Закон Грузии

Об информационной безопасности

Глава I. Общие положения

Статья 1. Цель Закона

Целью настоящего Закона является содействие действенному и эффективному осуществлению соблюдения информационной безопасности, установление прав и обязанностей публичного и частного секторов в сфере соблюдения информационной безопасности, а также определение механизмов государственного контроля за осуществлением политики информационной безопасности.

Статья 2. Разъяснение терминов

Термины, используемые в настоящем Законе, имеют следующие значения:

а) **информационная безопасность** – деятельность, обеспечивающая соблюдение правил доступа, единства, аутентичности, конфиденциальности информации и информационных систем и их работы в течение длительного времени;

б) **политика информационной безопасности** – совокупность норм и принципов, а также практики, предусмотренных настоящим Законом, другими нормативными актами и международными соглашениями Грузии, служащих обеспечению информационной безопасности и соответствующих международным стандартам, установленным в сфере их соблюдения;

в) **киберпространство** – пространство, отличительной особенностью которого является использование электронных устройств и электромагнитного спектра посредством связанных в сети систем и вспомогательной физической инфраструктуры для хранения, замены или обмена данными;

г) **кибератака** – деяние, во время совершения которого электронное устройство или (и) связанная с ним сеть либо система используется вследствие нарушения, создания препятствий или уничтожения систем, имущества или функций, входящих в критическую информационную систему, либо путем незаконного добывания информации;

д) **компьютерный инцидент** – реальное или потенциальное нарушение в сфере политики информационной безопасности в результате использования информационных технологий, влекущее доступ, разглашение информации без разрешения на то, ее повреждение или создание помех либо завладение информационным ресурсом;

е) **критическая информационная система** – информационная система, непрерывное функционирование которой имеет важное значение для обороны или (и) экономической безопасности страны, нормального функционирования органов государственной власти или (и) общества;

ж) **субъект критической информационной системы** – государственный орган или юридическое лицо, непрерывное функционирование информационной системы которого имеет важное значение для обороны или (и) экономической безопасности страны, сохранения государственной власти или (и) общественной жизни;

з) **конфиденциальная информация** – информация, посягательство на конфиденциальность, целостность или доступность которой может повлечь значительный вред в отношении функций субъекта критической информационной системы и целью классификации которой в качестве конфиденциальной информации является обеспечение правил управления информационными активами, за исключением правил, согласно которым Общий административный кодекс Грузии определяет доступность публичной информации;

и) **информация для внутрислужебного пользования** – информация, предназначенная только для сотрудников субъекта критической информационной системы или (и) для лиц, имеющих с ним договорные отношения, посягательство на конфиденциальность, целостность или доступность которой может повлечь создание существенных препятствий при выполнении субъектом критической информационной системы своих функций либо нанести ущерб безопасности органа государственной власти, государственным интересам или деловой репутации частных лиц и целью классификации которой в качестве информации для внутрислужебного пользования является обеспечение правил управления информационными активами, за исключением правил, согласно которым Общий административный кодекс Грузии определяет доступность публичной информации;

к) **информационный актив** – вся информация и знания (в частности, технологические средства хранения, обработки и передачи информации, сотрудники и их знания относительно обработки информации), которые представляют ценность для субъекта критической информационной системы;

л) **информационная система** – любая комбинация информационных технологий и действий, осуществленных с использованием данных технологий, содействующих управлению или (и) принятию решения;

м) **сетевой сенсор** – устройство, специально предназначенное для мониторинга сегмента сети с целью выявления деяний, указывающих на атаку против информационной системы или на проникновение в нее.

