Сравнительный анализ подходов к регулированию критической информационной инфраструктуры

Оглавление

I. Список используемых сокращений

Агентство по обмену данными – юридическое лицо публичного права, действующее в сфере управления Министерства юстиции Грузии.

Бюро кибербезопасности – юридическое лицо публичного права, действующее в сфере управления Министерства обороны Грузии.

ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Директива NIS – Директива Европейского парламента и Совета Европейского Союза «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» от 06.07.2016 N 2016/1148.

ЖВУ – жизненно важные услуги в значении, закрепленном Директивой NIS.

Закон BSIG – Закон ФРГ об имплементации положений Директивы 2016/1148 от 14.08.2009 (в ред. 23.06.2017).

КИИ – критическая информационная инфраструктура.

НКЦКИ - Национальный координационный центр по компьютерным инцидентам РФ.

ОГВ – органы государственной власти

ОЖВУ – оператор жизненно-важных услуг в значении Директивы NIS.

ОКИ – оператор критической инфраструктуры в значении закона BSIG ФРГ.

Статут № 506 – статут Соединенного Королевства о регламенте сети и информационных систем от 20.04.2018 № 506.

ФЗ О безопасности КИИ – ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ.

ФСБ – Федеральная Служба Безопасности Российской Федерации.

ФСТЭК – Федеральная служба по техническому и экспортному контролю Российской Федерации.

CMCA – Закон о нарушениях в компьютерной сфере Сингапура от 19.08.1993.

CSL – Закон о кибербезопасности КНР.

CTL – Закон о борьбе с терроризмом КНР.

GDPR – Регламент Европейского парламента и Совета Европейского Союза о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46 / ЕС от 27.04.2016 № 2016/679 (Общий Регламент по защите персональных данных).

HSPD-7 – Директива Президента США по национальной безопасности «Критическая инфраструктура: идентификация, расстановка приоритетов и защита», опубликованная 17.12.2003 № 7.

NSL – Закон о национальной безопасности КНР от 01.06.2015.

PPD-21 – Директива Президентской политики США «Безопасность и устойчивость критической инфраструктуры» от 12.02.2013.

Модели правового регулирования в сфере обеспечения безопасности КИИ

В ходе настоящего исследования было изучено регулирование защиты КИИ в ЕС, непосредственно в ФРГ и Соединенном Королевстве; странах Азии, в частности, в КНР, Японии и Сингапуре; а также в Российской Федерации, Казахстане и Грузии. Каждая юрисдикция представляет определенные особенности, тем не менее любое сравнительно-правовое исследование предполагает выявление не только отличных, но и схожих черт.

В качестве обобщения можно выделить две основные модели регулирования безопасности КИИ в зависимости от непосредственного предмета регулирования: «объектную» (РФ, Казахстан, Германия) и «субъектно-деятельностную» (ЕС кроме Германии, Грузия, Сингапур, Китай, Япония).

В ряде юрисдикций выделенных моделей можно найти наличие сходных терминов, аналогичные обязанности субъектов КИИ, идентичные полномочия компетентных органов в сфере обеспечения безопасности КИИ, установление административной и уголовной ответственности за нарушения в сфере КИИ. Указанное объясняется общей целью соответствующего регулирования – обеспечение безопасности КИИ.

Среди особенностей «объектной» модели можно назвать:

- Регулирование направлено непосредственно на объекты КИИ;
- Наличие иерархически стройной системы регулирования в сфере КИИ;
- Построение терминологического аппарата от определения КИИ и ее объектов;
- Установление четких критериев категорирования через формирование «пороговых значений»;
- Точное определение обязанностей субъектов на транспарантной основе. Основные обязанности содержатся в Законе;
- Ограниченное количество уполномоченных органов с четко-определенной компетенцией.

Указанный подход позволяет, с одной стороны, упорядочить гражданский оборот (новый собственник объекта понимает, к какой категории он относится и какие обязанности на него будут возложены), с другой – упрощает задачу государственным органам по осуществлению контроля за владельцами таких объектов даже в тех случаях, если последние неправильно осуществили категорирование.

Вместе с тем, указанному подходу недостает гибкости в части установления требований к безопасности конкретного объекта.

Среди особенностей «субъектно-деятельностной» модели можно отметить:

- Регулирование деятельности субъектов в сфере КИИ;
- Разрозненность нормативно-правового регулирования в сфере безопасности КИИ;
- Построение терминологического аппарата от определения жизненно-важных услуг (сервисов);
- Гибкость в вопросах категорирования, риск-ориентированный подход;
- Множество регуляторов в разных сферах КИИ.

