность министерств, ведомств, государственных учреждений, а также банков, операторов платежных систем, кредитных и платежных организаций по реформированию системы кибербезопасности;

(г) ежеквартально проводить обсуждение исполнения поручений, определенных настоящим Указом.

19. Контроль за исполнением настоящего Указа возложить на Премьер-министра Республики Узбекистан Арипова А.Н. и секретаря Совета безопасности при Президенте Республики Узбекистан Махмудова В.В.

Президент
Республики Узбекистан **Ш. Мирзиёев**

O'ZBEKISTON RESPUBLIKASI PREZIDENTI ADMINISTRATSIYASI
KANSELYARIYA
1

город Ташкент

Приложение № 1
к Указу Президента Республики Узбекистан
от 10 марта 2026 года № УП–38

СТРАТЕГИЯ
кибербезопасности Республики Узбекистан на 2026–2030 годы

Глава 1. Основная цель и задачи Стратегии

1. Основной целью настоящей Стратегии является определение приоритетных направлений обеспечения кибербезопасности на последующие пять лет.

2. Задачами достижения основной цели Стратегии являются:

(а) дальнейшее развитие системы государственной защиты, предусматривающей защиту от киберугроз информационных систем и ресурсов, а также объектов критической информационной инфраструктуры государственных органов и организаций;

(б) повышение киберустойчивости объектов информатизации и критической информационной инфраструктуры государственных органов и организаций;

(в) обеспечение стабильного и бесперебойного функционирования объектов критической информационной инфраструктуры, государственных информационных систем и ресурсов;

(г) выявление и предотвращение преступлений и иных правонарушений, совершаемых посредством информационных технологий, широкое использование в этих целях цифровой криминалистики;

(д) совершенствование мер и методов борьбы с киберпреступностью, а также усиление ответственности за совершение незаконных действий в киберпространстве;

(ж) усиление контроля за строгим соблюдением требований кибербезопасности на объектах критической информационной инфраструктуры, а также установление ответственности за нарушение требований законодательства в сфере кибербезопасности;

(з) формирование позитивного имиджа страны и укрепление ее авторитета на международной арене путем представления достоверной и качественной, объективной информации о государственной политике в сфере кибербезопасности;

(и) создание системы повышения уровня профессионального образования специалистов в сфере кибербезопасности, а также оценки уровня их квалификации;

(к) разработка действенных механизмов интеграции образования, науки и предпринимательства для широкого применения результатов научных исследований, опытно-конструкторских и технологических работ;

(л) создание необходимых условий для беспрепятственного доступа к интернету, особенно дальнейшее повышение культуры пользования интернетом молодежью, предупреждение становления молодых людей жертвами ложной информации, формирования их мировоззрения под влиянием негативных идей, а также повышение грамотности граждан по пользованию интернетом;

(м) развитие организационно-технической базы по обеспечению кибербезопасности государственных органов и объектов критической информационной инфраструктуры;

(н) внедрение передовых и инновационных технологий по обеспечению кибербезопасности;

(о) дальнейшее укрепление сотрудничества с компетентными органами зарубежных стран, международными и зарубежными структурами и организациями в сфере кибербезопасности. В частности, развитие сотрудничества с государствами Организации Объединенных Наций, Содружества Независимых Государств, Шанхайской организации сотрудничества, Организации тюркских государств, Лиги арабских государств, в рамках других международных и региональных организаций по вопросам кибербезопасности, а также привлечение международного опыта и технологий посредством стратегического партнерства;

(п) развитие совместных инициатив по вопросам кибербезопасности и борьбы с киберпреступностью в Центральной Азии.

Глава 2. Приоритетные направления Стратегии

3. Приоритетными направлениями реализации Стратегии являются:

(а) совершенствование нормативно-правового и организационно-технического обеспечения сферы кибербезопасности;

(б) поддержка развития государственной системы защиты информационных систем и ресурсов, а также объектов критической информационной инфраструктуры государственных органов и организаций;

(в) внедрение системы мониторинга состояния кибербезопасности, а также обеспечение активного и оперативного взаимодействия субъектов кибербезопасности с уполномоченным органом в целях предупреждения инцидентов кибербезопасности;

(г) создание благоприятных условий для разработки и развития производства средств обеспечения кибербезопасности, инновационного развития научных организаций и производственных предприятий в сфере кибербезопасности;

(д) повышение эффективности системы предупреждения и противодействия преступлениям в сфере информационных технологий;

(ж) развитие государственно-частного партнерства по обеспечению кибербезопасности, а также привлечение частного сектора в процессы предупреждения киберугроз и защиты от них;

(з) усиление мер по противодействию киберугрозам в деятельности кредитных и платежных организаций, операторов платежных систем, валютных бирж и кредитных бюро, а также по обеспечению кибербезопасности в информационных системах и мобильных приложениях;

(и) повышение квалификации кадров и киберграмотности населения в сфере обеспечения кибербезопасности;

(к) усиление международного сотрудничества в сфере обеспечения кибербезопасности и повышение эффективности совместных действий против трансграничных киберугроз.

