Перевод

# ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОЛДОВА

## ПОСТАНОВЛЕНИЕ № 111

**от 7 марта 2023 г.**

**Кишинэу**

**О проекте закона**
**о кибернетической безопасности**

---

Правительство ПОСТАНОВЛЯЕТ:

Одобрить и представить Парламенту на рассмотрение проект закона о кибернетической безопасности.

**Премьер-министр** **ДОРИН РЕЧАН**

Контрасигнуют:

Заместитель Премьер-министра,
министр экономического
развития и цифровизации — Думитру АЛАЙБА

Министр финансов — Вероника Сирецяну

Министр юстиции — Вероника Михайлов-Морару

**UE**
*Проект*
*Перевод*

# ПАРЛАМЕНТ РЕСПУБЛИКИ МОЛДОВА

## ЗАКОН
## о кибернетической безопасности

Парламент утверждает настоящий органический закон.

Настоящий закон перелагает статью 1; статью 2; части (1)–(3) статьи 3; части (1) и (2) статьи 4; части (1)–(17) статьи 6; части (1)–(5) статьи 8; части (1)–(4) статьи 9; части (1)–(4) статьи 10; пункты (a)–(f) части (1) статьи 11, пункты (a)–(e), (g), (h) части (3); часть (1) статьи 12; статью 20; части (2) и (3) статьи 21; части (1)–(3), пункты (a), (b), (d) и (e) части (4) статьи 23; часть (1) статьи 24; часть (1) статьи 25; пункты (a) и (b) части (1), части (2)–(4) статьи 29; пункты (a) и (b) части (1), часть 2 статьи 30; часть (1) статьи 31; часть (1)–(8) статьи 32; части (1)–(5) статьи 33; статью 34; часть (1) статьи 35; статью 36 Директивы (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению общего высокого уровня кибербезопасности в Союзе, вносящих поправки в Регламент (ЕС) № 910/2014 и Директиву (ЕС) 2018/1972 и отменяющих Директиву (ЕС) 2016/1148 (Директива NIS 2), опубликованной в Официальном журнале Европейского Союза, серия L № 333 от 27 декабря 2022 года.

## Глава I
## ОСНОВНЫЕ ПОЛОЖЕНИЯ

**Статья 1. Объект регулирования закона**

Настоящий закон регулирует правовые, организационные рамки и рамки сотрудничества в области кибербезопасности, устанавливает компетенцию органов государственной власти и публичных учреждений в области кибербезопасности, определяет общенациональные рамки управления кризисами в сфере кибербезопасности, устанавливает требования, меры и механизмы для обеспечения сетевой безопасности и информационных систем, которые имеют решающее значение для функционирования общества, а также для управления киберинцидентами.

**Статья 2. Основные понятия и их определение:**

Для целей настоящего закона следующие понятия означают:

*кибернетическая угроза* – любое обстоятельство, событие или потенциальное действие, способное нанести ущерб или нарушить работу сетей или информационных систем, а также пользователей таких систем и других лиц, или иным образом оказать на них негативное влияние;

*значительная киберугроза* – киберугроза, о которой можно предположить, исходя из ее технических характеристик, что она способна серьезно повлиять на сети и информационные системы юридического лица, оказывающего услуги, или пользователей оказываемых им услуг, причинив материальный ущерб или значительный моральный ущерб;

*скоординированное раскрытие уязвимостей* – структурированный процесс, посредством которого информация об уязвимостях передается производителю или поставщику потенциально уязвимых ИКТ-продуктов или ИКТ-услуг таким образом, который позволяет ему диагностировать и устранить уязвимость до того, как будет опубликована подробная информация об уязвимости для раскрытия третьим лицам или общественности;

*поставщик услуг* – юридическое лицо публичного или частного права, зарегистрированное в Республике Молдова, которое предоставляет услуги в одном или нескольких секторах и/или подсекторах, установленных Правительством, и которое идентифицируется компетентным органом в соответствии с положениями настоящего закона и нормативной базаы, утвержденной для его реализации;

*управление киберинцидентом* – все действия и процедуры, направленные на предотвращение, обнаружение, анализ, ограничение и изоляцию киберинцидента, либо направленные на реагирование и восстановление после этого инцидента;

*кибернетический инцидент* – любое событие, которое ставит под угрозу доступность, подлинность, целостность или конфиденциальность данных, хранящихся, передаваемых или обрабатываемых, или связанных с ними услуг, предлагаемых сетями и информационными системами или доступных через них;

*предельно предотвращенный киберинцидент* – событие, которое могло поставить под угрозу доступность, подлинность, целостность или конфиденциальность хранимых, передаваемых или обрабатываемых данных или услуг, предоставляемых сетями и информационными системами или доступных через них, но которое было успешно предотвращено от материализации или которое не материализовалось;

*меры безопасности* – операции и/или организационные, физические и информационные технологические ресурсы, применяемые для достижения и поддержания безопасности сетей и информационных систем и данных, обрабатываемых через них;

*процесс информационно-коммуникационных технологий (процесс ИКТ)* – совокупность действий, осуществляемых для проектирования, разработки, предоставления или обслуживания продукта или услуги ИКТ;

*продукт информационно-коммуникационных технологий (продукт ИКТ)* – элемент или группа элементов сети или информационной системы;

*сеть и информационная система:*

a) сеть электронной связи в соответствии с Законом об электронных коммуникациях №. 241/2007 или

b) любое устройство или группа взаимосвязанных или связанных устройств, одно или несколько из которых выполняют в соответствии с программой автоматическую цифровую обработку данных или

c) цифровые данные, хранящиеся, обрабатываемые, восстанавливаемые или передаваемые элементами, предусмотренными в п. a) и b) ввиду управления, использования, защиты и хранения таких данных.