Субъектно-деятельностная модель определения предмета регулирования является более гибкой. Так, конкретный объект может принадлежать конкретному лицу, но не использоваться, следовательно, ущерб объекту не окажет существенного влияния.

В данной модели имеет значение хозяйственная деятельность субъекта в той или иной сфере и возможный ущерб такой значимой деятельности от компьютерного инцидента.

Указанная модель предусматривает большую степень самостоятельности субъектов и, как правило, предполагает риск-ориентированный подход (когда субъект в каждом конкретном случае принимает решение о соразмерности предпринимаемых мер существующим киберугрозам).

Вместе с тем, указанная модель является менее структурированной и недостаточно прозрачной. Указанный вывод характерен в особенности для США.

На ранних этапах развития правового регулирования в сфере безопасности КИИ рекомендуется использовать объектный подход. Без установления четких критериев категорирования, оставляя определение категории объекта на усмотрение государственного органа или самого лица – владельца объекта КИИ, затруднительно обеспечить единообразие в сфере защищенности объектов КИИ от потенциальных угроз.

Расширение дискреционных полномочий ОГВ вне четких критериев представляет собой коррупциогенный фактор. Кроме того, расширение степени усмотрения субъектов хозяйственной деятельности, вне установления четких критериев несёт в себе риски игнорирования публичных интересов, низкого уровня защищенности объектов КИИ (в тех случаях, когда сама организация не считает необходимым предпринимать эффективные меры по защите). Ввиду вышеизложенного при разработке нормативно-правового регулирования в сфере КИИ в Киргизии рекомендуется в качестве основной модели использовать объектную модель регулирования безопасности КИИ.

II. Сравнительно-правовой анализ подходов к регулированию критической информационной инфраструктуры

1. Общие положения

1.1. Сравнительно-правовое исследование. Общие положения

В предмет сравнительного исследования подходов к правовому регулированию в сфере критической информационной инфраструктуры вошли подходы РФ, стран ЕС (Германии, Великобритании), США, Казахстана, Грузии, Сингапура, Японии и КНР.

Основное внимание было уделено сравнению подходов к регулированию по следующим аспектам:

1. Используемый терминологический аппарат;
2. Принципы регулирования;
3. Предмет регулирования;
4. Критерии отнесения к КИИ/ категорирование;
5. Сферы обеспечения безопасности КИИ;
6. Субъекты обеспечения безопасности КИИ, их правовой статус;
7. Публичные органы в сфере обеспечения безопасности КИИ, их полномочия, взаимодействие между собой и с субъектами;
8. Экономическая модель регулирования: порядок распределения издержек;
9. Ответственность в сфере обеспечения безопасности КИИ.

Ниже представлен общий анализ подходов к регулированию в сфере КИИ в каждой из исследуемых юрисдикций, а также более подробный анализ регулирования по каждому из обозначенных аспектов.

1.2. Подход ЕС: наднациональное регулирование. Подход Германии и Соединенного Королевства. Общие положения

Основным источником, регулирующим вопросы защиты КИИ (точнее ЖВУ) в ЕС является Директива №2016/1148 (далее – Директива NIS) Европейского парламента и Совета Европейского Союза «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» от 06.07.2016[1].

Указанный акт является далеко не единственным, регулирующим вопросы кибербезопасности в ЕС. Инциденты в сфере КИИ, которые охватываются указанной Директивой, также являются предметом регулирования других Директив и Регламентов ЕС (например, GDPR[2]). Указанный факт учитывается в самой Директиве. Схожего мнения придерживается и Координационная группа (CG), о которой будет упомянуто далее[3]. Схематично области регулирования можно изобразить следующим образом:

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 30.06.2019).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 30.06.2019).

[3] Reference document on Incident Notification for Operators of Essential Services Circumstances of notification CG Publication 02/2018. URL: http://ec.europa.eu/information_society/newsroom/image /document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf (дата обращения: 30.06.2019).

Директива ЕС, в отличие от регламента, требует трансформации во внутреннее право, то есть не действует напрямую[4]. Государствам-членам предоставляется определенная свобода в вопросах имплементации положений директивны, которая определяет лишь минимальный стандарт защиты.