§ 1. Нормативно-правовое и организационно-техническое совершенствование сферы кибербезопасности в целях повышения уровня защиты от киберугроз государственных информационных систем и ресурсов, других объектов информатизации, а также объектов критической информационной инфраструктуры

4. В данном направлении осуществляются:

(а) установление нормативных стандартов, требований и мер, направленных на:

(i) организационно-техническое обеспечение объектов критической информационной инфраструктуры с учетом их категорий и с применением единых подходов и методов их киберзащиты;

(ii) обеспечение безопасных загрузки и обновления посредством интернета системных и прикладных программ, используемых в защищенных закрытых информационных системах, а также на объектах критической информационной инфраструктуры государственных органов и организаций;

(iii) обеспечение интеграции государственных информационных систем для безопасного обмена данными в рамках цифрового правительства, а также идентификации и классификации защищенной информации в информационных системах и обмене между ними на основе метаданных (metadata);

(iv) обеспечение кибербезопасности сетей операторов телекоммуникаций, оказывающих услуги доступа к интернету;

(б) совершенствование организационной структуры в государственных органах и организациях, а также на субъектах критической информационной инфраструктуры для эффективного обеспечения кибербезопасности;

(в) усиление ответственности должностных лиц за невыполнение требований законодательства в сфере информационных технологий и кибербезопасности;

(г) совершенствование инфраструктуры единого оператора и единого узла кибербезопасности, обеспечение подключения к ним информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры;

(д) повышение уровня кибербезопасности при интеграции государственных информационных систем в рамках цифрового правительства;

(ж) повышение уровня защищенного использования (установление требований по идентификации и многофакторной аутентификации, а также защищенному подключению при доступе к онлайн-услугам) информационных систем и ресурсов при оказании государственных и коммерческих услуг в формате онлайн;

(з) усиление контроля за использованием руководителями государственных органов и организаций эффективных методов и средств защиты от современных киберугроз и проблем кибербезопасности, а также за политикой информационной безопасности организаций;

(и) внедрение системы мониторинга соблюдения требований обеспечения кибербезопасности объектов информатизации, предназначенных для обработки сведений, содержащих государственные секреты;

(к) внедрение системы контроля соблюдения требований кибербезопасности в системе Вооруженных Сил Республики Узбекистан;

(л) разработка системы технического регулирования в сфере кибербезопасности;

(м) внедрение механизма признания сертификатов соответствия и протоколов испытаний, осуществленных в рамках международных договоров в сфере кибербезопасности.

§ 2. Государственная поддержка развития государственной системы защиты информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры

5. В данном направлении осуществляются:

(а) ежегодное планирование средств, необходимых для обеспечения кибербезопасности (продление лицензии средств обеспечения кибербезопасности, повышение квалификации специалистов, подключение к узлу кибербезопасности и прочие) в государственных органах, за счет внебюджетных средств;

(б) привлечение иностранных инвестиций и грантов при внедрении сертифицированных и прошедших экспертизу средств и систем защиты информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры.

§ 3. Внедрение системы мониторинга состояния кибербезопасности, а также обеспечение активного и оперативного взаимодействия субъектов кибербезопасности и уполномоченного органа в целях предупреждения инцидентов кибербезопасности

6. В данном направлении осуществляются:

(а) образование центров создания Национальной системы мониторинга и реагирования на инциденты кибербезопасности (SOC);

(б) формирование системы оперативного взаимодействия субъектов критической информационной инфраструктуры, уполномоченного органа по кибербезопасности и правоохранительных органов по реагированию на инциденты кибербезопасности;

(в) создание и внедрение систем по обнаружению уязвимостей и недостатков в информационных системах и ресурсах, а также на объектах критической информационной инфраструктуры государственных органов и организаций;

(г) обеспечение оперативного обмена данными по новым киберугрозам и уязвимостям, информирование о них участников в сфере кибербезопасности для эффективного реагирования на них и повышения защищенности объектов.

§ 4. Создание благоприятных условий для разработки и развития производства средств обеспечения кибербезопасности, инновационного развития научных организаций и производственных предприятий в сфере кибербезопасности

7. В данном направлении осуществляются:

(а) с привлечением частных организаций по государственной поддержке использования средств обеспечения кибербезопасности и обеспечение их участия в технопарках;

(б) определение приоритетных направлений исследований и разработок в сфере кибербезопасности, в частности внедрение технологий искусственного интеллекта и блокчейн, формирование и оказание целевой государственной поддержки государственных заказов на проведение указанных работ для государственных нужд;

(в) разработка эффективных форм сотрудничества и осуществление совместных научных исследований с научными и академическими учреждениями, профессиональными и общественными объединениями;

(г) проведение исследований правовых, организационных, технических и практических аспектов противодействия современным кибератакам и киберпреступлениям, ускорение научных и практических исследований в сфере кибербезопасности в целях разработки инновационных и эффективных методов, технологий и стратегий защиты, основанных на международном опыте.

§ 5. Создание эффективной системы предупреждения и противодействия преступлениям и другим правонарушениям в сфере информационных технологий

8. В данном направлении осуществляются:

(а) усиление деятельности подразделений правоохранительных органов, ответственных за предупреждение, выявление и раскрытие преступлений и правонарушений, совершаемых с использованием информационных технологий, а также создание и повышение на постоянной основе уровня подготовки оперативных групп, занимающихся развитием внедрения современных технологий в сферу и эффективным реагированием на кибератаки;

(б) внедрение подготовки киберкриминалистов в целях обеспечения активного использования современных форм, средств и методов оперативно-розыскной и следственной деятельности, обеспечения кибербезопасности на наиболее высоком уровне и эффективного противодействия киберпреступности;

(в) развитие сферы цифровой криминалистики в правоохранительных органах, включая подготовку и обучение специалистов, создание специализированных лабораторий, сбор и анализ цифровых доказательств, а также разработку и внедрение методов и технологий расследования;