*риск* – потенциальные потери или сбои, вызванные киберинцидентом, и которые должны быть выражены как комбинация величины таких потерь или сбоев и вероятности возникновения киберинцидентов;

*кибернетическая безопасность* – действия, необходимые для защиты сетей и информационных систем, пользователей таких систем и других лиц, пострадавших от киберугроз;

*безопасность сетей и информационных систем* – способность сети и информационной системы выдерживать с заданным уровнем достоверности любое действие, которое ставит под угрозу доступность, подлинность, целостность или конфиденциальность данных, хранимых, передаваемых или обрабатываемых, или услуг, предоставляемых сетью или соответствующими информационными системами или доступных через них;

*услуга информационно-коммуникационных технологий (услуга ИКТ)* – услуга, полностью или преимущественно заключающаяся в передаче, хранении, извлечении или обработке информации посредством сетей и информационных систем;

*уязвимость* – слабое место, восприимчивость или недостаток в продуктах или услугах ИКТ, которое может быть использовано киберугрозами.

**Статья 3. Область применения**

(1) Настоящий закон применяется к юридическим лицам частного права, которые квалифицируются как средние предприятия в соответствии с классификацией, установленной законодательством о малых и средних предприятиях, и к юридическим лицам частного права, которые превышают предельные значения для средних предприятий, предоставляющих услуги в одном или нескольких секторах или подотраслях, установленных Правительством, и которые

идентифицированы как поставщики услуг компетентным органом, назначенным в соответствии со статьей 7, в соответствии с положениями настоящего закона и подзаконными нормативными актами.

(2) Независимо от их размера, настоящий закон применяется и к юридическим лицам, определенных Правительством, если они соотвествуют хотя бы одному из следующих условий:

a) являются поставщиками сетей электронной связи общего пользования или общедоступных услуг электронной связи согласно законодательству об электронных коммуникациях;

b) являются поставщиками доверительных услуг согласно законодательству об электронной идентификации и доверительных услугах;

c) является национальным Регистратором домена высшего уровня .md;

d) оказывает услуги по регистрации доменных имен;

e) является единственным в Республике Молдова поставщиком услуг, необходимых для поддержки критически важной общественной и экономической деятельности;

f) предоставляет услугу, зависящую от сети и/или информационной системы, сбой в работе которой может оказать существенное влияние на общественный порядок, общественную безопасность или здоровье населения или может создать значительный системный риск, особенно для секторов, где такой сбой может иметь трансграничное воздействие;

g) имеет особое значение в силу своей специфической важности на национальном или региональном уровне для рассматриваемого сектора или типа услуги или для других взаимозависимых секторов;

h) предоставляет услугу, зависящую от сети и/или информационной системы и объекта критической инфраструктуры, и идентифицируется в соответствии с национальной нормативно-правовой базой в качестве оператора такой инфраструктуры;

i) являются юридическими лицами публичного права.

(3) Данный закон не применяется:

(a) к деятельности, осуществляемой органами государственной власти в области защиты государственной тайны, в связи с обслуживанием сетей и информационных систем, предназначенных для обработки такой информации;

(b) к деятельности органов государственной власти в сфере национальной безопасности, национальной обороны, специальной следственной деятельности и уголовному преследованию в связи с обслуживанием сетей и информационных систем, предназначенных для обработки информации в этих сферах.

(4) В случае, если международными договорами, участницей которых является Республика Молдова, установлены иные нормы, чем те, которые

предусмотрены настоящим законом, применяются нормы международных договоров.

(5) Если законы, регулирующие деятельность поставщиков услуг, а также секторов и подсекторов, установленных Правительством, предусматривают выполнение мер безопасности или обязательств по уведомлению об инцидентах со значительным воздействием, последствия которых, по крайней мере, эквивалентны последствиям обязательств, установленных настоящим законом, положения соответствующих законов имеют особый характер по отношению к положениям настоящего закона.

(6) Если обязательства, предусмотренные частью (5), установленные законами, регулирующими деятельность поставщиков услуг, секторов и подотраслей, установленных Правительством, распространяются на более узкий круг юридических лиц, чем это предусмотрено настоящим Законом и нормативными актами, его реализующих, положения настоящего Закона распространяются на юридических лиц, на которых не распространяются обязанности, возлагаемые соответствующими законами.

(7) Положения частей (5) и (6) применяются компетентным органом в каждом отдельном случае в процессе идентификации поставщиков услуг в соответствии с положениями нормативного акта, установленного в части (2) статьи 4.