н) **Агентство по обмену данными** – юридическое лицо публичного права, действующее в сфере управления Министерства юстиции Грузии (далее – Агентство по обмену данными);(24.12.2013 №1829)

о) **Бюро кибербезопасности** – юридическое лицо публичного права, действующее в сфере управления Министерства обороны Грузии (далее – Бюро кибербезопасности).(24.12.2013 №1829)

Статья 3. Сфера действия Закона

1. Действие настоящего Закона распространяется на все юридические лица и государственные органы, являющиеся субъектами критической информационной системы. Действие настоящего Закона также распространяется на организации и ведомства, которые подчиняются субъекту критической информационной системы или связаны с данным субъектом отношениями в сфере занятости, стажировки, договорными или иными отношениями и которые обеспечивают доступ к информационным активам в пределах данных отношений.

2. Список субъектов критической информационной системы утверждается и классификация критичности соответствующего субъекта устанавливается постановлением Правительства Грузии, проект которого представляет на утверждение Правительству Грузии Министерство юстиции Грузии по согласованию с Министерством обороны Грузии и Министерством внутренних дел Грузии и Службой государственной безопасности Грузии. Во время составления данного списка во внимание принимаются следующие критерии: тяжесть и масштаб предполагаемых последствий работы информационной системы с помехами или ее выхода из строя; тяжесть предполагаемого экономического ущерба для субъекта или (и) государства; необходимость оказания информационной системой услуг для нормального функционирования общества; число пользователей информационной системы; материальное положение субъекта и размер предполагаемых расходов вследствие возложения на него обязательств исходя из настоящего Закона. (8.07.2015 N3933)

3. Действие настоящего Закона не распространяется на масс-медиа, редакции изданий, научные, образовательные, религиозные и общественные организации и политические партии независимо от степени значимости их деятельности для обороны или (и) экономической безопасности страны, сохранения государственной власти или (и) общественной жизни.

4. Любое юридическое лицо и орган государственной власти, не являющиеся субъектами критической информационной системы, вправе в добровольном порядке взять на себя обязательства, вытекающие из настоящего Закона.

5. Действие настоящего Закона не распространяется на действия, разрешенные с предварительного согласия субъекта критической информационной системы, целью которых является тестирование информационной безопасности.

6. Положения настоящего Закона не оказывают влияния на действие норм, предусмотренных законодательством Грузии, регулирующих свободу информации, обработку персональных данных, охрану государственной, коммерческой и личной тайны.

Глава II. Организация и обеспечение информационной безопасности

Статья 4. Правила информационной безопасности

1. Субъект критической информационной системы обязан принять правила информационной безопасности для внутрислужебного пользования, которые служат исполнению положений настоящего Закона и определяют политику информационной безопасности организации.

2. Политика информационной безопасности должна удовлетворять минимальным требованиям информационной безопасности (с учетом классификации критичности субъекта критической информационной системы), определенным Агентством по обмену данными в соответствии со стандартами и требованиями, установленными Международной организацией стандартизации (ISO) и Ассоциацией аудита и контроля информационных систем (ISACA). (24.12.2013 №1829)

3. Субъект критической информационной системы представляет Агентству по обмену данными на рассмотрение правила информационной безопасности для внутрислужебного пользования, принятые согласно пункту первому настоящей статьи. Агентство по обмену данными также уведомляется о любом изменении, вносимом в правила информационной безопасности для внутрислужебного пользования. Агентство по обмену данными осуществляет общий анализ документов, предоставленных подобным образом, и представляет рекомендации для устранения выявленных в них недостатков.

4. За исключением документов, предусмотренных пунктом 3 настоящей статьи, Агентство по обмену данными лишено доступа к информации и информационным активам субъекта критической информационной системы, кроме случая, когда субъект критической информационной системы добровольно обеспечивает доступность информации и информационных активов для Агентства по обмену данными.

Статья 5. Управление информационными активами

1. Субъект критической информационной системы в соответствии с правилами для внутрислужебного пользования, предусмотренными пунктом первым статьи 4 настоящего Закона, проводит инвентаризацию информационных систем с целью учета всех информационных активов, в результате чего каждому информационному активу присваивается соответствующий класс критичности – для конфиденциального или внутрислужебного пользования. Все остальные информационные активы, не требующие классификации, считаются открытой информацией.