(г) осуществление правоохранительными органами профилактических мероприятий по противодействию мошенничеству и иным правонарушениям в киберпространстве, создание эффективных механизмов взаимодействия правоохранительных органов и населения по информированию граждан о киберпреступлениях, а также упрощение процесса направления заявлений и сообщений о киберпреступлениях путем создания онлайн-услуг и платформ диалога с гражданами;

(д) регулярное информирование работников государственных организаций и общественности о новостях по кибербезопасности, проведение тренингов по обучению руководителей и работников, а также разъяснение населению понятий кибербезопасности в форме тщательно разработанных роликов в средствах массовой информации;

(ж) совершенствование Уголовного кодекса и Кодекса об административной ответственности в части усиления ответственности за преступления и правонарушения, совершаемые с использованием информационных технологий, а также установления ответственности за новые общественно опасные деяния, совершаемые в киберпространстве;

(з) разработка и реализация мер противодействия киберпреступности с использованием средств телекоммуникаций для защиты граждан от телефонного и интернет-мошенничества, в том числе:

(и) создание антифишинговой платформы для автоматического обнаружения и противодействия мошенническим веб-сайтам;

(к) выявление и блокировка потенциально мошеннических звонков или направление оповещения о них;

(л) определение обязательств операторов и провайдеров мобильной связи по блокированию ложных (подозрительных) звонков или принятие мер, направленных на предупреждение и защиту пользователей от нежелательных вызовов;

(м) ограничение (отклонение) рекламных и спам-вызовов и другие;

(н) обеспечение оперативного взаимодействия и интеграции государственных органов, правоохранительных органов, субъектов критической информационной инфраструктуры для противодействия преступлениям в сфере информационных технологий, включая разработку регламента оперативного взаимодействия государственных органов, правоохранительных органов, коммерческих банков (далее – банки), операторов телекоммуникаций по предотвращению киберпреступлений.

§ 6. Привлечение частных организаций в сфере кибербезопасности

9. В данном направлении осуществляются:

(а) вовлечение частного сектора в сферу обеспечения кибербезопасности, включая обеспечение киберзащиты, мониторинг и управление инцидентами кибербезопасности, оценку киберзащищенности, подготовку и повышение квалификации специалистов, разработку стандартов и другие, а также создание условий для внесения частным сектором инвестиций в данную сферу;

(б) установление требований по обеспечению кибербезопасности облачных услуг (дата-центры, хостинг-сайты, облачные хранилища файлов и другие), используемых для формирования или размещения информационных систем, ресурсов и иных объектов информатизации государственных органов и организаций;

(в) установление контроля за исполнением требований кибербезопасности организациями, оказывающими услуги аутсорсинга и облачные услуги;

(г) создание механизмов обмена данными между государственными органами и частными организациями для своевременного выявления и ликвидации киберугроз;

(д) создание платформ взаимодействия и сотрудничества государственных органов и частных организаций в сфере кибербезопасности, включая интернет-платформы и форумы, платформы тестирования технологий кибербезопасности и другие.

§ 7. Усиление мер по противодействию киберугрозам в деятельности кредитных и платежных организаций, операторов платежных систем, валютных бирж и кредитных бюро, а также по обеспечению кибербезопасности в информационных системах и мобильных приложениях

10. В данном направлении осуществляются:

(а) определение требований по противодействию киберугрозам, предъявляемых к банкам, операторам платежных систем, платежным и кредитным организациям, включая:

(i) обеспечение киберустойчивости банковских и платежных систем;

(ii) повышение операционной надежности и бесперебойности деятельности по оказанию финансовых услуг организаций кредитно-банковской сферы;

(б) разработка мер по противодействию различным видам мошенничества в сфере банковских услуг с учетом современного международного опыта, включая:

(i) тесное сотрудничество банков с клиентами в сфере противодействия киберпреступности;

(ii) информирование (повышение осведомленности) клиентов о таких угрозах, как фишинг и социальная инженерия, а также их обучение безопасному пользованию онлайн-банкингом и другим;

(в) создание механизмов активного сотрудничества в соответствии с актами законодательства между кредитными и платежными организациями, операторами платежных систем, валютными биржами, кредитными бюро и правоохранительными органами по предотвращению и расследованию киберпреступлений в деятельности указанных организаций;

(г) создание эффективных механизмов («телефоны доверия», чат-боты, прочие онлайн-услуги и платформы) взаимодействия Центрального банка и банков с населением по информированию о киберпреступлениях, предоставлению консультаций.

§ 8. Развитие кадрового потенциала в сфере кибербезопасности, а также повышение квалификации работников, уровня правовой и цифровой культуры (киберграмотности) населения в сфере кибербезопасности

11. В данном направлении осуществляются:

(а) внедрение механизма обучения специалистов государственных органов и организаций, субъектов критической информационной инфраструктуры по различным направлениям кибербезопасности, включая аудит, анализ инцидентов кибербезопасности, цифровую криминалистику, кибербезопасность на объектах критических информационной инфраструктуры, кибербезопасность в банковской сфере и другим направлениям;

(б) создание условий для получения специалистами в сфере кибербезопасности сертификатов CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CEH (Certified Ethical Hacker), CompTIA Security+ и других международных сертификатов, а также внедрение механизма покрытия расходов, связанных с обучением;

(в) внедрение системы аттестации специалистов по кибербезопасности, допущенных к работе в государственных органах и организациях, а также субъектах критической информационной инфраструктуры;

(г) создание механизма взаимодействия и стимулирования обмена информацией между государственными органами и населением по вопросам обеспечения кибербезопасности, а также повышение осведомленности населения о киберугрозах и наилучших практиках безопасности, включая обучение безопасному пользованию интернетом и онлайн-услугами;

(д) организация занятий по кибергигиене для учащихся и студентов по обучению базовым знаниям безопасных действий в сети интернет в рамках воспитательных часов для учащихся старших классов, а также создание платформ, предоставляющих бесплатные онлайн-курсы по основам кибербезопасности для студентов и учащихся школ;

(ж) организация клубов кибербезопасности по поддержке талантливой молодежи в сфере кибербезопасности в регионах республики.