**Статья 4. Идентификация поставщиков услуг**

(1) Компетентный орган составляет и ведет список поставщиков услуг, который включает как минимум тип, категорию поставщика услуг, а также критический сектор и подсектор, в которых они предоставляют соответствующую услугу, и обеспечивает, когда это необходимо, но не реже, чем через каждые два года, его обновление.

(2) Правительство утверждает перечень критических отраслей и подотраслей, и, соответственно, видов и категорий юридических лиц, оказывающих услуги в этих секторах и подосекторах, устанавливает методологическую базу по идентификации юридических лиц публичного и частного права в качестве поставщиков услуг, а также способ составления, ведения и обновления списка поставщиков услуг.

(3) По запросу компетентного органа, Служба информации и безопасности предоставляет, не более чем за 30 дней с даты запроса, список операторов, которые управляют объектами критической инфраструктуры, а также любые изменения в списке, не более чем за 30 дней с даты внесения изменений.

(4) Государственные органы, ответственные за реализацию государственной политики в критических секторах или подсекторах, установленных Правительством, государственные учреждения, ответственные за управление областями, относящимися к соответствующим секторам и подсекторам, а также, при необходимости,

органы государственного регулирования этих секторов или подсекторов, оказывают необходимую поддержку компетентному органу, по его запросу, в процессе идентификации поставщиков услуг.

**Статья 5. Принципы обеспечения кибернетической безопасности**

В процессе обеспечения кибернетической безопасности, а также с целью обеспечения реализации положений настоящего Закона, ответственные лица должны действовать с учетом следующих принципов:

1) принцип индивидуальности – обеспечение безопасности сетей и информационных систем организуется поставщиками услуг;

2) принцип комплексной защиты – поставщики услуг проверяют потенциальные риски, исходящие от принадлежащих им сетей и ИТ-систем, и применяют соответствующие организационные и технические меры для их защиты;

3) принцип минимизации негативных последствий – в случае киберинцидента поставщик услуг применяет необходимые меры во избежание эскалации последствий киберинцидента и возможного его распространения на другую сеть или другую информационную систему и уведомляет об этом киберинциденте компетентный орган в соответствии с настоящим законом;

4) принцип соразмерности - заключается в обеспечении баланса между рисками, которым подвержены сети и информационные системы, и применяемыми требованиями безопасности;

5) принцип сотрудничества - при обеспечении кибербезопасности и решении киберинцидентов ответственные лица сотрудничают и при необходимости учитывают взаимную связь между системами и сервисами и их зависимость.

## Глава II
## ИНСТИТУЦИОНАЛЬНАЯ ОСНОВА, СОТРУДНИЧЕСТВО И СТРАТЕГИЧЕСКАЯ КООРДИНАЦИЯ НА НАЦИОНАЛЬНОМ УРОВНЕ

**Статья 6. Планирование и стратегическое координирование в области кибернетической безопасности на национальном уровне**

(1) Стратегическое координирование на национальном уровне в области кибернетической безопасности осуществляется Правительством, посредством специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности.

(2) Для обеспечения выполнения функции стратегического координирования, Правительство утверждает и устанавливает порядок организации и деятельности Координационного совета в области

кибербезопасности, коллегиального органа без юридического лица, основной функцией которого является продвижение и координирование на стратегическом и оперативном уровне политики кибербезопасности.

(3) Национальная стратегия кибербезопасности является документом политик, определяющим стратегические цели, а также меры политики и регулирования, направленные на достижение и поддержание высокого уровня кибербезопасности. Национальная стратегия кибербезопасности утверждается Парламентом по предложению Правительства.

**Статья 7. Компетентный орган**

(1) Правительство назначает компетентный орган на национальном уровне в области кибернетической безопасности и устанавливает порядок его организации и деятельности.

(2) Компетентный орган также выполняет функции национального единого контактного пункта и группы реагирования на киберинциденты на национальном уровне.

(3) Компетентный орган выполняет следующие основные обязанности:

a) идентифицирует и ведет учет поставщиков услуг на территории Республики Молдова;

b) разрабатывает и обеспечивает продвижение передового опыта управления киберинцидентами и рисками;

c) обеспечивает стратегическое взаимодействие на международном уровне и обмен опытом с другими государствами, международными организациями или созданными ими субъектами по вопросам, связанным с кибербезопасностью;

d) обеспечивает взаимодействие в сфере кибербезопасности с национальными органами государственной власти и учреждениями и с поставщиками услуг;

e) осуществляет надзор и контроль за соблюдением поставщиками услуг обязательств, возложенных на них в соответствии с настоящим законом;

f) издает обязательные к исполнению документы, рекомендации и методические указания для поставщиков услуг и устранению выявленных недостатков и устанавливает срок их выполнения;

g) рассматривает уведомления о неисполнении или ненадлежащем исполнении обязательств поставщиками услуг;

h) иные полномочия, вытекающие из положений настоящего закона и нормативных актов.