Согласно ст. 25 Директивы NIS государства-члены ЕС должны опубликовать соответствующие законодательные положения для выполнения требований Директивы. При этом, соответствующие акты должны содержать ссылки на эту Директиву. Учитывая вышеизложенные отличия Директивы от Регламента, а также положения ст. 5 Директивы NIS, государства-члены свободны в выборе способа имплементации соответствующих положений. Государства-члены могут установить более высокие стандарты безопасности. Как указано в п. 6 Преамбулы Директивы NIS, не исключено применение операторами жизненно-важных услуг и провайдерами цифровых услуг более строгих мер[5]. Несмотря на то, что положения преамбулы формально не имеют юридической силы[6], они имеют значение для толкования соответствующих положений исследуемого акта.

23.06.2017 Германия приняла Закон об имплементации положений Директивы и внесении изменений в соответствующие законодательные акты[7]. В целом, в Германии рассматриваемый вопрос урегулирован в Законе BSIG (ред. от 23.06.2017)[8], а также в Указе об определении критических инфраструктур в соответствии с Законом BSIG (ред. от 21.06.2017)[9]. Германское регулирование во многом схоже с российским подходом и представляет интерес, главным образом, в части категоризации объектов КИИ.

---

[4] Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. // СПС "КонсультантПлюс".

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Preamble. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 30.06.2019).

6 Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» // СПС "КонсультантПлюс".

7 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netzund Informationssystemen in der Union (BSIGuaÄndG k.a.Abk.). URL: https://www.buzer.de/gesetz/12607/index.htm (дата обращения: 30.06.2019).

[8] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) URL: https://www.buzer.de/gesetz/8987/index.htm (дата обращения: 30.06.2019).

[9] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) URL: https://www.buzer.de/gesetz/12020/index.htm (дата обращения: 30.06.2019).

Интересно, что в вопросах имплементации не осталась в стороне и Великобритания, которая, несмотря на BREXIT, приняла соответствующий статут № 506, который вступил в силу 10 мая 2018 года[10].

В силу положений п. 2 ст. 1, ст. 7 Директивы NIS, государства-члены должны принять национальные стратегии по обеспечению безопасности сетевых и информационных систем, а также установить требования к соответствующим субъектам, в частности, определить критерии существенности возможного негативного воздействия, установить категоризацию таких субъектов в зависимости от этих критериев. В п. 19 Преамбулы Директивы NIS отмечается: государства-члены ЕС ответственны за определение организаций, которые соответствуют критериям определения оператора жизненно-важных услуг. Список идентифицированных операторов должен регулярно пересматриваться государствами-членами ЕС и при необходимости обновляться. Аналогичное положение содержится и в п. 25 Преамбулы, согласно которой в результате идентификационного процесса государства-члены ЕС должны принять меры по определению организаций, которые должны исполнять обязательства по обеспечению безопасности сетевых и информационных систем. Указанные цели могут быть достигнуты путем принятия перечня всех операторов жизненно-важных услуг или принятия национальных мер, в том числе объективных количественных критериев, таких как производительная мощность оператора или количество пользователей, которые позволят определить организации, обязанные исполнять требования по обеспечению безопасности сетевых и информационных систем.

Национальные стратегии кибербезопасности действуют в большинстве стран ЕС. В Стратегии кибербезопасности Германии особое внимание (в Разделе 2) уделяется вопросам защиты критической инфраструктуры[11]. Внимание данному вопросу также уделяется в Национальной стратегии цифровой безопасности Франции[12]. В Национальной стратегии кибербезопасности Соединенного Королевства на 2016 – 2021 годы идет речь о защите критической национальной инфраструктуры (CNI) через защиту наиболее важных организаций и компаний от кибератак. Уполномоченные должностные лица таких компаний несут ответственность за обеспечение безопасности. Они должны идентифицировать критические системы и регулярно оценивать их уязвимость. Органы государственной власти также берут на себя ряд обязательств в вышеназванной сфере[13].

Важно также отметить, что исследуемая Директива NIS не применяется:

- К микропредприятиям и малым предприятиям, в соответствии с п. 11 ст. 16 Директивы 2016/1148. (Малое предприятие – это предприятие, на котором работает менее 50 человек и чей годовой оборот и / или годовой баланс не превышает 10 млн. евро. Микропредприятие – это предприятие на котором работает менее 10 человек и чей годовой оборот и / или годовой баланс не превышает 2 млн. евро[14]);

[10] The Network and Information Systems Regulations 2018 URL: https://www.legislation.gov.uk/uksi/2018/506/made (дата обращения: 30.06.2019).