2. В результате учета информационных активов описывается значение, ценность, безопасность и существующий уровень защиты каждого информационного актива.

3. Во время создания информационного актива соответствующий класс критичности устанавливает автор актива или (и) лицо, ответственное за актив.

4. Правила управления информационными активами, в частности, правила их описания, классификации, доступа к ним, выдачи (опубликования), изменения и уничтожения, устанавливает Агентство по обмену данными нормативным актом, за исключением правил,

согласно которым Общий административный кодекс Грузии определяет доступность публичной информации.

Статья 6. Аудит информационной безопасности и тестирование информационных систем

1. С согласия субъекта критической информационной системы Агентство по обмену данными или лицо либо организация, подобранная субъектом критической информационной системы из авторизованных Агентством по обмену данными лиц, проводит оценку соответствия правил информационной безопасности для внутрислужебного пользования (политики информационной безопасности) минимальным стандартам безопасности, установленным Агентством по обмену данными. После проведения аудита составляется заключение, выполнение требований которого является обязательным.

2. Правила проведения аудита информационной безопасности, предусмотренного пунктом первым настоящей статьи, устанавливает Агентство по обмену данными нормативным актом.

3. Стоимость аудита информационной безопасности, проведенного Агентством по обмену данными, определяется договором, оформленным с субъектом критической информационной системы.

4. Агентство по обмену данными нормативным актом устанавливает порядок прохождения авторизации лицами и организациями, наделенными полномочиями на проведение аудита информационной безопасности, процедуры авторизации и стоимость авторизации.

5. С согласия субъекта критической информационной системы Агентство по обмену данными или с предварительного разрешения Агентства по обмену данными независимое лицо либо организация с соответствующей компетенцией, подобранная субъектом критической информационной системы, проводит тест на определение степени проникновения в информационную систему (пенетрация) и оценку уязвимости данной системы по заранее запланированной и документированной задаче.

6. Если в результате аудита или тестирования, предусмотренного настоящей статьей, будет выявлено несоответствие требованиям политики информационной безопасности, субъект критической информационной системы проводит анализ причины несоответствия и в случае необходимости определяет и осуществляет надлежащие мероприятия по исправлению указанного, график проведения которых представляет Агентству по обмену данными.

Статья 7. Менеджер информационной безопасности

1. Субъект критической информационной системы обязан определить конкретное лицо (лица) или сотрудника (сотрудников), который (которые) ответствен (ответственны) за выполнение требований информационной безопасности субъекта критической информационной системы (менеджер информационной безопасности).

2. Основными обязанностями менеджера информационной безопасности являются:

а) ежедневный мониторинг выполнения требований политики информационной безопасности;

б) описание информационных активов и доступа к ним;

в) подготовка внутриведомственной документации в связи с политикой информационной безопасности;

г) сбор информации об инцидентах в сфере информационной безопасности и мониторинг реагирования на них;

д) отчетность по вопросам информационной безопасности и административная (организационная) деятельность иного рода;

е) организация и проведение общих и отраслевых тренингов в сфере информационной безопасности;

ж) другие обязанности, определенные субъектом критической информационной системы.

3. Менеджер информационной безопасности подотчетен перед руководителем субъекта критической информационной системы или соответственно уполномоченным им сотрудником либо группой лиц с полномочиями на осуществление политики информационной безопасности (коллегиальным органом). Все важные решения, касающиеся осуществления политики информационной безопасности, принимаются лицом (лицами), определенным (определенными) настоящим пунктом, или по предварительному согласованию с ним (с ними).

4. Менеджер информационной безопасности устанавливает план действий в отношении информационной безопасности и представляет ежегодный отчет о выполнении данного плана лицу (лицам), определенному (определенным) пунктом 3 настоящей статьи, и Агентству по обмену данными.