(4) При выполнении функции группы реагирования на киберинциденты на национальном уровне, компетентный орган выполняет следующие основные функции:

1) координирует процесс обеспечения кибербезопасности, предотвращения и устранения киберинцидентов в соответствии с положениями настоящего закона и нормативных актов, утвержденных в целях его исполнения;

2) осуществляет мониторинг и анализ киберугроз, уязвимостей и киберинцидентов на национальном уровне, а также оказывает содействие поставщикам услуг, по их запросу, в процессе мониторинга ими своих сетей и информационных систем;

3) выдает ранние предупреждения, оповещения, объявления и распространяет информацию о киберугрозах, уязвимостях и киберинцидентах;

4) получает уведомления о киберинцидентах;

5) обеспечивает реагирование на киберинциденты в порядке, установленном настоящим законом и нормативными актами по его применению, в том числе оказывает содействие поставщикам услуг;

6) собирает и анализирует криминалистические данные и предоставляет динамический анализ рисков и инцидентов и ситуационную осведомленность в области кибербезопасности;

7) сотрудничает на национальном и международном уровнях с группами реагирования на киберинциденты, в том числе в рамках платформы управления киберинцидентами и обмена информацией;

8) выполняет, по запросу поставщика услуг, упреждающее сканирование сетей и информационных систем заявителя для выявления значительных уязвимостей, в соответствии с нормативным актом, утвержденным Правительством в соответствии с частью (9) статьи 12;

9) внедряет безопасные технические средства и решения при обмене информацией с поставщиками услуг и другими соответствующими лицами, а также обеспечивает в соответствии с законодательством защиту информации, ставшей ему известной в процессе исполнения им своих обязанностей;

10) исполняет обязанности координатора процесса согласованного раскрытия уязвимостей в соответствии с нормативной базой, утвержденной Правительством, по предложению специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности, включая:

a) посредничество и содействие взаимодействию между физическим или юридическим лицом, сообщившим об уязвимости, и производителем или поставщиком потенциально уязвимых продуктов или услуг ИКТ, по запросу любого из этих субъектов;

b) выявление вовлеченных физических или юридических лиц и установление контакта с ними;

c) оказание содействия физическим или юридическим лицам, которые сообщают об уязвимости;

d) согласование календарей раскрытия и управление уязвимостями, затрагивающими больше субъектов;

e) обеспечение анонимности физических или юридических лиц, которые сообщают об уязвимости, в случае, когда они ее запрашивают.

(5) В качестве единого национального контактного пункта, компетентный орган выполняет следующие основные функции:

a) обеспечивает связь национальных органов публичной власти и учреждений с аналогичными органами других государств и (или) с международными организациями, или учрежденными ими субъектами;

b) передает по запросу органов власти и государственных учреждений или групп реагирования на киберинциденты в единые контактные пункты других государств уведомления и запросы о киберинцидентах;

c) передает национальным органам государственной власти и учреждениям, в соответствии с их компетенцией, уведомления и запросы по вопросам кибербезопасности, полученные от других государств или от международных организаций, или учрежденных ими субъектов.

**Статья 8. Правительственный центр реагирования на киберинциденты**

(1) Для обеспечения кибербезопасности на правительственном уровне, Правительство создает правительственный центр реагирования на киберинциденты на уровне сетей и информационных систем, принадлежащих государству, назначает юридическое лицо публичного права, ответственное за выполнение соответствующих функций и определяет порядок организации и работы этого центра.

(2) Правительство несет ответственность за обеспечение государственного центра реагирования на киберинциденты необходимыми ресурсами для предотвращения, анализа, выявления и реагирования на киберинциденты на уровне сетей и информационных систем, принадлежащих государству.

(3) Государственный центр реагирования на киберинциденты несет ответственность за обеспечение безопасности сетей и информационных систем, находящихся в государственной собственности, и за содействие по выполнению поставщиками услуг - юридическими лицами публичного права обязательств по обеспечению кибербезопасности, предусмотренных настоящим закона, в том числе обязательств по уведомлению, и их взаимодействию с компетентным органом и национальной группой реагирования на киберинциденты.

**Статья 9. Национальная система управления кризисными ситуациями в области кибербезопасности**

(1) Компетентный орган ответственен за управление киберинцидентами и кризисами в области кибербезопасности на национальном уровне.

(2) С этой целью компетентный орган разрабатывает и утверждает национальный план реагирования на киберинциденты и кризисы в области кибербезопасности, в котором определяются цели и методы управления киберинцидентами и кризисами кибербезопасности на национальном уровне.

(3) Национальный план реагирования на киберинциденты и кризисы в области кибербезопасности должен включать как минимум, но не ограничиваться следующим:

a) цели национальных подготовительных мер и мероприятий;

b) задачи и обязанности компетентных национальных органов;

c) процедуры управления кризисами и каналы обмена информацией;

d) подготовительные мероприятия, включая тренинги и повышение квалификации;

e) поставщики услуг, взаимодействие между ними и ответственными государственными органами или учреждениями, а также задействованная инфраструктура;

f) процедуры и механизмы взаимодействия ответственных государственных органов и учреждений на национальном уровне, а также их скоординированное взаимодействие в управлении масштабными инцидентами и кризисами кибербезопасности, в том числе на европейском и международном уровне.

(4) Правительство утверждает методологическую базу по разработке, актуализации и внедрению положений национального плана реагирования на киберинциденты и кризисы кибербезопасности, взаимодействие между органами власти и государственными учреждениями с полномочиями в процессе разработки и актуализации, а также их взаимодействие с частным сектором.