§ 9. Дальнейшее укрепление сотрудничества в сфере обеспечения кибербезопасности с международными и зарубежными структурами и организациями

12. В данном направлении осуществляются:

(а) дальнейшее укрепление сотрудничества в сфере кибербезопасности с международными и зарубежными структурами и организациями. В частности, развитие сотрудничества с государствами ООН, СНГ, ШОС, Организации тюркских государств и Лиги арабских государств, в рамках других международных и региональных организаций по вопросам кибербезопасности, а также привлечение международного опыта и технологий посредством стратегического партнерства. Развитие совместных инициатив по вопросам кибербезопасности и борьбы с киберпреступностью в Центральной Азии;

(б) активизация сотрудничества с зарубежными государственными и частными структурами, службами кибербезопасности, включая CERT-службы;

(в) участие в формировании международной системы кибербезопасности, направленной на противодействие использованию киберпространства в террористических, преступных и иных незаконных целях, подготовка и продвижение национальных инициатив, соответствующих интересам страны и способствующих укреплению ее кибербезопасности.

Глава 3. Результаты, ожидаемые от реализации Стратегии

13. Посредством выполнения установленных Стратегией задач ожидается достижение следующих результатов:

(а) укрепление цифрового суверенитета страны, защита национальной экономики от цифровых угроз и повышение доверия к кибербезопасности в обществе;

(б) формирование эффективного подхода к надежной защите кибербезопасности государственных информационных систем, ресурсов, других объектов информатизации и критической информационной инфраструктуры, обеспечение их стабильного и бесперебойного функционирования;

(в) уменьшение количества преступлений, совершаемых с использованием информационных технологий, а также повышение уровня их раскрываемости;

(г) повышение доверия пользователей к цифровым услугам;

(д) привлечение частного сектора и населения к обеспечению кибербезопасности;

(ж) создание условий для повышения квалификации специалистов в сфере кибербезопасности, а также привлечение талантливой молодежи к процессам обеспечения кибербезопасности;

(з) увеличение доли средств защиты информации в производстве локальных информационно-коммуникационных продуктов;

(и) постоянное совершенствование научных исследований и разработок в сфере кибербезопасности, а также повышение уровня инновационной активности производственных предприятий;

(к) повышение киберграмотности и укрепление культуры кибербезопасности населения при использовании цифровых сервисов;

(л) усиление ответственности должностных лиц и организаций за соблюдение требований обеспечения кибербезопасности.

Глава 4. Заключительные положения

14. Настоящая Стратегия служит основой для разработки ведомственных программ, научно-исследовательских работ, планов мероприятий и стандартов по обеспечению кибербезопасности.

15. Контроль за исполнением пунктов Стратегии и оценка эффективности реализуемых мер возлагаются на секретариат Совета безопасности при Президенте Республики Узбекистан.

Приложение № 2
к Указу Президента Республики Узбекистан
от 10 марта 2026 года № УП–38

«ДОРОЖНАЯ КАРТА»
по реализации Стратегии кибербезопасности Республики Узбекистан на 2026–2030 годы

№	Наименование мер	Механизм реализации	Форма реализации	Сроки исполнения	Ответственные исполнители
I. Совершенствование нормативно-правового и организационно-технического обеспечения сферы кибербезопасности государственных информационных систем и ресурсов, других объектов информатизации и объектов критической информационной инфраструктуры					
1.	Определение правил, требований и мер по обеспечению кибербезопасности государственных информационных систем и ресурсов, других объектов информатизации и объектов критической информационной инфраструктуры.	1. Разработка нормативно-правовых актов, определяющих требования и меры по обеспечению кибербезопасности, с учетом категорий объектов информатизации и объектов критической информационной инфраструктуры.	Проект нормативно-правового акта	Май 2026 года	СГБ, Минобороны, МВД, МЧС, ГСБП, Нацгвардия, Минцифры, ЦРЭТ, заинтересованные министерства и ведомства
		2. Разработка требований и практических рекомендаций по безопасному обновлению систем и прикладных программ посредством сети интернет с учетом результатов практических исследований и испытаний.	Проект нормативно-правового акта	Июнь 2026 года	
		3. Разработка требований по обеспечению кибербезопасности сетей операторов телекоммуникаций, *предоставляющих услуги доступа к сети* интернет.	Проект нормативно-правового акта	Август 2026 года	
		4. Разработка требований по обеспечению кибербезопасности сетей операторов телекоммуникаций, предоставляющих услуги доступа к сети интернет.	Проект нормативно-правового акта	Сентябрь 2026 года	СГБ, Минцифры, Минобороны, МВД, заинтересованные министерства и ведомства

