

Отахонов Фозилжон

*Ўзбекистон Республикаси Олий Мажлиси ҳузуридаги Қонунчилик
муаммолари ва парламент тадқиқотлари институти директори, ю.ф.д.,
профессор*

Тўраев Акмал

*Ўзбекистон Республикаси Олий Мажлиси ҳузуридаги Қонунчилик
муаммолари ва парламент тадқиқотлари институти бош илмий ходими*

**КИБЕРХАВФСИЗЛИК ТАЪМИНЛАНИШИНING ҲУҚУҚИЙ
АСОСЛАРИ: АМАЛДАГИ ҲОЛАТ ВА ТАКОМИЛЛАШТИРИШ
МАСАЛАЛАРИ**

Отахонов Фозилжон

*Профессор, доктор юридических наук, директор Института проблем
законодательства и парламентских исследований при Олий Мажлисе
Республики Узбекистан*

Тураев Акмал

*Главный научный сотрудник Института проблем законодательства и
парламентских исследований при Олий Мажлисе Республики Узбекистан*

**ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ:
ТЕКУЩЕЕ СОСТОЯНИЕ И ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ**

Otakhonov Foziljon

*Director of The Legislation and Parliamentary Research Institute under the Oliy
Majlis of the Republic of Uzbekistan, Doctor of Law, Professor*

Turaev Akmal

*Chief research fellow in The Legislation and Parliamentary Research Institute
under the Oliy Majlis of the Republic of Uzbekistan*

**CYBERSECURITY LEGAL FRAMEWORK:
CURRENT STATE AND IMPROVEMENT ISSUES**

Аннотация. Мақолада киберхавфсизлик таъминланишида муҳим аҳамиятга эга бўлган ҳуқуқий асосларнинг амалдаги ҳолати ва такомиллаштириш масалалари таҳлил қилинган. Мазкур йўналишда амалиётда учраётган муаммолар ва қонунчилик муаммолари ўрганилиб, камчиликларни бартараф этишга қаратилган асосли таклифлар ишлаб чиқилган.

Калит сўзлар: киберхавфсизлик, молиявий зарар, киберхавфсизликни таъминлаш харажатлари, норматив-ҳуқуқий база, халқаро шартномалар, БРМ, парламент.

Аннотация. В статье проанализированы текущее состояние и вопросы совершенствования правовых основ, имеющие важное значение в обеспечении кибербезопасности. По итогам изучения практики и проблем законодательства выработаны обоснованные предложения по устранению недостатков.

Ключевые слова: кибербезопасность, финансовые потери, расходы по обеспечению кибербезопасности, нормативно-правовая база, международные договоры, ЦУР, парламент.

Abstract: The article analyzes the current state and issues of improving the legal framework that are important in ensuring cybersecurity. Based on the results of the study of the practice and problems of the legislation, reasonable proposals were developed to eliminate the shortcomings.

Keywords: cybersecurity, financial losses, cybersecurity costs, regulatory framework, international treaties, SDGs, parliament.

Информационные технологии и кибербезопасность

В век информационных технологий наряду с цифровизацией всех сфер общественной жизни, с каждым днем возрастает количество угроз кибербезопасности.

По состоянию на январь 2022 года в мире насчитывается около 4.95 млрд пользователей всемирной сети Интернет, что составляет примерно 62.5% населения мира. По данным пресс-службы Министерства по развитию информационных технологий и коммуникаций Узбекистана, число интернет-пользователей в Узбекистане по итогам 2021 года превысило 27,2 млн. По сравнению с 2020 годом подключённых к интернету стало на 23% больше (*тогда интернет-пользователей было чуть больше 22 млн*).

Сегодня многие вызовы кибербезопасности подрывают доверие к глобальной сети и мешают цифровому обществу показать весь свой потенциал. По некоторым подсчетам, в мире каждые 39 секунд совершаются кибератаки, что имеет, кроме прочего, тяжелые экономические последствия. Например, глобальные потери от киберпреступлений оцениваются в 1 трлн долларов США в 2020 году и до 6 трлн долларов США в 2021 году и, по некоторым прогнозам, к 2025 году потери составят 10.5 трлн долларов США.

Наряду с этим, также увеличиваются расходы мирового сообщества на обеспечение кибербезопасности. По некоторым оценкам эти расходы в 2021 году составили 150 млрд долларов США, а к 2025 году эти расходы могут составить 1.75 трлн долларов США.

В 2017 году была совершена так называемая «Вестминстерская утечка данных», когда была предпринята несанкционированная попытка получить доступ к аккаунтам электронной почты, принадлежащим ряду политиков в палатах парламента Соединенного Королевства.