[11] Cyber-Sicherheitsstrategie für Deutschland. 2016. URL: http://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (дата обращения: 30.06.2019).

[12] Stratégie nationale pour la sécurité du numérique. URL: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (дата обращения: 30.06.2019).

[13] UK National cyber security strategy 2016-2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (дата обращения: 30.06.2019).

[14] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361 (дата обращения: 30.06.2019).

- К предприятиям, оказывающим услуги в сфере общественных сетей связи и общедоступных электронных коммуникаций[15], в соответствии с п. 3 ст. 1 Директивы и п. 7 Преамбулы;
- К провайдерам удостоверительных сервисов для электронных транзакций[16], в соответствии с п. 3 ст. 1 Директивы и п. 7 Преамбулы;
- К иным предприятиям, деятельность которых является предметом регулирования (настоящего или будущего) внутриотраслевых актов ЕС, содержащих нормы о безопасности сетевых и информационных систем, за исключением случаев дублирования аналогичных положений (п. 9 Преамбулы);
- К платежным и расчетным системам (п. 14 Преамбулы);
- К предприятиям, оказывающим онлайн-услуги, в рамках которых представляется сравнительный анализ цен на определенные товары или услуги, предоставляемые различными поставщиками, и осуществляется дальнейшее направление пользователя к выбранному им поставщику для покупки продукта (п. 15 Преамбулы).

Необходимо отметить существенный успех в унификации подхода стран-членов ЕС в ходе имплементации положений Директивы NIS. Вместе с тем, стоит отметить небольшую разницу в подходах. Так, одни страны, например, Соединенное Королевство, используют субъектно-деятельностный подход, другие страны, например, Германия, идут от определения объектов КИИ. Также можно отметить несущественные терминологические различия между используемыми категориями «критический» (kritischer – нем.) и «жизненно»-важный (essential – англ.).

Киргизии рекомендуется обратить внимание на прогрессивный европейский подход. Особое место должна занять адаптация соответствующих «пороговых значений», которые могут быть взяты из приведенных Таблиц в немецком Указе. В вопросах ответственности необходимо обратить внимание на опыт Соединенного королевства, а именно: на пропорциональное установление коррелирующих значений ущерба и размера штрафа, а также на возможность установления дифференцированных вариантов административного штрафа, как это сделано в ФРГ. Дополнительно можно обратить внимание на установление уголовной ответственности за кибератаки на объекты критической инфраструктуры по немецкому образцу.

1.3. Подход РФ. Общие положения

В качестве одного из национальных интересов в информационной сфере Доктрина информационной безопасности РФ называет обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь КИИ и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время. Стратегической целью обеспечения информационной безопасности является защита КИИ. Одним из направлений обеспечения информационной

[15] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0021 (дата обращения: 30.06.2019).

[16] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1558488707271&uri=CELEX:32014R0910 (дата обращения: 30.06.2019).

безопасности Доктрина считает повышение защищенности КИИ, повышение безопасности функционирования ее объектов[17].

Основным актом, регулирующим вопросы КИИ в РФ, является ФЗ О безопасности КИИ[18].

Система защиты КИИ в РФ является разработанной не только на уровне Федерального Закона, но и на уровне множества подзаконных актов Президента, Правительства, ФСБ и ФСТЭК. Законодательство предусматривает конкретные правила категорирования объектов КИИ, обязанности субъектов КИИ, порядок их взаимодействия с ФСБ и ФСТЭК. Уголовный кодекс устанавливает наказание за неправомерное воздействие на КИИ.

Вместе с тем, стоит отметить, что оценить успешность применения положений НПА в указанной сфере представляется затруднительным так как согласно ст. 5 Закона РФ О государственной тайне сведения о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак относятся к сведениям, составляющим государственную тайну[19].

Ввиду детальной проработанности российского подхода к защите КИИ можно констатировать, что опыт Российской Федерации в сфере регулирования КИИ может быть полезен при разработке подхода Киргизии, как в целом, в определении законодательной модели (ввиду близости правопорядков двух стран), так и по конкретным аспектам регулирования (например, в части категорирования объектов КИИ).

1.4. Подход Сингапура. Общие положения

Сингапур активно развивает свои режимы защиты данных, кибербезопасности и противодействия киберпреступности. Как указано в Отчете Сингапура о Стратегии кибербезопасности, «Правительство рассматривает свои усилия в этих областях как часть интегрированного плана кибербезопасности, чтобы защитить страну от киберугроз и укрепить репутацию Сингапура в качестве ведущего центра информационных систем»[20].