Глава III. Обеспечение кибербезопасности

Статья 8. Группа помощи Агентства по обмену данными по реагированию на компьютерные инциденты

1. Исполнение положений настоящего Закона, в частности, управление инцидентами против информационной безопасности в киберпространстве Грузии, а также другую, направленную на координацию информационной безопасности, связанную с ней деятельность, которая служит устранению первостепенных угроз кибербезопасности, осуществляет Группа помощи Агентства по обмену данными по реагированию на компьютерные инциденты – CERT.GOV.GE (далее – Группа помощи).

2. К первостепенным угрозам кибербезопасности относятся:

а) кибератака, создающая угрозу жизни и здоровью людей, государственным интересам или обороноспособности страны;

б) кибератака против информационных систем субъекта критической информационной системы;

в) кибератака, создающая угрозу финансовым ресурсам или (и) праву собственности в отношении государства, организации или частного лица;

г) все остальные деяния, которые исходя из характера, цели, источника, объема или размера либо из объема ресурсов, необходимых для пресечения указанных деяний, представляют значительную угрозу для нормального функционирования критической информационной системы.

3. Обязанностями Группы помощи являются:

а) выдача рекомендаций относительно соблюдения информационной безопасности критической информационной системы;

б) своевременное выявление компьютерных инцидентов;

в) реагирование на компьютерные инциденты и координация реагирования на них;

г) учет компьютерных инцидентов, а также установление и категоризация приоритетов реагирования на них;

д) анализ компьютерных инцидентов;

е) оказание помощи в исправлении последствий компьютерных инцидентов и в процессе минимизации вреда;

ж) координация мер по превенции компьютерных инцидентов и содействие внедрению подобных мер;

з) повышение сознательности по вопросам информационной безопасности, в том числе – предоставление информации об угрозах и уязвимых местах в критической информационной системе, если доступность указанной информации не причинит вред информационной безопасности;

и) предупреждение широкого круга потребителей о возможных угрозах и предоставление ему соответствующей информации;

к) образовательное и информационное обеспечение по вопросам информационной безопасности;

л) представительство и координация в вопросах информационной безопасности на международном уровне;

м) другие обязанности, связанные с целями информационной безопасности и определенные законом или иными нормативными актами.

4. Группа помощи вправе потребовать доступ к информационному активу субъекта критической информационной системы, его информационной системе или (и) предмету, входящему в информационную инфраструктуру, если указанный доступ необходим для надлежащего реагирования на происходящий или происшедший компьютерный инцидент. Менеджер информационной безопасности после рассмотрения требования в разумный срок незамедлительно извещает Группу помощи о возможности или невозможности соответствующего доступа.

5. Компетенция Группы помощи, процедуры работы, механизмы реагирования на компьютерные инциденты и другие правила деятельности устанавливаются нормативным актом Агентства по обмену данными.

Статья 9. Специалист по компьютерной безопасности

1. Субъект критической информационной системы обязан определить конкретное лицо (лица) или сотрудника (сотрудников), который (которые) ответствен (ответственны) за практическое обеспечение безопасности компьютерных систем субъекта критической информационной системы (специалист по компьютерной безопасности).

2. Основными обязанностями специалиста по компьютерной безопасности являются:

а) ежедневный мониторинг и оценка компьютерных систем;

б) идентификация компьютерных инцидентов и реагирование на них;

в) анализ и отчетность компьютерных инцидентов и мер безопасности;

г) координация с Группой помощи;

д) другие обязанности, определенные субъектом критической информационной системы.

3. Специалист по компьютерной безопасности подотчетен перед руководителем службы информационных технологий субъекта критической информационной системы или соответственно уполномоченным им сотрудником.

4. Специалист по компьютерной безопасности должен быть готов к оказанию услуг в любое время, в том числе – по истечении рабочих часов. Он обязан обеспечивать постоянную координацию с Агентством по обмену данными в условиях происходящих или возможных кибератак на субъекта критической информационной системы, а также в процессе устранения последствий данной кибератаки.

