

Ключевые положения Закона «О  
кибербезопасности»  
от 15 апреля 2022 года

Июнь 2022



## Наша команда (1/2)



**Динара Танашева**

Партнер, Руководитель практики налоговых и юридических услуг по Казахстану и Центральной Азии

Тел.: +7 (727) 258 5960

E-mail: Dinara.Tanasheva@kz.ey.com

- ▶ Динара является Руководителем практики налоговых и юридических услуг компании EY в Казахстане и Центральной Азии.
- ▶ Является активным участником следующих рабочих групп:
  - ▶ Рабочая группа по цифровизации Совета иностранных инвесторов при Президенте Республики Казахстан;
  - ▶ Рабочая группа Американской торговой палаты в Казахстане (АТП) по Иностранным Инвестициям, Технологиям и Инновациям;
  - ▶ Рабочая группа Комитета ЕВРОБАК по цифровизации;
  - ▶ Рабочая группа по вопросам трудового законодательства, развития человеческого капитала и привлечения иностранной рабочей силы Совета иностранных инвесторов под председательством Президента РК, а также Совета по улучшению инвестиционного климата в РК, Председателем HR комитета ЕВРОБАК.
- ▶ Динара имеет большой опыт в руководстве по подготовке изменений в казахстанское законодательство и участие в различных рабочих группах по совершенствованию казахстанского законодательства, в том числе по внесению изменений в Трудовой кодекс, Таможенный кодекс, Налоговый кодекс, Кодекс об административных правонарушениях, Гражданский кодекс, Гражданский процессуальный кодекс, Уголовный кодекс, Кодекс «О недрах и недропользовании», Правил выдачи разрешений на работу.
- ▶ Динара участвовала и руководила проектами в сфере регулирования облачных технологий. В частности, такие проекты включали анализ законодательства РК в отношении действующих ограничений для развития cloud computing, а также в сфере персональных данных.



**Наргиз Сулейменова**

Старший юрист, Департамент налоговых и юридических услуг

Тел.: +7 (727) 258 5960

E-mail: Nargiz.Suleimenova@kz.ey.com

- ▶ Наргиз является старшим юристом департамента налоговых и юридических услуг компании EY Kazakhstan.
- ▶ Наргиз окончила Высшую школу права «Адилет». Получила степень Магистра права (LL.M.) в Китайском университете политических наук и права (CUPL).
- ▶ Наргиз является членом Палаты юридических консультантов «Kazakhstan Bar Association» и Ассоциации юристов нефтегазовой отрасли.
- ▶ Является активным участником следующих рабочих групп:
  - ▶ Рабочая группа по цифровизации Совета иностранных инвесторов при Президенте Республики Казахстан;
  - ▶ Рабочая группа Американской торговой палаты в Казахстане (АТП) по Иностранным Инвестициям, Технологиям и Инновациям;
  - ▶ Рабочая группа Комитета ЕВРОБАК по цифровизации;
- ▶ Наргиз выступала по следующим темам:
  - ▶ Площадка ЕВРОБАК (2 июня 2021 года): Планируемые изменения и дополнения в законодательство по вопросам защиты персональных данных;
  - ▶ Площадка АТП (28 сентября 2021 года): Облачные службы (сервисы) в контексте законодательства Республики Казахстан;
  - ▶ Площадка АТП (21 декабря 2021 года): Цифровизация госсектора: GovTech;
  - ▶ Площадка ЕВРОБАК (21 декабря 2021 года): Электронный документооборот: правовое регулирование и практика.

## Наша команда (2/2)



Маржона Хафизова

Юриисконсульт, Департамент налоговых и юридических услуг

Тел.: + 998 78 140 6482

E-mail: Marjona.Khafizova@uz.ey.com

- ▶ Маржона является консультантом юридической практики EY в Узбекистане
- ▶ Маржона имеет диплом с отличием Международного Вестминстерского Университета в Ташкенте по специальности коммерческое право.
- ▶ Работает в Ташкентском офисе компании EY с августа 2019 года.
- ▶ Маржона имеет опыт в предоставлении юридических консультационных услуг по различным сферам законодательства Узбекистана, в том числе корпоративное, трудовое, валютное, фармацевтическое законодательство.
- ▶ Маржона участвовала в проектах связанными с последними изменениями в сфере персональных данных в Узбекистане.
- ▶ Маржона участвует в проектах по юридическому консультированию как отечественных, так и международных компаний в различных областях законодательства, включая корпоративное, трудовое, антимонопольное валютное, хозяйственное законодательство и т.д.
- ▶ Маржона участвует в анализе и изучении изменений в законодательстве Узбекистана, а также применение на практике для узбекских и иностранных предприятий.