Республика Узбекистан также не застрахована от таких угроз. Согласно отчету ГУП «Центр кибербезопасности», в ходе мониторинга информационных систем государственных органов, подключенных к межведомственной сети передачи данных (МСПД), зафиксировано 33.317.648 событий безопасности, из которых 347.742 событий могли привести к несанкционированному получению доступа и утечке конфиденциальной информации.

Правовые основы кибербезопасности

Наряду с совершенствованием технических возможностей в борьбе с киберугрозами, разработка законодательных основ играет ключевую роль в защите общества и продвижении безопасной и надежной цифровой среды и должны быть отправной точкой любых национальных усилий в области кибербезопасности.

Правовые рамки включают в себя создание законодательства, устанавливающего понятие незаконной деятельности в киберпространстве вместе с определением необходимых процессуальных инструментов для расследования и обеспечения соблюдения такого законодательства.

Законодательство является динамичным инструментом, который позволяет государству реагировать на новые социальные проблемы и проблемы безопасности. Оно обеспечивает баланс между защитой частной жизни и борьбой с преступностью, устанавливает ответственность субъектов правоотношений в области кибербезопасности.

В настоящее время Узбекистан активно развивает и поощряет внедрение цифровых технологий как в государственном, так и в частном секторе. Руководством страны и правительством ведется взвешенная политика по повсеместному внедрению ИКТ во все сферы общественной жизни.

Тому свидетельством служит включение национальной задачи по существенному расширению доступа к ИКТ и стремлению к обеспечению всеобщего и недорогого доступа к сети Интернет (задача 9.с) в Национальные цели и задачи в области устойчивого развития на период до 2030 года, утвержденные постановлением Кабинета Министров от 21 февраля 2022 года №83.

Правовые нормы по вопросам обеспечения кибербезопасности частично реализованы в законодательстве Республики Узбекистан. На сегодняшний день данная сфера регулируется отдельными подзаконными актами, такими как Постановление Президента Республики Узбекистан от 21 ноября 2018 г. № ПП–4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты»; Постановление Президента Республики Узбекистан от 14 сентября 2019 г. № ПП–4452 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты»; Указ Президента

Республики Узбекистан от 15 июня 2020 г. №УП-6007 «О мерах по внедрению Государственной системы защиты информационных систем и ресурсов Республики Узбекистан»; Постановление Президента Республики Узбекистан от 15 июня 2020 г. №ПП-4751 «О мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан»; Постановление Кабинета Министров Республики Узбекистан от 5 сентября 2018 г. № 707 «О мерах по совершенствованию информационной безопасности во всемирной информационной сети Интернет» и ряд других актов правительства и ведомств.

Кроме того, законами «О телекоммуникациях», «Об информатизации», «О персональных данных» регулируется деятельность органов, ответственных за реализацию государственной политики в области информационной безопасности. Однако полноценным, непосредственно направленным на урегулирование общественных отношений в сфере кибербезопасности стал Закон Республики **Узбекистан от 15 апреля 2022 г. №ЗРУ-764 «О кибербезопасности».**

Закон направлен на регулирование отношений в сфере обеспечения безопасности в киберпространстве Республики Узбекистан, установление требований по обеспечению кибербезопасности информационных систем и ресурсов государственных органов и организаций, реагирование на кибератаки и обеспечение эффективной работы CERT (Центров реагирования на компьютерные инциденты), а также на создание эффективной правовой базы для поощрения и дальнейшего развития отечественной индустрии кибербезопасности: принятие мер государственной поддержки, обучение специалистов по кибербезопасности.

При разработке законопроекта был тщательно проанализирован опыт зарубежных стран в этом направлении, что послужило включению в Закон нижеследующих норм:

первое, основные принципы обеспечения кибербезопасности;

второе, полномочия, права и обязанности уполномоченного государственного органа в сфере обеспечения кибербезопасности;

третье, требования по обеспечению кибербезопасности информационных систем и ресурсов государственных органов и организаций;

четвертое, меры реагирования на инциденты кибербезопасности;

пятое, формирование нормативно-правовой базы по уровню значимости критических информационных инфраструктур;

шестое, создание благоприятных условий и стимулирование национальных проектов и кадров в сфере обеспечения кибербезопасности.

Закон позволит усовершенствовать систему государственного регулирования в сфере кибербезопасности, правового, организационного, научно-технического обеспечения кибербезопасности, содействует целостности информационных систем и ресурсов, их защите от несанкционированных действий (уничтожения, изменения, подделки, копирования, блокировки) и послужит предотвращению киберугроз.