**Статья 10. Государственный регистр киберинцидентов**

(1) В целях учета данных о возникновении, развитии и разрешении киберинцидентов, а также автоматизации процессов идентификации, регистрации, документирования, классификации, анализа и управления такими инцидентами, мониторинга и регистрации оповещений, киберугроз и уязвимостей кибербезопасности, Правительство, по предложению компетентного органа, устанавливает и регламентирует порядок организации и функционирования Государственного регистра киберинцидентов и, соответственно, информационной системы, предназначенной для его ведения.

(2) Доступ к регистру ограничен, а данные регистра предназначены для внутреннего пользования, если нормативно-правовой базой не предусмотрено иное.

## Глава III
## ОБЯЗАННОСТИ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

### Статья 11. Меры безопасности

(1) Поставщик услуг обязан постоянно применять меры безопасности в целях:

a) предотвращения киберинцидентов;

b) устранения киберинцидентов;

c) предотвращения и смягчения воздействия киберинцидента на непрерывность услуги или безопасность сети и/или информационной системы;

d) предотвращения и смягчения возможного воздействия на непрерывность услуги, сети или информационной системы, зависящих от поставщика услуг.

(2) В процессе применения мер безопасности поставщик услуг обязан:

a) оценивать уязвимости и риски сети и информационной системы, определять серьезность воздействия возможного киберинцидента, произошедшего в результате материализации рисков, описать меры по решению киберинцидента, а также составить отчет в этом отношении;

b) предпринимать соответствующие, пропорциональные технические и организационные меры, в соответствии со стандартами, упомянутыми в части 4 буква a), для управления рисками, связанными с безопасностью сетей и информационных систем, которые использует в своей деятельности. Меры безопасности должны включать по меньшей мере следующее:

1) политику, касающуюся анализа рисков и безопасности сетей и информационных систем;

2) политику и процедуру по управлению инцидентами (предотвращение, обнаружение и реакция на инциденты);

3) политику и процедуру, касающуюся использования криптографии и шифрования, в особенности шифрования от одного конца к другому;

4) политику и процедуру оценивания эффективности внедренных мер безопасности;

5) меры, касающиеся непрерывности деятельности, включая управление резервными копиями и восстановление в случае катастрофы, а также управления кризисами;

6) меры безопасности, применяемые при закупке, развитии и обслуживании сетей и информационных систем, включая управление уязвимостями и их раскрытие;

7) меры безопасности персонала, политики контроля доступа и управление активами;

8) меры, касающиеся безопасности цепочки поставок, включая вопросы безопасности, касающиеся отношений поставщика услуг с его поставщиками или с его прямыми поставщиками услуг;

9) основные практики в области кибергигиены и обучения кибербезопасности;

10) использование решений по аутентификации, безопасной голосовой, видео и текстовой связи и безопасных систем экстренной связи поставщиком услуг;

c) поддерживать в актуальном состоянии документацию о мерах безопасности;

d) обеспечивать мониторинг ситуации в отношении безопасности своих сетей и информационных систем, в том числе с целью выявления ИКТ-услуг, ИКТ-процессов или ИКТ-продуктов, компрометирующих эти сети или системы;

e) предпринимать меры, ориентированные на уменьшение воздействия и распространение киберинцидента, включая, если необходимо, ограничивание использования или доступа к сети или информационной системе;

f) проверять достаточность и соответствие применения мер безопасности, в том числе посредством проведения аудитов безопасности, и документировать результаты этой проверки.

(3) В случае делегирования поставщиком услуг третьей стороне управлением сетью и/или информационной системой или использования услуг третьей стороны для размещения информационной системы, он несет ответственность за применение третей стороной мер безопасности сети и/или информационной системы.

(4) В целях обеспечения выполнения обязательств, предусмотренных настоящей статьей, и безопасности сетей и информационных систем поставщиков услуг, Правительство:

a) посредством национального органа по стандартизации обеспечивает утверждение национальных стандартов в области информационной безопасности и кибербезопасности на основе европейских и международных стандартов и технических спецификаций, относящихся к безопасности сетей и информационных систем;

b) по предложению специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности, утверждает специфические

требования безопасности сетей и информационных систем в зависимости от сетора, подсектора, категории и (или) типа поставщика услуг.

**Статья 12. Обязанности по уведомлению**

(1) Поставщик услуг немедленно информирует компетентный орган, но не позднее 24 часов с момента, как ему стало известно о:

a) киберинциденте, который оказывает значительное влияние на безопасность сети или информационной системы или на непрерывность услуги;

b) киберинциденте, существенное влияние которого на безопасность сети или информационной системы, или на непрерывность услуги неочевидно, но может быть разумно предположено;

c) существенном влиянии киберинцидента, затронувшего третью сторону, на непрерывность услуги или если предоставление этой услуги зависит от услуг, предоставляемых этой третьей стороной.

(2) Компетентный орган без неоправданной задержки, но не позднее, чем через 24 часа после получения информации, указанной в части (1), предоставляет поставщику услуг первоначальный ответ, касающийся значительного инцидента, и, по запросу поставщика услуг, ориентировки или оперативные инструкции относительно реализации возможных мер по решению киберинцидента, в том числе смягчению его воздействия, а также непрерывности деятельности, включая применение механизмов восстановления в случае катастрофы.