Адилет Сагиев

Старший юриисконсульт, Департамент налоговых и юридических услуг

Тел.: +7 727 2585960

E-mail: Adilet.Sagiyev@kz.ey.com

- ▶ Адилет является старшим юриисконсультот практики налоговых и юридических услуг компании EY в Казахстане.
- ▶ Является активным участником следующих рабочих групп:
  - ▶ Рабочая группа по цифровизации Совета иностранных инвесторов при Президенте Республики Казахстан;
  - ▶ Рабочая группа Американской торговой палаты в Казахстане (АТП) по Иностранным Инвестициям, Технологиям и Инновациям;
  - ▶ Рабочая группа Комитета ЕВРОБАК по цифровизации.
- ▶ Адилет имеет опыт в проектах в сфере персональных данных, регулирования облачных технологий. В частности, такие проекты включали анализ законодательства РК в отношении действующих ограничений для развития облачных сервисов.
- ▶ Адилет также имеет опыт сопровождения деятельности Российской платформы электронной коммерции на территории РК, включающий вопросы персональных данных, обработки платежных карт с точки зрения законодательства РК.

## Содержание

I.	Используемые сокращения	5
II.	Закон «О кибербезопасности»: цели и принципы	6
III.	Полномочия государственных органов в сфере кибербезопасности	7
IV.	Права СГБ	9
V.	Права и обязанности субъекта кибербезопасности	10
VI.	Механизмы обеспечения кибербезопасности	11
VII.	ОКИИ	13
VIII.	Основные положения в отношении ОКИИ	14
IX.	Преступления в сфере ИТ	15

## Используемые сокращения

ГО	Государственные органы
РУз	Республика Узбекистан
Закон «О кибербезопасности»	Закон РУз «О кибербезопасности» № ЗРУ-764 от 15 апреля 2022
СГБ	Служба Государственной Безопасности
УК РУз	Уголовный Кодекс Республики Узбекистан (Утвержден Законом РУз от 22.09.1994 г. N 2012-II)
НПА	Нормативные правовые акты
ИС	Информационные системы
ИТ	Информационные технологии
ИКТ	Информационно-коммуникационные технологии
КИИ	Критическая информационная инфраструктура
ОКИИ	Объекты критической информационной инфраструктуры
СКИИ	Субъекты критической информационной инфраструктуры

# Закон «О кибербезопасности»: цели и принципы

## Дата / статус:

25 февраля 2022 года - принят Законодательной палатой

17 марта 2022 года - одобрен Сенатом

15 апреля 2022 года - подписан Президентом

17 июля 2022 - вступает в силу

## Цель Закона:

регулирование отношения в сфере кибербезопасности

## Кибербезопасность:

состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве

## Основные принципы обеспечения кибербезопасности:

- законность
- приоритет защиты интересов личности, общества и государства в кибербезопасности
- единый подход к регулированию сферы кибербезопасности
- приоритет участия отечественных производителей в создании системы кибербезопасности
- Открытость РУз к международному сотрудничеству в обеспечении кибербезопасности

# Полномочия государственных органов в сфере кибербезопасности (1/2)

## Органы управления

Президент РУз

СГБ

## Полномочия

- Определяет единую государственную политику в сфере кибербезопасности
- Разработка НПА и государственных программ
- Проведение оперативно-розыскных мероприятий, доследственных проверок и следственных действий по инцидентам кибербезопасности
- Предупреждение, выявление и предотвращение инцидентов кибербезопасности и принятие по ним соответствующих мер, в том числе организационно-технических мер по устранению их последствий
- Организация работ по сертификации аппаратных, аппаратно-программных и программных средств в ИС и ресурсах в соответствии с требованиями кибербезопасности
- Формирование единого реестра ОКИИ, а также организация и обеспечение его ведения
- Принятие решения о включении объектов в единый реестр ОКИИ на основе сведений, представленных субъектами кибербезопасности
- Определение порядка проведения аттестации объектов информатизации и ОКИИ в соответствии с требованиями кибербезопасности
- Лицензирование деятельности по разработке, производству и реализации средств криптографической защиты информации