Международное сотрудничество Узбекистана в области кибербезопасности

Помимо национального законодательства, нормы международного права также имеют особую значимость, т.к. они охватывают отношения между государствами во всех их бесчисленных формах. Положения как национального законодательства, так и международного права имеют непосредственное отношение к кибербезопасности.

В настоящее время международное сотрудничество в области кибербезопасности находится на стадии становления: отсутствует всеобъемлющая международно-правовая база в сфере киберпространства.

Одним из самых универсальных многосторонних договоров, касающихся преступной деятельности в сфере информационных технологий, является Конвенция о преступности в сфере компьютерной информации, принятая 23 ноября 2001 г. в Будапеште. Конвенция направлена на гармонизацию материального и процессуального уголовного законодательства по борьбе с киберпреступностью, содействие взаимной правовой помощи, а также на обеспечение правовой базы для содействия развитию и пониманию вопросов, связанных с киберпреступностью.

Узбекистан не является участником Конвенции, в которой имеются некоторые спорные положения. Например, пункт b ст. 32 Конвенции предусматривает возможность для государства-участника получить трансграничный доступ к информации, источник которой находится в другом государстве без уведомления компетентных органов государства, в котором находится источник информации.

Кроме вышеназванной Конвенции имеется также ряд резолюций ГА ООН: Резолюция (A/RES/53/70) от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», Резолюция (A/RES/64/211) от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» и прочие. Эти и другие резолюции ГА ООН призывают государства к сотрудничеству в сфере информационной безопасности, разработке международных принципов обеспечения безопасности глобальных информационных систем.

В СНГ в сфере обеспечения информационной безопасности были приняты «Соглашение об информационном взаимодействии государств-участников СНГ в области цифрового развития общества», «Стратегия обеспечения информационной безопасности государств-участников СНГ», «Соглашение о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности». На этих документах базируется сотрудничество государств СНГ в сфере обеспечения информационной безопасности на двустороннем, региональном и международном уровнях.

29 июня 2021 года в Ташкенте состоялся Международный экспертный форум СНГ по вопросам обеспечения информационной безопасности, который был проведен по инициативе Президента Узбекистана Шавката Мирзиёева, выдвинутой на прошедшем под его председательством в онлайн-режиме саммите государств Содружества 18 декабря 2020 года.

Особое внимание уделяется также сотрудничеству в сфере кибербезопасности в рамках ШОС. Этот вопрос был акцентирован Президентом Шавкатом Мирзиёевым в книге «Стратегия Нового Узбекистана», где сотрудничество с ШОС, в том числе в сфере кибербезопасности, отмечается как направление особой значимости.

Вышеприведенное доказывает готовность руководства страны к дальнейшему расширению сотрудничества в сфере обеспечения информационной безопасности.

Парламент и кибербезопасность

В вопросе обеспечения кибербезопасности национальные парламенты играют ключевую роль по следующим основаниям.

Во-первых, парламенты принимают законы, которые определяют основные направления государственной политики в сфере кибербезопасности, назначают ответственных за безопасность киберпространства, устанавливают меры ответственности за нарушение кибербезопасности.

Во-вторых, одним из основных направлений деятельности парламентов является осуществлений действенного парламентского контроля за деятельностью государственных органов, органов хозяйственного управления и их должностных лиц по исполнению законов Республики Узбекистан, решений палат Олий Мажлиса Республики Узбекистан, государственных программ в сфере кибербезопасности, а также по реализации возложенных на них задач и функций.

В-третьих, парламенты играют ключевую роль в выстраивании международного сотрудничества в сфере кибербезопасности, в том числе путем ратификации и денонсации международных договоров в области обеспечения кибербезопасности.

Сегодня Олий Мажлисом принимаются комплексные меры по обеспечению защиты и безопасности цифровых данных: приняты законы Республики Узбекистан «Об информатизации», «О персональных данных», «Об электронном правительстве», «О кибербезопасности», активизировалась работа по установлению действенного парламентского контроля над правительством.

Однако анализ сложившейся в мире ситуации вокруг обеспечения информационной безопасности, позволяют сформулировать следующие выводы касательно повышения роли парламента в данном направлении.

Во-первых, с каждым днем появляются все новые и новые способы и средства совершения киберпреступлений. Это, в свою очередь, требует от парламентариев постоянного повышения знаний и осведомленности о

новых цифровых технологиях, чтобы законодательство соответствовало новым реалиям. Кроме того, парламентариям следует усилить работу по систематическому мониторингу действующего законодательства в сфере кибербезопасности и принимать меры по его совершенствованию.