		5. Разработка классификатора уровня кибербезопасности информационных систем и ресурсов государственных органов и организаций. 6. Разработка требований по обеспечению информационной и кибербезопасности при интеграции государственных информационных систем в рамках цифрового правительства.	Проект нормативно-правового акта Национальные стандарты	Октябрь 2026 года Январь 2027 года	Минцифры, ЦРЭТ, СГБ
2.	Совершенствование организационной структуры государственных органов и организаций, а также субъектов критической информационной инфраструктуры для эффективного обеспечения их кибербезопасности.	1. Проведение анализа вопросов организации деятельности структурных подразделений по обеспечению кибербезопасности государственных органов и организаций, а также субъектов критической информационной инфраструктуры. 2. Разработка требований, предъявляемых к организационно-штатной структуре подразделений по обеспечению кибербезопасности государственных органов и организаций, а также объектов критической информационной инфраструктуры. 3. Разработка типового положения о структурном подразделении по обеспечению кибербезопасности государственных органов и организаций, объектов КИИ.	Аналитическая справка в секретариат Совета безопасности Проект постановления Кабинета Министров	Июль 2026 года Август 2026 года	СГБ, Минобороны, МВД, МЧС, ГСБП, Нацгвардия, Минцифры, ЦРЭТ, заинтересованные министерства и ведомства
3.	Установление ответственности должностных лиц за невыполнение требований законодательства в сфере информационной и кибербезопасности.	Разработка проекта закона, предусматривающего привлечение должностных лиц к ответственности за невыполнение требований законодательства в сфере информационной и кибербезопасности.	Проект закона	Октябрь 2026 года	СГБ, Генпрокуратура, Минюст, Минцифры, Центральный банк

4.	Совершенствование инфраструктуры единого оператора и единого узла кибербезопасности, обеспечение подключения к ним информационных систем и ресурсов государственных органов и организаций, а также объектов КИИ.	1. Предусмотрение подключения информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры к сети интернет посредством Единого оператора со скоростью не менее 1 Гбит/с. 2. Подключение органов исполнительной власти на местах к Единому оператору.	План мер План мер	Январь 2027 года Декабрь 2029 года	СГБ, Минцифры
5.	Повышение уровня кибербезопасности при интеграции государственных информационных систем в рамках цифрового правительства.	1. Разработка требований по обеспечению киберзащиты Межведомственной интеграционной платформы для защищенного обмена данными при интеграции государственных информационных систем. 2. Реализация мер киберзащиты Межведомственной интеграционной платформы.	Ведомственный акт План мер	Апрель 2027 года Сентябрь 2027 года	Минцифры, СГБ, ГСБП
6.	Повышение уровня защищенного использования информационных систем и ресурсов при оказании государственных, банковских и других электронных коммерческих услуг в режиме онлайн.	1. Разработка проекта нормативно-правового акта, определяющего требования организации защищенного соединения при идентификации, многофакторной аутентификации и пользовании онлайн-услугами. 2. Реализация мер защищенного использования информационных систем и ресурсов при предоставлении онлайн-услуг.	Проект нормативно-правового акта План мер	Май 2027 года Декабрь 2027 года	СГБ, Минцифры, Центральный банк
7.	Внедрение системы контроля соблюдения требований кибербезопасности в системе Вооруженных Сил Республики Узбекистан.	1. Подготовка предложений по внедрению системы контроля соблюдения требований кибербезопасности в Вооруженных Силах. 2. Разработка соответствующего проекта нормативно-правового акта.	Аналитическая справка секретариату Совета безопасности Проект нормативно-правового акта	Декабрь 2026 года Март 2027 года	Минобороны, СГБ, ГСБП, Нацгвардия

8.	Развитие системы регулирования технических требований в сфере кибербезопасности.	1. Изучение и анализ международного и зарубежного опыта в области технического регулирования. 2. Разработка требований, предъявляемых к средствам обеспечения кибербезопасности и проверяемых на соответствие в период их сертификации. 3. Разработка технического регламента, определяющего классификацию средств обеспечения кибербезопасности и общие требования, предъявляемые к ним.	Аналитическая справка в секретариат Совета безопасности Национальные стандарты Технический регламент	Ноябрь 2026 года Декабрь 2029 года Согласно отдельно утвержденному плану-графику	СГБ, ГСБП, заинтересованные министерства и ведомства СГБ, Узбекское агентство по техническому регулированию
9.	Организация работ по признанию результатов оценки соответствия в сфере кибербезопасности, проведенной в зарубежных государствах.	1. Установление сотрудничества между ведомствами по сертификации в сфере кибербезопасности Узбекистана и службами сертификации в данной сфере США, Канады, Китая, России, Беларуси, Южной Кореи, Японии, Сингапура и государств ЕС. 2. Изучение правовых основ работ по оценке соответствия в сфере кибербезопасности, проводимых в зарубежных государствах. 3. Достижение соглашений (договоренностей) о взаимном признании результатов оценки соответствия со службами сертификации зарубежных государств.	Практические меры Международные соглашения	До 2030 года на постоянной основе До 2030 года на постоянной основе	СГБ, Узбекское агентство по техническому регулированию