Ключевые нормативные акты о кибербезопасности Сингапура включают, но не ограничиваются:

- Закон о защите персональных данных 2012 года (далее PDPA), первая в Сингапуре всеобъемлющая правовая основа, созданная для обеспечения защиты персональных данных;
- Закон о неправомерном использовании компьютеров и кибербезопасности[21] (далее CMCA) для борьбы с киберпреступностью и другими киберугрозами;
- Закон о кибербезопасности 2018 года[22], в котором основное внимание уделяется защите важнейшей информационной инфраструктуры Сингапура (КИИ) и созданию всеобъемлющей национальной системы кибербезопасности.

---

[17] Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС Консультант плюс.

[18] ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ // СПС Консультант плюс.

[19] Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 // СПС Консультант плюс

[20] Сингапурская стратегия кибербезопасности, Агентство кибербезопасности Сингапура (октябрь 2016 г.) (Отчет о кибербезопасности) URL: https://www.csa.gov.sg/~/media/csa /documents/publications/singaporecybersecuritystrategy.pdf (дата обращения: 30.06.2019).

[21] Computer Misuse And Cybersecurity (Amendment) Act 2017 URL: https://sso.agc.gov.sg/Acts-Supp/22-2017/Published/20170511?DocDate=20170511 (дата обращения: 30.06.2019).

[22] Cybersecurity Act 2018 (Act. 9 of 2018) https://sso.agc.gov.sg/Acts-Supp/9-2018/ (дата обращения: 30.06.2019).

1.5. Подход КНР. Общие положения

В апреле 2014 года в своем выступлении председатель КНР, Генеральный Секретарь ЦК КПК Си Цзиньпин впервые упомянул «Общую концепцию национальной безопасности». После этого был ускоренно принят ряд законодательных актов, касающихся национальной безопасности. Указанные законы включают положения, касающиеся информационной и технологической безопасности.

1 июля 2015 года Постоянный комитет Всекитайского собрания народных представителей принял Закон о национальной безопасности (The National Security Law, NSL)[23]. NSL впервые предусматривает «защиту национального суверенитета в киберпространстве» и указывает кибербезопасность и информационную безопасность в качестве важных частей национальной безопасности. NSL требует от государства создать систему проверки национальной безопасности для рассмотрения вопросов и действий, которые влияют или могут повлиять на национальную безопасность, включая те, которые касаются продуктов и услуг сетевых информационных технологий.

Закон о борьбе с терроризмом (The Counter-Terrorism Law, CTL)[24] был принят в конце 2015 года, вступил в силу 1 июня 2017 года и стал основным законом в Китае по защите кибербезопасности и личной информации. CTL является первым законом о борьбе с терроризмом в Китае, который включает в себя большой массив положений, имеющих своей целью охватить все аспекты контртеррористической деятельности. CTL обеспечивает обязательства телекоммуникационных и интернет-предприятий сотрудничать с государственными органами в расследовании террористической деятельности. Например, согласно CTL, провайдеры телекоммуникационных и интернет-услуг обязаны оказывать государственным органам техническую помощь в расшифровке сообщений.

Закон о кибербезопасности (The Cyber Security Law, CSL)[25] содержит различные обязательства по защите безопасности для сетевых операторов, включая, но не ограничиваясь следующими:

- соблюдение ряда требований к многоуровневым системам кибербезопасности;
- проверку подлинности личности пользователя (обязанность для определенных операторов сети);
- разработку планов реагирования на чрезвычайные ситуации в области кибербезопасности;
- оказание помощи и поддержки следственным органам, в случае необходимости, для защиты национальной безопасности и расследования преступлений.

CSL налагает ряд повышенных обязательств в области безопасности для операторов КИИ, среди которых можно выделить:

- Требования к внутренней организации, обучению, резервному копированию данных и аварийному реагированию на инциденты;
- Требование о защищенном хранении личной информации и другой важной информации на территории КНР;

---

[23] National Security Law of the People's Republic of China (2015) URL: http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm (дата обращения: 01.07.2019).

[24] Закон КНР «О национальной безопасности» (принят на 18-й сессии Постоянного комитета ВСНП КНР двенадцатого созыва 27.12.2015 г., обнародован Указом Председателя КНР от 27 декабря 2015 г. № 36; вступает в силу с 1 января 2016 г.) URL: http://www.mps.gov.cn (дата обращения: 01.07.2019).