Во-вторых, следует усилить парламентский контроль над деятельностью государственных органов и их должностных лиц по исполнению законов Республики Узбекистан, решений палат Олий Мажлиса Республики Узбекистан, государственных программ и стратегий в сфере кибербезопасности, а также по реализации возложенных на них задач и функций.

В-третьих, способствовать защите конституционных прав и свобод граждан в информационных системах и сети Интернет, в том числе защите прав частной собственности, защите информационно-коммуникационной инфраструктуры от внешнего вмешательства, распространения недостоверной и деструктивной информации в цифровом пространстве посредством имплементации международных договоров в сфере кибербезопасности.

Таким образом, построение эффективной нормативно-правовой базы окажет превентивное воздействие на киберугрозы, а потому обеспечение национальной кибербезопасности напрямую зависит от наличия действенных правовых механизмов, внедряемых, в первую очередь, национальным парламентом.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Ш.М. Мирзиёев. “Янги Ўзбекистон стратегияси”. Т., Издательство “O‘zbekiston”. 2021. – С. 464.
2. Закон Республики Узбекистан от 15 апреля 2022 г. №ЗРУ-764 «О кибербезопасности». [Электронный ресурс] – Режим доступа: <https://xs.uz/ru/site/download?id=2193> – Дата доступа: 16.04.2022 г.
3. Закон Республики Узбекистан от 20 августа 1999 г. №822-I «О телекоммуникациях». [Электронный ресурс] – Режим доступа: <https://lex.uz/acts/33152> – Дата доступа: 15.04.2022 г.
4. Закон Республики Узбекистан от 20 августа 1999 г. №822-I «О телекоммуникациях». [Электронный ресурс] – Режим доступа: <https://lex.uz/acts/33152> – Дата доступа: 15.04.2022 г.
5. Закон Республики Узбекистан от 11 декабря 2003 г. №560-II «Об информатизации». [Электронный ресурс] – Режим доступа: <https://lex.uz/acts/82956> – Дата доступа: 15.04.2022 г.
6. Закон Республики Узбекистан от 2 июля 2019 г. №ЗРУ-547 «О персональных данных». [Электронный ресурс] – Режим доступа: <https://lex.uz/docs/4396428> – Дата доступа: 15.04.2022 г.
7. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). [Электронный ресурс] – Режим доступа: <https://base.garant.ru/4089723/> – Дата доступа: 15.04.2022 г.

8. Тексты резолюций ГА ООН. [Электронный ресурс] – Режим доступа: <https://www.un.org/ru/development/ict/res.shtml> – Дата доступа: 15.04.2022 г.

9. SIMON KEMP: Digital 2022: global overview report. [Электронный ресурс] – Режим доступа: <https://datareportal.com/reports/digital-2022-global-overview-report> – Дата доступа: 14.04.2022 г.

10. Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги томонидан 2021 йилда олиб борилган ишлар таҳлили. [Электронный ресурс] – Режим доступа: <https://telegra.ph/Ahborot-tehnologiyalari-va-kommunikatsiyalarini-rivozhlantirish-vazirligi-tomonidan-2021-jilda-olib-borilgan-ishlar-taxlili-01-10> – Дата доступа: 15.04.2022 г.

11. Hackers attack every 39 seconds. [Электронный ресурс] – Режим доступа: <https://www.nbcnews.com/id/wbna17034719> – Дата доступа: 15.04.2022 г.

12. Zhanna Malekos Smith and Eugenia Lostri James A. Lewis. The Hidden Costs of Cybercrime. [Электронный ресурс] – Режим доступа: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf> – Дата доступа: 15.04.2022 г.

13. Cybercrime To Cost the World \$10.5 Trillion Annually By 2025. [Электронный ресурс] – Режим доступа: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> – Дата доступа: 15.04.2022 г.

14. 2022 cybersecurity spending trends. [Электронный ресурс] – Режим доступа: <https://www.cuinsight.com/2022-cybersecurity-spending-trends/> – Дата доступа: 15.04.2022 г.

15. Cyber-attack on parliament leaves MPs unable to access emails. [Электронный ресурс] – Режим доступа: <https://www.theguardian.com/politics/2017/jun/24/cyber-attack-parliament-email-access> – Дата доступа: 15.04.2022 г.

16. Обеспечение кибербезопасности в Республике Узбекистан. [Электронный ресурс] – Режим доступа: <https://www.csec.uz/upload/iblock/906/1.%20Итоги%202021%20ру.pdf> – Дата доступа: 15.04.2022 г.

17. Данельян А.А. Международно-правовое регулирование киберпространства. [Электронный ресурс] – Режим доступа: <https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-kiberprostranstva/viewer> – Дата доступа: 15.04.2022 г.