(3) Поставщик услуг представляет компетентному органу немедленно, но не позднее, чем через 72 часа после того, как ему стало известно о киберинциденте, обновленную информацию, представленную в соответствии с частью (1), и первоначальную оценку киберинцидента со значительным воздействием, включая его сложность и воздействие, а также индикаторы компрометации, если они доступны.

(4) В случае если сеть или информационная система поставщика услуг управляется и/или размещается третьей стороной, поставщик услуг должен удостовериться, что третья сторона информирует его в сроки, установленные в частях (1) и (3), о киберинциденте, указанном в части (1), или, что третья сторона одновременно информирует в те же сроки компетентный орган о возникновении такого киберинцидента.

(5) Киберинцидент оказывает существенное воздействие, если выполняется хотя бы одно из следующих условий:

a) тяжесть последствий киберинцидента определена как минимум высокая в отчете об оценке рисков сети и информационной системы, составленном в соответствии с положениями статьи 11 части (2) пункта a) и требованиями, предусмотренными в упомянутых актах в статье 11 часть (4);

b) по причине киберинцидента оказание услуги не может быть продолжено по истечении максимально допустимого срока, установленного в договоре о согласованном уровне услуг, заключенном в рамках договорных отношений поставщика услуг с другими лицами, или предусмотренных требованиями о непрерывности услуги, установленными в документации, предусмотренной статьей 11 часть (2) пункты a), b) и c);

c) непрерывность услуги другого поставщика услуг нарушена киберинцидентом;

d) поставщику услуг, уведомившему о киберинциденте, другому поставщику услуг или пользователям услуг причинен или может быть причинен значительный материальный или нематериальный ущерб в результате киберинцидента.

(6) Поставщик услуг обязан информировать без необоснованных задержек, но не позднее 24 часов с момента, когда ему стало известно о значительной киберугрозе, получателей предоставляемых им услуг, которые могут быть затронуты такой угрозой, относительно мер, включая корректирующие меры, которые они могли бы предпринять, во избежание осуществления этой угрозы. В случае если поставщик услуг не может индивидуально определить и уведомить потенциально затронутых получателей, он информирует общественность. В случае если обнаруживается, что осуществление значительной киберугрозы неизбежно, поставщик услуг информирует получателей своих услуг о фактической значительной киберугрозе.

(7) В случае если поставщик услуг не выполняет обязательства по уведомлению, предусмотренные частью (6) в соответствующий срок, компетентный орган напрямую требует от поставщика услуг выполнения обязательства по уведомлению и, в случае его невыполнения им в трехчасовой срок с момента запроса, компетентный орган уведомляет потенциально затронутых получателей или общественность, уведомляя об этом поставщика услуг. Порядок информирования получателей поставщиками услуг или компетентным органом является предметом регулирования нормативного акта, предусмотренного частью (9).

(8) В случае устранения киберинцидента со значительным воздействием, поставщик услуг обязан в течение не более одного месяца с момента передачи обновленной информации в соответствии с частью (3), передать компетентному органу отчет, который включает по меньшей мере информацию о причинах киберинцидента, времени его устранения, примененных мерах и воздействии киберинцидента.

(9) Процедура уведомления о киберинцидентах, включая взаимодействие между поставщиком услуг и компетентным органом, порядок определения воздействия киберинцидента и формат информации из оценок и отчетов, представляемых в процессе управления киберинцидентом, устанавливаются Правительством по предложению

специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности.

(10) Обязанность, предусмотренная частью (1), не ограничивает право поставщика услуг уведомлять компетентный орган о киберугрозах и инцидентах, которые удалось избежать на пределе, а также о киберинцидентах, не оказывающих значительного воздействия, предусмотренного в части (5).

(11) Поставщики услуг – юридические лица публичного права уведомляют о киберинцидентах правительственный центр реагирования на киберинциденты в целях выполнения обязательств, предусмотренных настоящей статьей. Правительственный центр реагирования на киберинциденты информирует компетентный орган о киберинцидентах, указанных в пунктах a)-c).

**Статья 13. Добровольное уведомление**

(1) Юридические лица публичного или частного права, которые не идентифицированы компетентным органом как поставщики услуг, а также физические лица могут направлять ему уведомления о значительных киберинцидентах, киберугрозах и киберинцидентах, которые удалось избежать на пределе.

(2) Уведомления, указанные в частях (1) и (2), решаются компетентным органом в установленном настоящим законом порядке и актом, утвержденным в соответствии со статьей 12, частью (8), с приоритетом рассмотрения и решения обязательных уведомлений в соответствии с положениями настоящего закона, обеспечивая конфиденциальность и надлежащую защиту информации, предоставленной уведомителем.

(3) Добровольное уведомление не налагает на лиц, указанных в частях (1) и (2), каких-либо дополнительных обязательств, которые не возникли бы у них, если бы они не отправили уведомление, за исключением обязательств, которые возникают или могут у них возникнуть согласно соответствующему законодательству в рамках мероприятий по предупреждению, расследованию, выявлению и уголовному преследованию преступлений.