[25] Закон о кибербезопасности КНР URL: http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm (дата обращения: 01.07.2019).

- Требование о прохождении проверки безопасности в отношении закупаемых сетевых продуктов и услуг, которые могут повлиять на национальную безопасность;
- Требование о представлении ежегодных отчетов о результатах оценки безопасности и мерах по улучшению в компетентные государственные органы.

1.6. Подход Японии. Общие положения

В Японии действует «Основной закон о кибербезопасности» (The Basic Act on Cybersecurity)[26], который был принят 6 ноября 2014 года. Основной закон о кибербезопасности является первым законом о кибербезопасности, который был принят среди стран G7.

Ключевой задачей Основного закона о кибербезопасности является обеспечение кибербезопасности при одновременном обеспечении свободного распространения информации. Целью Основного закона о кибербезопасности является продвижение всеобъемлющей и эффективной политики, связанной с кибербезопасностью, и содействие созданию более энергичного и постоянно развивающегося экономического общества, что будет способствовать национальной безопасности Японии.

В настоящее время в Японии существуют другие законы, касающиеся кибербезопасности и киберпреступности, в частности:

- Уголовный кодекс и иные уголовные законы;
- Закон о предотвращении недобросовестной конкуренции;
- Закон о запрещении несанкционированного доступа к компьютеру;
- Основной закон о формировании передового информационного и телекоммуникационного сетевого общества.
- Закон о защите личной информации.

2. Терминология

2.1. Терминология: сравнительно-правовой анализ

Ключевым понятием в исследуемой сфере является понятие КИИ. В целом, понятия КИИ или ЖВУ являются сформированными в правопорядках ЕС, РФ, США.

Так, например, в РФ под КИИ понимаются объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Под ЖВУ в ЕС понимаются услуги в определенных сферах (энергетики, транспорта, банковского дела, финансового рынка, здравоохранения, поставки питьевой воды, цифровой инфраструктуры), которые являются жизненно-важными с точки зрения поддержания важнейшей социальной и/или экономической деятельности; зависят от сетевых и информационных систем; возможный инцидент в их отношении может оказать существенное негативное воздействие.

Общими признаками КИИ (ЖВУ) для исследуемых юрисдикций являются:

- определимость через объекты (системы и активы) или услуги (деятельность) в определенных сферах (энергетика, транспорт и так далее);
- функционирование КИИ зависит от информационных систем;

[26] The Basic Act on Cybersecurity (Act No. 91 of 2018) URL: http://www.japaneselawtranslation.go.jp/law/detail/?printID=&ft=2&re=02&dn=1&yo=Basic+Act+on+Cybersecurity&ia=03&ph=&x=52&y=22&ky=&page=1&vm=02 (дата обращения: 01.07.2019).

- наступление негативных последствий вследствие ущерба, причиненного КИИ, может привести к негативным последствиям.

Для понимания смысла дефиниции КИИ (ЖВУ) необходимо обратиться к понятию объектов КИИ. При этом, важно сделать оговорку о том, что понятие объектов КИИ установлено лишь в ряде стран. Так, объект КИИ не определен в законодательстве многих стран ЕС, поскольку в ЕС преобладает подход, в котором важен субъект и осуществляемая им деятельность, в то время как определение непосредственно объекта КИИ не имеет юридического значения. Исключением является Германия.

Общими для Германии, РФ, Грузии и Казахстана в понимании объекта КИИ являются следующие признаки:

- объект относится к категории информационно-коммуникационной инфраструктуры (информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры) в определенной сфере;
- нарушение или прекращение функционирования таких объектов может привести к ущербу для отдельных сфер или общественной безопасности.

Кроме того, российский подход предполагает также выделение категории значимых объектов КИИ. Отношение к определенной категории значимости означает большую вероятность негативных последствий в определенной сфере и повышенные требования к титульным владельцам таких объектов.

Важность в рамках настоящего исследования представляет и понятие безопасности КИИ. В РФ, Казахстане, безопасность КИИ определяется через защищенность КИИ от внешних и внутренних угроз. В США безопасность КИИ предполагает снижение риска (а не стопроцентную защищенность).

Представляется необходимым дополнительно отметить, в целом, схожесть подходов ЕС, РФ, Казахстана и Грузии в понимании компьютерных инцидентов. Последние определяются через событие, оказывающее негативное воздействие на КИИ.

Во всех исследуемых правопорядках, за исключением ЕС, субъекты КИИ определяются через владение соответствующими объектами КИИ.