II. Государственная поддержка развития государственной системы защиты информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры					
10.	Привлечение иностранных инвестиций и грантов для внедрения сертифицированных и прошедших экспертизу средств и систем защиты в информационные системы и ресурсы государственных органов и организаций, а также объекты критической информационной инфраструктуры.	1. Определение потребности министерств и ведомств в привлечении иностранных инвестиций, грантов и кредитов для внедрения средств и систем защиты. 2. Принятие мер по привлечению инвестиций, грантов и кредитов на основе проектной документации, разработанной в установленном порядке.	Программа мероприятий	Сентябрь 2026 года В сроки, согласованные с иностранной стороной	Министерство инвестиций, промышленности и торговли, заинтересованные министерства и ведомства Министерство инвестиций, промышленности и торговли, Министерство экономики и финансов
III. Внедрение системы мониторинга состояния кибербезопасности и обеспечение активного и оперативного взаимодействия субъектов кибербезопасности и уполномоченных органов в целях предотвращения инцидентов кибербезопасности					
11.	Образование центров путем создания Национальной системы мониторинга инцидентов кибербезопасности и реагирования на них (SOC).	1. Определение структуры Национальной системы мониторинга инцидентов кибербезопасности и реагирования на них, состоящей из центрального и отраслевых SOC. 2. Разработка проекта нормативно-правового акта, устанавливающего требования к Национальной системе мониторинга инцидентов кибербезопасности и реагирования на них. 3. Разработка и реализация проекта по созданию национальной системы мониторинга инцидентов кибербезопасности и реагирования на них.	Практические меры Проект постановления Кабинета Министров Технические задания и план мер	Декабрь 2026 года Март 2027 года Декабрь 2029 года	СГБ, ГСБП, МВД, Минцифры, ЦРЭТ, Центральный банк, заинтересованные министерства и ведомства

12.	Формирование системы оперативного взаимодействия по реагированию на инциденты кибербезопасности субъектов критической информационной инфраструктуры с уполномоченным органом по кибербезопасности и правоохранительными органами.	Подготовка регламента взаимодействия с субъектами критической информационной инфраструктуры по реагированию на инциденты кибербезопасности.	Проект нормативно-правового акта	Декабрь 2026 года	СГБ, МВД, Минцифры, ЦРЭТ, Минобороны, заинтересованные министерства и ведомства
IV. Создание благоприятных условий для разработки и развития производства средств кибербезопасности, а также инновационного развития научных организаций и производственных предприятий в сфере кибербезопасности					
13.	Привлечение частных организаций для государственной поддержки применения средств обеспечения кибербезопасности и обеспечение их участия в технопарках.	1. Изучение передового зарубежного опыта создания благоприятных условий для использования средств защиты информации, привлечение частных организаций. 2. Подготовка проекта нормативно-правового акта по созданию благоприятных условий для разработки, производства и использования средств кибербезопасности, а также привлечение частных организаций с учетом зарубежного опыта. 3. Установление связей с иностранными компаниями, специализирующимися на разработке и производстве средств защиты информации для использования на объектах информатизации и объектах КИИ.	Аналитическая справка в секретариат Совета безопасности Проект постановления Кабинета Министров Соглашение (Меморандум)	Август 2026 года Сентябрь 2026 года Январь 2027 года	СГБ, Минобороны, Минцифры, МВД, ГСБП, Центральный банк, Министерство экономики и финансов, Нацгвардия, заинтересованные министерства и ведомства

14.	Определение приоритетных направлений исследований и разработок в сфере кибербезопасности, включая внедрение искусственного интеллекта, квантовых и блокчейн-технологий, формирование государственных заказов на выполнение указанных работ для государственных нужд, их государственная целевая поддержка.	1. Формирование необходимых тем исследований и направлений разработок в сфере кибербезопасности. 2. Подготовка и утверждение программы исследований и разработок, осуществляемых в сфере кибербезопасности на 2026–2030 годы.	Практические меры Программа исследований и разработок с указанием исполнителей, объема и источников финансирования	Сентябрь 2026 года Январь 2027 года	СГБ, ГСБП, Минобороны, Министерство высшего образования, науки и инноваций, Минцифры, заинтересованные министерства и ведомства
15.	Проведение исследований по правовым, организационным, техническим и практическим аспектам противодействия современным кибератакам и киберпреступлениям, ускорение научно-практических исследований по разработке основанных на международной практике инновационных и эффективных методов, технологий и стратегий защиты в сфере кибербезопасности.	1. Обучение и проведение научных исследований в направлении правового обеспечения кибербезопасности. 2. Подача в установленном порядке заявок для участия в конкурсах на осуществление научно-исследовательских проектов в сфере кибербезопасности научными и академическими учреждениями, профессиональными и общественными объединениями. 3. Принятие мер по внедрению в практику результатов научно-исследовательских работ (PhD, DSc) и научных статей в сфере кибербезопасности.	Программа научных исследований	Январь 2027 года	СГБ, Минобороны, Министерство высшего образования, науки и инноваций, Минцифры

V. Создание эффективной системы предупреждения и противодействия преступлениям и иным правонарушениям в сфере информационных технологий					
16.	Усиление деятельности подразделений правоохранительных органов, ответственных за предупреждение, выявление и раскрытие преступлений и правонарушений, совершаемых с использованием информационных технологий, а также развитие внедрения современных технологий в данную сферу.	1. Изучение зарубежного опыта и подготовка предложений по увеличению штатов подразделений органов внутренних дел, ответственных за противодействие преступлениям в сфере информационных технологий, соразмерно криминогенной обстановке в данном направлении, а также развитию внедрения современных технологий в данную сферу.	Аналитическая справка в секретариат Совета безопасности	Август 2027 года	МВД, СГБ
		2. Разработка и внесение в Кабинет Министров в установленном порядке проекта постановления Президента Республики Узбекистан по усилению деятельности подразделений органов внутренних дел, ответственных за противодействие преступлениям в сфере информационных технологий.	Проект постановления Президента Республики Узбекистан	Ноябрь 2027 года	
		3. Привлечение квалифицированных специалистов в специализированные структурные подразделения Министерства внутренних дел по противодействию киберпреступности и другим правонарушениям.	Программа мероприятий	Ноябрь 2027 года	
17.	Развитие сферы цифровой криминалистики в правоохранительных органах, включая подготовку и обучение специалистов.	1. Подготовка учебной программы по цифровой криминалистике для специалистов правоохранительных органов.	Учебная программа	Июнь 2026 года	МВД, Генпрокуратура, СГБ, ЦРЭТ, Минюст
		2. Разработка и внесение проекта нормативно-правового акта о совершенствовании деятельности по цифровой криминалистике в системе Министерства внутренних дел, а также	Проект постановления Кабинета Министров	Декабрь 2026 года	