5. Если происходящая или возможная кибератака создает особую угрозу обороноспособности, экономической безопасности страны, нормальному функционированию государственной власти или (и) общества, Агентство по обмену данными правомочно осуществлять

временную координацию специалистов по компьютерной безопасности в целях предотвращения, отражения кибератак или (и) устранения их последствий.

Статья 10. Идентификация компьютерного инцидента

1. Субъект критической информационной системы осуществляет идентификацию компьютерных инцидентов, что подразумевает изучение и описание каждого инцидента и реагирование на них.

2. По согласованию с субъектом критической информационной системы Агентство по обмену данными и специалист по компьютерной безопасности осуществляют в сети субъекта критической информационной системы конфигурирование и управление сетевым сенсором (система сенсоров), необходимым для идентификации и исследования компьютерных инцидентов. Правила конфигурации сетевого сенсора устанавливаются нормативным актом Агентства по обмену данными.

3. Группа помощи незамедлительно уведомляется об идентификации компьютерного инцидента, и в случае необходимости осуществляются неотложные мероприятия в целях хранения и защиты информации о данном инциденте.

4. Группа помощи изучает и описывает компьютерные инциденты и осуществляет адекватное на них реагирование при выполнении функций, предусмотренных настоящим Законом.

Глава III[1]

Бюро кибербезопасности (24.12.2013 №1829)

Статья 10[1]. Статус и функции Бюро кибербезопасности 24.12.2013 №1829)

1. Политика информационной безопасности для субъектов критической информационной системы в сфере обороны должна удовлетворять минимальным требованиям информационной безопасности в сфере обороны (с учетом классификации критичности субъекта критической информационной системы в сфере обороны), определенным Бюро кибербезопасности в соответствии со стандартами и требованиями, установленными Международной организацией стандартизации (ISO) и Ассоциацией аудита и контроля информационных систем (ISACA).

2. Бюро кибербезопасности создается в соответствии с настоящим Законом и Законом Грузии «О юридическом лице публичного права».

3. Сфера действия Бюро кибербезопасности не распространяется на Агентство по обмену данными, полномочия, функции и сфера действия которого определяется настоящим Законом и Законом Грузии «О создании юридического лица публичного права – Агентства по обмену данными».

4. Перечень субъектов критической информационной системы в сфере обороны утверждается и классификация критичности соответствующего субъекта устанавливается соответствующим актом Правительства Грузии, проект которого представляет на утверждение Правительству Грузии Министерство юстиции Грузии по согласованию с Министерством обороны Грузии, Министерством внутренних дел Грузии и Службой государственной безопасности Грузии. При составлении этого списка во внимание принимаются следующие критерии: тяжесть и масштаб предполагаемых последствий работы информационной системы с помехами или ее выхода из строя с точки зрения обороноспособности государства; тяжесть предполагаемого экономического ущерба для субъектов или (и) государства; необходимость оказания информационной системой услуг для беспрепятственного функционирования в сфере обороноспособности государства; число пользователей информационной системы; материальное положение субъекта и размер предполагаемых расходов вследствие возложения на него соответствующих обязательств. (8.07.2015 N3933)

5. Положение о Бюро кибербезопасности и его структуру утверждает Министр обороны Грузии.

6. Основной функцией Бюро кибербезопасности является осуществление деятельности в пределах полномочий, предоставленных ему законодательством Грузии, в том числе – настоящим Законом.

7. Действие статей 6 и 7, пункта 4 статьи 9 и пункта 2 статьи 10 настоящего Закона не распространяется на деятельность Бюро кибербезопасности.

Статья 10[2]. Директор Бюро кибербезопасности (24.12.2013 №1829)

1. Директора Бюро кибербезопасности назначает на должность и освобождает от должности Министр обороны Грузии.