**Статья 14. Меры безопасности сетей и информационных систем юридических лиц публичного права**

(1) Юридические лица публичного права обязаны применять меры, установленные в статье 11 частях (1), (2) и (3), и требования об обязательном уведомлении о киберинциденте, предусмотренные статьей 12.

(2) Обязательные минимальные меры безопасности для юридических лиц публичного права устанавливаются Правительством по предложению специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности.

**Статья 15. Предотвращение и устранение киберинцидентов**

(1) В целях обеспечения кибербезопасности, компетентный орган осуществляет мониторинг доменных имен в адресном пространстве Интернета Республики Молдова и связанных с доменом верхнего уровня .md, анализирует риски, а также их воздействие на государство, общество и безопасность сетей и информационных систем.

(2) Для противодействия непосредственной значительной киберугрозе безопасности сетей и информационных систем или для устранения или смягчения последствий значительного киберинцидента, компетентный орган ограничивает использование или доступ к сети или информационной системе, если совокупно выполняются следующие условия:

a) киберинцидент ставит под угрозу или наносит ущерб безопасности другой сети или информационной системы;

b) администратор сети или информационной системы не в состоянии своевременно противодействовать значительной угрозе или устранить серьезный сбой, вызванный киберинцидентом;

c) невозможно противодействовать серьезной угрозе или устранить серьезный сбой, вызванный киберинцидентом, посредством применения иной меры;

d) противодействие серьезной угрозе или устранение сбоя, возникшего в результате киберинцидента, не причиняет несоразмерного ущерба.

(3) Компетентный орган уведомляет как можно скорее, но не позднее 24 часов, о применении мер, предусмотренных в части (2), получателя и, в случае поставщика услуг, орган публичной власти, осуществляющий государственную политику в соответствующей области, и, при необходимости, орган, регулирующий рынок в области, в которой предоставляется соответствующая услуга.

(4) При осуществлении своей компетенции в процессе управления киберинцидентами, компетентный орган обязан учитывать деловые интересы поставщика услуг, обеспечивать сохранение коммерческой тайны в соответствии с законодательством. Компетентный орган обеспечивает защиту сведений, отнесенных к государственной тайне, и персональных данных в соответствии с положениями нормативных актов в этих областях.

(5) Компетентный орган информирует Службу информации и безопасности немедленно, но не позднее, чем через 24 часа после того, как

ему стало известно о киберинцидентах со значительным воздействием, предотвращенных или устраненных, которые были направлены на объекты критической инфраструктуры.

**Статья 16. Трансграничный обмен информацией**

В связи с выполнением функциональных обязанностей, предусмотренных настоящим законом, или на основании обязательства, вытекающего из международного договора, Компетентный орган вправе передавать другому государству или международной организации информацию о предотвращении и устранении киберинцидента, если нет риска того, что передаваемая информация может нанести ущерб национальной безопасности или проведению уголовно-процессуальных действий.

**Статья 17. Добровольный обмен информацией**

(1) Поставщики услуг и, в зависимости от обстоятельств, другие юридические лица, не подпадающие под действие настоящего закона, могут взаимно обмениваться информацией, касающейся кибербезопасности, на добровольной основе, включая обмен информацией, касающейся киберугроз, предотвращенных киберугроз, уязвимостей, техник и процедур, показателей компрометации, состязательной тактики, информацию об объектах угроз, оповещения о кибербезопасности и рекомендации по конфигурации инструментов кибербезопасности для обнаружения кибератак, если такой обмен информацией:

a) направлен на предотвращение и обнаружение инцидентов, реагирование на инциденты или восстановление после них, или смягчение их последствий;

b) повышает уровень кибербезопасности, в частности, путем повышения осведомленности о киберугрозах, ограничения или предотвращения возможности распространения таких угроз, поддержки ряда защитных возможностей, устранения и раскрытия уязвимостей, обнаружения угроз, методов ограничения и предотвращения угроз, стратегии смягчения или этапы процессов реагирования и восстановления, или содействия сотрудничеству между государственными и частными юридическими лицами в области исследования киберугроз.

(2) Компетентный орган выступает посредником в обмене информацией между юридическими лицами, указанными в части (1), путем создания и управления некоторыми платформами, в том числе технико-технологическими, и надежными сообществами. Для обеспечения защиты потенциально секретной информации, компетентный орган способствует подписанию соглашений об обмене информацией между участниками таких платформ и сообществ. Порядок подписания, содержание и другие

аспекты соглашений об обмене информацией определяются компетентным органом.

(3) Юридические лица публичного права могут заключать соглашения об обмене информацией в области кибербезопасности на условиях, установленных положением, утвержденным Правительством, по предложению специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности.

(4) Поставщики услуг обязаны информировать компетентный орган о подписании соглашений об обмене информацией в области кибербезопасности, указанных в части (2), или отзыве таких соглашений, в течение 3 дней с даты подписания или, в зависимости от обстоятельств, отзыва.