Особенностью европейского подхода является то, что в нем выделяются две категории субъектов: ОЖВУ и провайдер цифровых услуг. Под оператором жизненно-важных услуг в европейской Директиве NIS понимается государственное или частное предприятие, оказывающее услуги в определенных сферах (энергетики, транспорта, банковского дела, финансового рынка, здравоохранения, поставки питьевой воды, цифровой инфраструктуры), которые предоставляют услуги, являющиеся жизненно-важными с точки зрения поддержания важнейшей социальной и/или экономической деятельности; оказывают услуги, которые зависят от сетевых и информационных систем; возможный инцидент (например, кибератака) может оказать существенное негативное воздействие на оказание услуги. Под провайдером цифровых услуг Директива NIS понимает юридическое лицо, оказывающее цифровые услуги (Интернет-магазин, поисковик, облачный сервис).

Представляется, что ни один из анализируемых правопорядков не является идеальным для рецепции по критерию сформированности терминологического аппарата. В качестве возможной модели для терминологии в сфере КИИ может быть взят российский

подход с учётом особенностей существующего законодательства Киргизии в сфере информации и информационных технологий.

2.2. Подход ЕС к определению основных понятий: наднациональное регулирование, подход Германии и Соединенного Королевства

Основными понятиями, формирующими терминологический аппарат Директивы NIS, являются: ОЖВУ, провайдер цифровых услуг, безопасность, риск, инцидент.

Под оператором жизненно-важных услуг в Директиве NIS понимается государственное или частное предприятие, оказывающее услуги в определенных сферах (энергетики, транспорта, банковского дела, финансового рынка, здравоохранения, поставки питьевой воды, цифровой инфраструктуры), которые: предоставляют услуги, являющиеся жизненно-важными с точки зрения поддержания важнейшей социальной и/или экономической деятельности; оказывают услуги, которые зависят от сетевых и информационных систем; возможный инцидент может оказать существенное негативное воздействие на оказание услуги.

Под провайдером цифровых услуг Директива NIS понимает юридическое лицо, оказывающее цифровые услуги (Интернет-магазин, поисковик, облачный сервис).

Под безопасностью сетевых и информационных систем ст. 4 Директивы NIS понимает способность сетевых и информационных систем на заданном уровне уверенности противостоять любым действиям, угрожающим доступности, достоверности, целостности или конфиденциальности хранимых, передаваемых или обрабатываемых данных или связанных с ними услуг, предлагаемых или доступных через указанные сетевые и информационные системы.

Риск – это объективно предсказуемые обстоятельства или события, которые могут оказать отрицательное влияние на безопасность сетевых или информационных систем.

Инцидент означает любое событие, оказывающее реальное негативное влияние на безопасность сети и информационных систем.

Аналогичными терминами оперирует и Статут Соединенного Королевства о регламенте сети и информационных систем от 20.04.2018 № 506 (далее – статут № 506).

Закон ФРГ об имплементации положений Директивы 2016/1148 от 14.08.2009 (далее - BSIG) содержит определение объекта критической инфраструктуры, под которым понимается объект, установка или ее часть, относящиеся к секторам энергетики, информационных технологий, телекоммуникаций, транспорта, дорожного движения, здравоохранения, водоснабжения, питания, финансов, страхования; имеет большое значение для функционирования сообщества, потому что отказ в их работе или ухудшение их функционирования приведет к значительному дефициту поставок или угрозе для общественной безопасности.

2.3. Подход РФ к определению основных понятий

Доктрина информационной безопасности РФ в пп. з п. 2 определяет информационную инфраструктуру РФ как совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

ФЗ О безопасности КИИ в ст. 2 определяет КИИ, как объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Под объектами КИИ понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Под значимым объектом КИИ закон понимает объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры – это государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Под безопасностью КИИ закон понимает состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Под компьютерным инцидентом понимается факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

2.4. Подход США к определению основных понятий

Под критической инфраструктурой (critical infrastructure) понимаются системы и активы, физические или виртуальные, настолько жизненно важные для США, что нарушение функционирования или разрушение таких систем и активов окажет разрушительное влияние на безопасность, национальную экономическую безопасность, национальное здравоохранение или охрану здоровья или любое сочетание этих вопросов[27].