2. Директор Бюро кибербезопасности имеет двух заместителей, в том числе – одного первого заместителя, исполняющего обязанности директора в случае его отсутствия. Заместителей директора назначает на должность и освобождает от должности директор Бюро кибербезопасности по согласованию с Министром обороны Грузии.

3. Директор Бюро кибербезопасности действует в пределах полномочий, предоставленных ему настоящим Законом и Положением о Бюро кибербезопасности.

4. Директор Бюро кибербезопасности правомочен назначать на должность и освобождать от должности сотрудников Бюро кибербезопасности в порядке, установленном законодательством Грузии.

5. Директор Бюро кибербезопасности издает нормативный акт – приказ в случаях и пределах, определенных настоящим Законом и другими законодательными актами Грузии. Нормативные акты, регулирующие вопросы оборонной политики в сфере кибербезопасности, издает Министр обороны Грузии.

6. Штатное расписание и должностные оклады сотрудников Бюро кибербезопасности утверждает Министр обороны Грузии в порядке, установленном законодательством Грузии.

Статья 10^3. Группа помощи Бюро кибербезопасности по реагированию на компьютерные инциденты (24.12.2013 №1829)

1. Управление кибератаками на субъекты критической информационной системы в сфере обороны, создающими угрозу жизни и здоровью человека, государственным интересам и обороноспособности страны, а также другими инцидентами, направленными против информационной безопасности, и связанную с этим деятельность осуществляет Группа помощи Бюро кибербезопасности по реагированию на компьютерные инциденты – CERT.MOD.GOV.GE (далее – Группа помощи Бюро кибербезопасности).

2. Приоритетные угрозы для Группы помощи Бюро кибербезопасности и обязанности этой Группы в сфере обороны определяются пунктами 2 и 3 статьи 8 настоящего Закона.

Глава IV. Переходные и заключительное положения

Статья 11. Переходные положения

1. Президенту Грузии в 6-месячный срок после введения настоящего Закона в действие издать Указ «Об утверждении списка субъектов критической информационной системы».

2. Агентству по обмену данными в 6-месячный срок после введения настоящего Закона в действие издать следующие нормативные акты:

а) приказ «О Группе помощи Агентства по обмену данными по реагированию на компьютерные инциденты»;

б) приказ «Об утверждении минимальных стандартов в отношении менеджера информационной безопасности субъекта критической информационной системы»;

в) приказ «О правилах конфигурации сетевого сенсора»;

г) приказ «О минимальных требованиях информационной безопасности»;

д) приказ «О порядке прохождения авторизации лицами и организациями с полномочиями на проведение аудита информационной безопасности, процедурах авторизации и плате за авторизацию»;

е) приказ «О порядке проведения аудита информационной безопасности»;

ж) приказ «О правилах управления информационными активами».

3. Правительству Грузии до 1 апреля 2014 года обеспечить принятие постановления «Об утверждении перечня субъектов критической информационной системы».(20.09.2012 №1250)

4. До принятия постановления, предусмотренного пунктом 3 настоящей статьи, сохраняет юридическую силу Указ Президента Грузии от 11 марта2013 года № 157 «Об утверждении перечня субъектов критической информационной системы».(20.09.2012 №1250)

5. Министерству обороны Грузии до 1 апреля 2014 года обеспечить осуществление определенных законодательством Грузии соответствующих мероприятий по созданию Бюро кибербезопасности.(24.12.2013 №1829)

6. Министру обороны Грузии до 1 апреля 2014 года издать следующие нормативные акты (24.12.2013 №1829)

а) приказ «О юридическом лице публичного права – Группе помощи Бюро кибербезопасности по реагированию на компьютерные инциденты»;

б) приказ «О минимальных требованиях к информационной безопасности»;

в) приказ «О правилах управления информационными активами».

Статья 12. Заключительное положение

Настоящий Закон ввести в действие с 1-го июля 2012 года.

Президент Грузии **Михаил Саакашвили**

Тбилиси

5 июня 2012 года

№6391-Ic