## Полномочия государственных органов в сфере кибербезопасности (2/2)

*(Продолжение)*

### Органы управления

СГБ

*(продолжение)*

### Полномочия

- Регулирование деятельности подразделений кибербезопасности, служб и групп независимых экспертов, взаимодействие с правоохранительными органами в сфере противодействия киберугрозам
- Создание классификатора по уровню обеспеченности кибербезопасности в ИС и ресурсах
- Определение механизмов проведения экспертизы на соответствие требованиям кибербезопасности
- Определение методов оценки и оценка осуществления кибербезопасности объектов кибербезопасности и ОКИИ;
- Определение критериев категорирования и категорирование ОКИИ



## Права СГБ

---

### СГБ при осуществлении полномочий, перечисленных выше, вправе, помимо прочего:

- безвозмездно пользоваться техническими установками и услугами для принятия безотлагательных мер по устранению кибератак
- посещать государственные органы и иные организации, знакомиться с необходимыми документами и материалами, а также запрашивать и получать от государственных органов и иных организаций, граждан сведения и другие необходимые документы и материалы, проводить их идентификацию и использовать в следственных действиях по инцидентам кибербезопасности
- беспрепятственный доступ и подключение в установленном порядке к ИС и ресурсам государственных органов и организаций, ОКИИ, а также изучение данных в части внедрения и эксплуатации средств обеспечения кибербезопасности информационных систем и ресурсов этих объектов
- входить беспрепятственно, при необходимости с повреждением запирающих устройств и других предметов, в жилые помещения и иные объекты физических и юридических лиц, осматривать их при преследовании лиц, подозреваемых в совершении преступлений в сфере ИТ, либо при наличии достаточных оснований полагать, что там совершается или совершено такое преступление, или находится лицо, скрывшееся от правоохранительных органов, либо если промедление может поставить под угрозу жизнь и здоровье граждан, с последующим сообщением об этом прокурору в течение 24 часов, а также с возмещением причиненного вреда в порядке, установленном законодательством

## Права и обязанности субъекта кибербезопасности (ст. 16)

### Субъекты вправе:

1. получать от СГБ сведения о киберугрозах, уязвимостях программного обеспечения, оборудовании и технологиях в целях обеспечения своей кибербезопасности
2. получать сведения и консультации СГБ о средствах и методах защиты от кибератак, а также методах их выявления и предотвращения
3. разрабатывать и реализовывать меры по обеспечению своей кибербезопасности

### Субъекты обязаны, помимо прочего:

1. предотвращать незаконное распространение, хищение, утерю, нарушение целостности, блокировку и фальсификацию данных, а также иные виды несанкционированного доступа, принимать своевременные соответствующие меры
2. уведомлять СГБ о произошедших инцидентах кибербезопасности и киберпреступлениях, принимать меры по недопущению утери соответствующих цифровых следов, а также обеспечивать постоянное хранение сведений, необходимых для анализа инцидентов кибербезопасности и расследования киберпреступлений
3. осуществлять взаимный обмен с СГБ данными
4. обеспечивать функционирование механизмов принятия мер в отношении инцидентов кибербезопасности и работу подразделений по обеспечению кибербезопасности
5. обеспечить хранения данных ИС и ресурсов в соответствии с внутренней политикой ИС путем создания резервной копии данных, на срок менее 3 последних месяцев
6. предоставлять СГБ право доступа в мониторинговые системы и (или) объекты кибербезопасности

## Механизмы обеспечения кибербезопасности (1/2)

№	Механизм обеспечения кибербезопасности	Описание	Статус НПА
1.	Классификация объектов кибербезопасности (ст. 17)	Определение уровня организационно-технической сложности типа объектов кибербезопасности. Категории объектов кибербезопасности, подлежащие классификации, определяются в соответствии с законодательством.	На дату настоящей презентации НПА не утвержден
2.	Экспертиза на соответствие требованиям кибербезопасности (ст. 18)	Экспертиза может быть в обязательном порядке или по инициативе субъектов кибербезопасности. Экспертизе в обязательном порядке подлежат: (i) информационные ресурсы ГО, (ii) ИС ГО, (iii) ИС, включенные в категорию ОКИИ. Порядок проведения экспертизы определяется СГБ.	На дату настоящей презентации НПА не утвержден
3.	Сертификация аппаратных, аппаратно-программных и программных средств, применяемых для обеспечения кибербезопасности ИС и ресурсов (ст. 19)	Сертификация осуществляется в обязательном порядке. Порядок проведения сертификации определяется СГБ.	На дату настоящей презентации НПА не утвержден

