

ASGARDIA

PARLIAMENT



Закон об информационной кибербезопасности Асгардии (AISSCA)

Третье чтение

Редакция от: 24.06.2024 г.

Задача и ключевые принципы:

Наладить создание механизмов безопасности, необходимых для предотвращения и защиты от атак, шпионажа, государственной измены и прочих видов угроз системам безопасности Асгардии. Обеспечить защиту информации государственных органов управления и граждан от возможных посягательств на национальные интересы, а также гарантировать права каждого гражданина на безопасность и защищенность его информации, а также право доступа к ней. Данные статьи позволят разработать нормативные требования, обеспечивающие комплексное использование и защиту всех цифровых активов Асгардии от атак: внутренних и внешних, частных и государственных.

Правовая основа

Конституция Асгардии, Глава 6 (статьи 21-26), статья 30 и статья 40. Необходимо отметить, что в настоящем Законе отражены не все аспекты, приведенные в перечисленных статьях. Закон о Законах, 2018 г.

Определения

- *Законодательная власть Асгардии (ЛВА)*, которая состоит из Парламента (формулирующего настоящий Закон);
- *Исполнительная власть Асгардии (ЕВА)*, то есть Правительство, состоящее из Министерств; ЕВА реализует и выполняет настоящий

Закон;

- *Судебная власть Асгардии (JBA)*, которая разрешает юридические разногласия, а также толкует, защищает и применяет настоящий Закон в судебных делах;
- *Информация* — это знания, сведения, а также прочие данные и факты;
- *Обработка информации* включает доступ, создание, изменение, копирование, передачу и удаление информации.
- *Служба информационной и технологической безопасности (OIST)*
- *Аналитический центр безопасности Асгардии (ASAC)*
- *Операционный центр безопасности Асгардии (ASOC)*
- *Система управления информационной безопасностью Асгардии (AIMS)*

Статья 1: Службы информационной безопасности

1.1 Соответствующие органы государственного управления несут ответственность за исполнение настоящего Закона.

Статья 2: Категоризация и классификация

2.1 Вся цифровая и аналоговая информация, записанная или хранящаяся в Асгардии, будет классифицирована, категоризирована и маркирована в соответствии с формулировками и предписаниями Закона Асгардии об информации, подлежащей контролю.

2.1.1 Категоризация будет определять сферу назначения данных, систем или физического места.

2.1.2 Классификация определяет степень конфиденциальности данных, систем или физического места.

2.2 Любые сотрудники, имеющие доступ к системам, которые обрабатывают данные Асгардии, включая, помимо прочего, хранение, передачу, просмотр, обсуждение или уничтожение данных, будут обучены категоризации и классификации обрабатываемой информации.

2.3 Любые системы, обрабатывающие данные Асгардии, включая системы, связанные с хранением, передачей, просмотром, обсуждением или уничтожением данных, должны быть созданы или настроены с использованием технических средств управления, соответствующих категоризации и классификации обрабатываемой информации на основе присвоенной ей маркировки.

2.4 Любая государственная или частная организация Асгардии или физическое

лицо, не соблюдающее данное требование, будет подвергнуто штрафным санкциям в соответствии с применимым законодательством.

Статья 3: Обработка данных

- 3.1 Внедрение систем хранения, передачи, уничтожения, обработки и отображения данных должно соответствовать или превосходить требования стандартов, установленных соответствующими органами государственного управления и законодательством Асгардии, и предусматривать использование контрмер по обеспечению информационной безопасности на основании соответствующего международного законодательства.

3.1.1 Третьи стороны, предоставляющие услуги Правительству Асгардии, должны подтверждать посредством периодических проверок, что все системы и ресурсы, обрабатывающие данные Асгардии, соответствуют минимальным стандартам, требуемым нормативными актами.

Статья 4: Охрана и безопасность инфраструктуры

- 4.1 Соответствующие органы государственного управления обязаны создать и поддерживать работу Операционного центра безопасности Асгардии (ASOC) в случае и после его создания, в обязанности которого входит создание и поддержание надежной и безопасной цифровой инфраструктуры для Асгардии, согласно положениям применимых нормативных актов.

Статья 5: Должностные нарушения

5.1 Ни один Гражданин Асгардии не должен принимать участие в каких-либо действиях, прямо или косвенно приводящих к компрометации любой системы или информации с целью причинения вреда, что подлежит урегулированию в надлежащем судебном порядке.

5.1.2 Степень строгости санкций или исправительной меры/дисциплинарного взыскания за каждое нарушение будет определяться в соответствии с применимыми нормативными актами.

Статья 6: Свобода информации

6.1 Каждый Гражданин и/или резидент имеет право на получение в государственных учреждениях и органах государственной власти информации, представляющей интерес для него самого или же для общества, которая должна быть предоставлена в сроки, установленные законодательством Асгардии.

6.1.1 Подающий запрос Гражданин или резидент несет ответственность за оплату любых необходимых сборов за предоставление запрашиваемой информации.

6.2 Запросы на информацию могут быть отклонены исходя из национальных интересов или причин юридического характера. Отказ в удовлетворении запросов может быть пересмотрен на основании апелляции в суд.

6.3 Все информационные запросы будут одобрены по умолчанию, если только не будут отклонены в прямой форме на конкретных, определенных основаниях. Информация может быть разглашена частично или полностью (вымарана) в зависимости от уровня секретности и истечения срока рассекречивания. Соответствующие органы государственного управления могут продлить или сократить период сохранения грифа секретности.

Статья 7: Компьютерное мошенничество и злоупотребление

7.1 Мошенничество и связанная с ним деятельность

7.1 Любое лицо, которое умышленно получило доступ, сохранило или распространило данные без разрешения или вышло за рамки санкционированного доступа, что может нанести потенциальный вред Асгардии и противоречить общественным интересам, или же лицо, которое искажает данные, принадлежащие Асгардии или ее гражданам, подлежат исправительной мере или дисциплинарному взысканию, установленному судом.

Статья 8: Система управления информационной безопасностью Асгардии (AIMS)

- 8.1 Система управления информационной безопасностью Асгардии (AIMS) в случае и после его создания будет представлять собой систему метрик и процессов для обеспечения безопасности и защищенности всех информационных систем Асгардии и создаваться на основании соответствующих кодексов.

Статья 9: Безопасность медицинской документации и персональных данных

9.1.1 : В порядке, установленном статьей 22 Раздела 7 Конституции Асгардии, соответствующие органы государственного управления должны обеспечить целостность и безопасность всех персональных данных и медицинской документации граждан Асгардии.

9.1.2 : Правительство должно обеспечить гражданам Асгардии полный доступ и управление их собственной медицинской документацией и персональными данными.

Статья 10: Правительственная информация и информация, полученная в результате обработки данных

10.1.1 Предложения, вносимые Парламентом Асгардии, будут храниться в защищенной системе, согласно положениям соответствующих кодексов.

Статья 11: Минимальные стандарты безопасности Асгардии будут определены в соответствующем порядке