		созданию Киберлаборатории по информационно-технической поддержке оперативной деятельности. 3. *Разработка методов и технологий* сбора, анализа цифровых доказательств и ведения следствия.	Методические разработки и пособия	Декабрь 2027 года	
18.	Разработка и реализация мер противодействия киберпреступности, создание эффективных механизмов взаимодействия *правоохранительных органов* с населением, а также осуществление интеграции государственных органов, правоохранительных органов, банков и операторов телекоммуникаций в целях противодействия *киберпреступности.*	1. Создание информационной системы онлайн-взаимодействия государственных органов, правоохранительных органов, банков и операторов телекоммуникаций по оперативному выявлению и блокировке действий мошенников. 2. Создание Межведомственной рабочей группы специалистов по изучению и разработке мер упреждения мошеннических схем, реализуемых с использованием цифровых технологий, а также информирование населения о возможных способах и схемах мошенничества и требуемых действиях для защиты от них. 3. Разработка регламента оперативного взаимодействия государственных органов, правоохранительных органов, банков и операторов телекоммуникаций по предупреждению киберпреступлений. 4. Установление для операторов мобильной связи и провайдеров обязательства принятия ими мер, направленных на блокировку или предупреждение пользователей о ложных/подозрительных звонках, обеспечение их защиты от нежелательных звонков.	Комплекс мер Совместное постановление Проект нормативно-правового акта Проект нормативно-правового акта	Сентябрь 2026 года Октябрь 2026 года Декабрь 2027 года Декабрь 2027 года	МВД, Минцифры, СГБ, ЦРЭТ, Центральный банк

VI. Привлечение частных организаций в сфере кибербезопасности					
19.	Создание условий для вовлечения частного сектора в процессы экспертизы и сертификации в соответствии с требованиями кибербезопасности.	1. Проведение анализа реализованных зарубежными организациями проектов и программ в данном направлении. Подготовка мер по развитию частного аутсорсинга в сфере кибербезопасности на основе результатов анализа. 2. Разработка проекта нормативно-правового акта, регулирующего процессы участия частного сектора и аутсорсинговых организаций в обеспечении кибербезопасности государственных информационных систем и объектов КИИ.	Аналитическая справка Проект нормативно-правового акта	Август 2026 года Январь 2027 года	СГБ, Минцифры, заинтересованные министерства и ведомства СГБ, Минцифры
20.	Установление требований обеспечения кибербезопасности, предъявляемых к облачным услугам, используемым при формировании или размещении информационных систем, ресурсов и других объектов информатизации государственных органов и организаций.	1. Проведение инвентаризации действующих нормативно-правовых актов по облачным услугам. 2. Выявление правовых пробелов и проблем, связанных с регулированием в данном направлении. 3. Разработка требований по обеспечению кибербезопасности для облачных услуг.	Аналитическая справка Проект нормативно-правового акта	Август 2026 года Декабрь 2026 года	СГБ, Минцифры, ЦРЭТ, Центральный банк
21.	Установление контроля за соблюдением требований кибербезопасности организациями, предоставляющими аутсорсинговые и облачные услуги.	1. Анализ проектов и программ, реализованных организациями по направлению оказания аутсорсинговых и облачных услуг.	Аналитическая справка	Март 2027 года	СГБ, Минцифры, Центральный банк

		2. Изучение зарубежного опыта и подготовка предложений по контролю за соблюдением требований кибербезопасности организациями, предоставляющими аутсорсинговые и облачные услуги. 3. Подготовка проекта нормативно-правового акта по контролю организаций, предоставляющих аутсорсинговые и облачные услуги.	Проект нормативно-правового акта	Июнь 2027 года	
22.	Создание платформ сотрудничества и взаимодействия государственных органов и частных организаций в сфере кибербезопасности, в частности интернет-платформ и форумов, платформ тестирования технологий кибербезопасности и других.	1. Определение нормативно-правовых пробелов и проблем, связанных с налаживанием сотрудничества между государственными органами и частными организациями в сфере кибербезопасности. 2. Разработка программы платформы сотрудничества и взаимодействия государственных органов и частных организаций в сфере кибербезопасности с учетом зарубежного опыта и интересов частного сектора. 3. Реализация программы платформы сотрудничества и взаимодействия государственных органов и частных организаций в сфере кибербезопасности.	Программа мероприятий Создание цифровых услуг и платформ	Октябрь 2026 года Декабрь 2028 года	СГБ, Минобороны, МВД, МЧС, ГСБП, Нацгвардия, Минцифры, заинтересованные министерства и ведомства
VII. Развитие кадрового потенциала и повышение квалификации работников в сфере кибербезопасности, а также уровня правовой и цифровой культуры кибербезопасности (киберграмотности) населения					
23.	Организация уроков по кибергигиене по обучению базовым знаниям	1. Изучение передового зарубежного опыта в данном направлении.	Аналитическая справка	Август 2026 года	СГБ, Минцифры, Министерство высшего