## Глава IV
## ГОСУДАРСТВЕННЫЙ НАДЗОР И КОНТРОЛЬ

### Статья 18. Надзор

(1) Компетентный орган осуществляет функцию надзора за соблюдением поставщиками услуг положений настоящего закона путем постоянного мониторинга за тем, как они выполняют свои обязательства в соответствии с положениями настоящего закона и нормативных актов по его применению, в том числе путем осуществления аудитов безопасности.

(2) В случае если поставщик услуг, ответственный за управление киберинцидентом, не может своевременно отреагировать или устранить киберинцидент, компетентный орган обеспечивает применение необходимых мер для устранения киберинцидента.

(3) Порядок применения мер надзора устанавливается Правительством по предложению специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности.

### Статья 19. Государственный контроль

(1) Компетентный орган осуществляет контроль за соблюдением настоящего закона поставщиками услуг юридическими лицами частного права, применяя положения Закона № 131/2012 о государственном контроле за предпринимательской деятельностью.

(2) Компетентный орган осуществляет контроль исключительно на основании изданного для этой цели мотивированного акта, основанного на оценке риска для безопасности сетей и информационных систем поставщиков услуг, а также с предварительным уведомлением поставщика услуг о предполагаемом контроле.

(3) Для осуществления контроля компетентный орган имеет право доступа к информации, имуществу и помещениям, принадлежащим поставщику услуг, подлежащему контролю, необходимых для достижения целей контроля.

(4) Компетентный орган проводит проверки только в случае, если:

a) выявил и по результатам предварительного расследования подтвердил факты нарушения положений настоящего закона; и/или

b) был уведомлен о нарушениях, неисполнении или ненадлежащем исполнении поставщиком услуг обязанностей, предусмотренных настоящим законом.

(5) Правительство по предложению специализированного органа центрального публичного управления, ответственного за реализацию государственной политики в области кибербезопасности, устанавливает отдельно для поставщиков услуг – юридических лиц частного права и поставщиков услуг – юридических лиц публичного права, подробные процедуры, касающиеся порядка осуществления компетентным органом контроля за соблюдением ими своих обязательств в соответствии с настоящим законом.

## Глава V
## ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ. ФИНАНСИРОВАНИЕ

### Статья 20. Защита персональных данных

(1) При осуществлении полномочий, возложенных на него настоящим законом, компетентный орган обрабатывает персональные данные на условиях, установленных законодательством в этой области.

(2) Если в процессе осуществления своих функций компетентному органу становится известно о том, что нарушение поставщиком услуг обязательств, предусмотренных настоящим законом, может повлечь за собой нарушение законодательства о защите персональных данных, компетентный орган незамедлительно информирует орган контроля за обработкой персональных данных.

### Статья 21. Ответственность

(1) Сотрудники компетентного органа несут ответственность в соответствии с законодательством за неисполнение или ненадлежащее исполнение должностных обязанностей, установленных нормативными актами.

(2) Сотрудники государственных органов/учреждений, поставщиков услуг, взаимодействующие с компетентным органом в условиях настоящего закона, несут ответственность в соответствии с

законодательством за неисполнение или ненадлежащее исполнение должностных обязанностей, установленных нормативными актами.

**Статья 22. Финансирование внедрения настоящего закона**

(1) Финансирование деятельности компетентного органа осуществляется из государственного бюджета в пределах ассигнований, утвержденных законом о годовом бюджете.

(2) Реализация положений настоящего закона поставщиками услуг - юридическими лицами публичного права финансируется за счет бюджета, из которого финансируется деятельность соответствующих юридических лиц в пределах ассигнований, утвержденных законом/решением о годовом бюджете.

(3) Реализация положений настоящего закона поставщиками услуг - юридическими лицами частного права - осуществляется за счет средств этих юридических лиц.

(4) Для реализации положений настоящего закона Правительство может привлекать финансовые средства из проектов внешней помощи.

## Глава VI
## ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

**Статья 23. Вступление закона в силу и меры по его осуществлению**

(1) Настоящий закон вступает в силу 1 января 2025 года.

(2) Правительство:

a) в течение 9 месяцев со дня опубликования настоящего Закона предпримет необходимые меры по назначению компетентного органа, а также регулированию его организации и деятельности и утверждения структуры и лимита персонала;

b) в течение 6 месяцев со дня опубликования настоящего закона внесет в Парламент предложения о приведении нормативных актов в соответствие с настоящим законом;

c) в течение 12 месяцев со дня опубликования настоящего закона приведет свои нормативные акты в соответствие с настоящим законом, обеспечит разработку и принятие нормативных актов, необходимых для реализации положений настоящего закона, в том числе определит полномочия специализированного центрального государственного органа, ответственного за реализацию государственной политики в области кибербезопасности;

d) в течение 12 месяцев со дня вступления в силу настоящего Закона разработает, утвердит и представит на рассмотрение Парламента Национальную стратегию в области кибербезопасности.

(3) Компетентный орган:

a) в течение 3 месяцев со дня вступления в силу нормативных актов, предусмотренных статьей (4) частью (2), идентифицирует поставщиков услуг, уведомит их в установленном порядке и включит их в Список поставщиков услуг, составленный в соответствии с настоящим законом;

b) утвердит нормативные акты, необходимые для реализации положений настоящего закона.

**Председатель Парламента**