## Механизмы обеспечения кибербезопасности (2/2)

№	Механизм обеспечения кибербезопасности	Описание	Статус НПА
4.	Аттестация объектов информатизации и объектов критической информационной инфраструктуры (ст. 20)	Аттестацией объектов информатизации и ОКИИ является комплекс организационно-технических мероприятий, направленных на определение соответствия фактического состояния защищенности объектов информатизации требованиям государственных стандартов и НПА в сфере кибербезопасности. Категории объектов информатизации и ОКИИ, подлежащих аттестации, определяются в соответствии с законодательством. Порядок проведения аттестации определяется СГБ.	<i>На дату настоящей презентации НПА не утвержден</i>
5.	Оценка уровня обеспечения кибербезопасности (ст. 21)	Оценкой уровня обеспечения кибербезопасности является комплекс организационно-технических мероприятий, направленных на определение состояния защищенности ИС и ресурсов, а также эффективности принимаемых организационных мер. Категории объектов информатизации и ОКИИ, подлежащих обязательной оценке, определяются в соответствии с законодательством. Оценка уровня обеспечения кибербезопасности определяется СГБ.	<i>На дату настоящей презентации НПА не утвержден</i>

## ОКИИ

В соответствии с Законом «О кибербезопасности» к ОКИИ относятся системы информатизации, применяемые в следующих сферах:

1. в сфере государственного управления и оказания государственных услуг
2. обороны
3. обеспечения государственной безопасности и правопорядка
4. топливно-энергетического комплекса (атомной энергетики)
5. химической, нефтехимической отраслях
6. металлургии
7. водопользования и водоснабжения
8. сельского хозяйства
9. здравоохранения
10. жилищно-коммунального обслуживания
11. банковско-финансовой системы
12. транспорта
13. ИКТ
14. экологии и охраны окружающей среды, добычи и переработки полезных ископаемых стратегического значения
15. производственной сфере; а также
16. в других отраслях экономики и социальной сфере

## Основные положения в отношении ОКИИ

- i. **ОКИИ подразделяются на следующие категории:** *Критерии категорирования ОКИИ определяется СГБ*
- ОКИИ высокого уровня
  - ОКИИ среднего уровня
  - ОКИИ низкого уровня
- (На дату настоящего документа данные критерии не утверждены)*
- ii. **СГБ ведет единый реестр ОКИИ.** На дату настоящей презентации НПА в отношении категории ОКИИ, подлежащих обязательному внесению в единый реестр, а также порядок внесения не утверждены.
- iii. **Субъекты критической информационной инфраструктуры, помимо прочего, обязаны:**
- Доводить до сведения СГБ информацию об инцидентах кибербезопасности
  - Предоставлять СГБ права доступа в мониторинговые системы или на ОКИИ для осуществления организационно-технических мероприятий мониторинга состояния обеспечения кибербезопасности
  - Уведомлять СГБ при изменении сведений об объекте, включенном в единый реестр ОКИИ
  - Обеспечивать безопасность ОКИИ в соответствии с требованиями кибербезопасности

EY | Assurance | Tax | Transactions | Advisory

EY является мировым лидером в области предоставления гарантий, налоговых, транзакционных и консультационных услуг. Знания и качественные услуги, которые мы предоставляем, помогают укрепить доверие и уверенность на рынках капитала и в экономиках по всему миру. Мы развиваем выдающихся лидеров, которые объединяются в команду, чтобы выполнить наши обещания всем нашим заинтересованным сторонам. При этом мы играем решающую роль в создании лучшего рабочего мира для наших сотрудников, для наших клиентов и для наших сообществ.

EY сотрудничает с компаниями по всему СНГ и помогает им в реализации их бизнес-целей. 5500 специалистов работают в 19 офисах СНГ (в Москве, Екатеринбурге, Казани, Краснодаре, Новосибирске, Ростове-на-Дону, Санкт-Петербурге, Тольятти, Владивостоке, Алматы, Атырау, Нур-Султане, Баку, Бишкеке, Киеве, Минске, Ташкенте, Тбилиси, Ереване).

EY относится к глобальной организации и может относиться к одной или нескольким фирмам-членам Ernst & Young Global Limited, каждая из которых является отдельным юридическим лицом. Ernst & Young Global Limited, британская компания, ограниченная гарантией, не предоставляет услуги клиентам. Для получения дополнительной информации о нашей организации, пожалуйста, посетите [ey.com](http://ey.com).

Этот пресс-релиз был выпущен компанией EYGM Limited, членом глобальной организации EY, которая также не предоставляет никаких услуг клиентам.

© 2022 Аудиторская организация ООО "Эрнст энд Янг"/СП ООО "Эрнст энд Янг Консалтинг", Узбекистан.

Все права защищены.

[www.ey.com/en\\_uz](http://www.ey.com/en_uz)