	безопасных действий в сети интернет в рамках воспитательных часов для учащихся старших классов, а также создание платформ, предоставляющих бесплатные онлайн-курсы по основам кибербезопасности для студентов и учащихся школ.	2. Подготовка программы по созданию сервисов и платформ для обучения студентов и учащихся школ основам кибербезопасности и безопасного поведения в сети интернет с учетом зарубежного опыта.	Практические меры	Январь 2027 года	образования, науки и инноваций
24.	Создание на базе ГУП «Центр кибербезопасности» клубов кибербезопасности в регионах республики в целях поддержки талантливой молодежи в сфере кибербезопасности.	1. Обеспечение соответствующим техническим оборудованием, высокоскоростными интернет-каналами клубов кибербезопасности в Республике Каракалпакстан, областных центрах и городе Ташкенте. 2. Организация деятельности указанных клубов на республиканском уровне с привлечением молодежи. 3. Проведение и поощрение победителей конкурсов среди членов клубов в целях повышения знаний и навыков молодежи в сфере кибербезопасности.	План мер	Август 2026 года Декабрь 2026 года Ежегодно	Совет Министров Республики Каракалпакстан, хокимияты областей и города Ташкента, Минцифры, СГБ, заинтересованные министерства и ведомства
25.	Совершенствование системы подготовки кадров в сфере кибербезопасности.	1. Изучение зарубежного опыта по подготовке, распределению и целевому использованию кадров в сфере кибербезопасности и разработка соответствующих предложений. 2. Разработка предложений по повышению привлекательности осуществления деятельности в государственных структурах в сфере кибербезопасности.	Проект нормативно-правового акта	Август 2026 года	СГБ, Минцифры, Министерство высшего образования, науки и инноваций

		3. Разработка предложений о механизмах осуществления деятельности в государственных структурах выпускников высших образовательных учреждений, обучившихся по сфере кибербезопасности на основе государственного гранта. 4. Разработка проекта нормативно-правового акта по совершенствованию системы подготовки кадров в сфере кибербезопасности.			
VIII. Дальнейшее укрепление сотрудничества с международными и зарубежными структурами и организациями в сфере обеспечения кибербезопасности					
26.	Развитие совместных инициатив по борьбе с киберпреступностью в Центральной Азии. Дальнейшее укрепление сотрудничества с международными и зарубежными структурами и *организациями в сфере* кибербезопасности. В частности, развитие сотрудничества со странами ООН, СНГ, ШОС, ОТГ и ЛАГ, в рамках других международных и региональных организаций, а также привлечение международного опыта и технологий посредством стратегического партнерства.	1. По согласованию с секретариатом Совета безопасности, установление тесного сотрудничества с сопредельными государствами Центральной Азии в сфере обеспечения кибербезопасности. При этом согласовываются проведение конференции с участием представителей ответственных за кибербезопасность *ведомств государств* Центральноазиатского региона, определение рамок сотрудничества по направлениям сферы, а также мероприятия по борьбе с рисками кибербезопасности и меры реагирования на инциденты кибербезопасности в регионе. 2. Внесение предложения о создании аналитического подразделения по вопросам обеспечения кибербезопасности и противодействия киберпреступности в Международном институте Центральноазиатских исследований.	Первая конференция государств Центральноазиатского региона (в городе Ташкенте) Внесение обоснованных предложений в секретариат Совета безопасности	До 2030 года постоянно	СГБ, МВД, ГСБП, Минобороны, Минцифры, Центральный банк, Нацгвардия, МИД, МИЦАИ, заинтересованные министерства и *ведомства*

		3. Определение каналов обмена информацией о существующих киберугрозах и практиках. 4. Обмен опытом по обеспечению кибербезопасности и противодействию киберпреступлениям. 5. Участие в проводимых международных научно-практических семинарах и конференциях в сфере кибербезопасности.			
27.	Активизация сотрудничества с зарубежными государственными и частными структурами, службами кибербезопасности, включая службу CERT.	1. Расширение взаимодействия с зарубежными службами и центрами обеспечения кибербезопасности (включая Threat Intellegence Sharing, Hunting, MISP). 2. Достижение соглашений о взаимной практической помощи. 3. Участие в проводимых международных научно-практических семинарах и конференциях в сфере кибербезопасности.	Заключение соглашений (меморандумов)	До 2030 года постоянно	СГБ, Минобороны, МВД, ГСБП, Минцифры, Центральный банк, Нацгвардия, МИД, заинтересованные министерства и ведомства
28.	Участие в формировании международной системы кибербезопасности, направленной на противодействие использованию киберпространства в террористических, преступных и иных незаконных целях, подготовка и внесение национальных инициатив, соответствующих интересам страны и способствующих укреплению ее кибербезопасности.	1. Подготовка предложений по изучению международного опыта противодействия использованию киберпространства в террористических, преступных и иных незаконных целях. 2. Подготовка и продвижение национальных инициатив на международных площадках и мероприятиях, связанных с вопросами кибербезопасности.	Подготовка инициатив и участие в международных мероприятиях	До 2030 года постоянно	СГБ, Минобороны, МВД, ГСБП, Минцифры, Центральный банк, Нацгвардия, МИД, заинтересованные министерства и ведомства