HSPD-7[28] уточнила последствия потери критического актива, что, среди прочего, включает катастрофические для здоровья последствия или массовые потери, сравнимые с последствиями применения оружия массового уничтожения; ослабление способности федеральных агентств выполнять важные задачи или обеспечивать здоровье и безопасность населения; подрыв способностей государственного и местного правительства поддерживать порядок и предоставлять минимально необходимые общественные услуги; причинение ущерба способности частного сектора обеспечить упорядоченное функционирование экономики; оказание негативного влияния на экономику через каскадное нарушение других инфраструктур и иное.

Термин «система национальной безопасности» имеет значение, данное ему в Федеральном законе об управлении информационной безопасностью 2002 года (44 США

[27] Section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)). URL: https://www.law.cornell.edu/uscode/text/42/5195c (дата обращения: 30.06.2019).

[28] Впоследствии Директива HSPD-7 была заменена Директивой PDD-21.

355 (b)), а именно означает любую информационную систему (включая любую телекоммуникационную систему), используемую или управляемую агентством или подрядчиком агентства или другой организацией от имени агентства, (i) функция, действие или использование которых (I) включает в себя разведывательную деятельность; (II) включает в себя криптологическую деятельность, связанную с национальной безопасностью; (III) включает в себя командование и контроль над вооруженными силами; (IV) включает в себя оборудование, которое является неотъемлемой частью оружия или системы оружия; или же (V) с учетом подпункта (B), имеет решающее значение для непосредственного выполнения военных или разведывательных задач; или же (ii) всегда защищена процедурами, установленными для информации, которая была специально разрешена в соответствии с критериями, установленными исполнительным распоряжением или актом Конгресса, для сохранения в секрете в интересах национальной обороны или внешней политики[29].

Под устойчивостью понимается способность подготовиться к изменяющимся условиям и адаптироваться к ним, а также выдерживать и быстро восстанавливаться после сбоев. Устойчивость включает в себя способность противостоять и восстанавливаться после преднамеренных атак, аварий или естественных угроз или инцидентов.

Термины «безопасный» и «безопасность» относятся к снижению риска для критически важной инфраструктуры с помощью физических средств или защитных кибер-мер в отношении вторжений, атак или последствий стихийных бедствий или техногенных катастроф.

2.5. Подход Грузии к определению основных понятий

Под критической информационной системой в Грузии понимается информационная система, непрерывное функционирование которой имеет важное значение для обороны и (или) экономической безопасности страны, нормального функционирования органов государственной власти или общества.

Информационная безопасность – это деятельность, обеспечивающая соблюдение правил доступа, единства, аутентичности, конфиденциальности информации и информационных систем и их работы в течение длительного времени.

Под компьютерным инцидентом понимается 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.

В качестве субъекта критической информационной системы предлагается государственный орган или юридическое лицо, непрерывное функционирование информационной системы которого имеет важное значение для обороны и (или) экономической безопасности страны, сохранения государственной власти или общественной жизни.

2.6. Подход Казахстана к определению основных понятий

[29] При этом, подпункт (A) (i) (V) не включает систему, которая должна использоваться для рутинных административных и бизнес-приложений (включая приложения для расчета заработной платы, финансов, логистики и управления персоналом). The Federal Information Security Management Act of 2002 (44 U.S.C. 3542(b)). https://www.law.cornell.edu/uscode/text/44/3542#google_vignette (дата обращения: 15.05.2019).

Под информационной инфраструктурой понимается совокупность технических средств и систем формирования, создания, преобразования, обработки, передачи, использования и хранения информации[30].

Под критически важными объектами информационно-коммуникационной инфраструктуры в Казахстане понимаются объекты информационно-коммуникационной инфраструктуры, в том числе информационно-коммуникационной инфраструктуры «электронного правительства», нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории.

Информационная безопасность в сфере информатизации - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Событие информационной безопасности – это состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации[31].

2.7. Подход Сингапура к определению основных понятий

Закон о кибербезопасности Сингапура определяет критическую информационную инфраструктуру как компьютер или компьютерную систему, которая необходима для непрерывного предоставления основных услуг, связанных с утратой или негативным воздействием на национальную безопасность, оборону, международные отношения, экономику, общественного здравоохранения, общественной безопасности или общественного порядка Сингапура[32].

2.8. Подход КНР к определению основных понятий

Национальная стратегия кибербезопасности Китая содержит положение, согласно которому национальная критическая информационная инфраструктура относится к национальной безопасности, национальной экономике и средствам существования людей в сферах, включающих информационные сети, энергетику, финансы, транспорт, образование, научные исследования, охрану водных ресурсов, промышленное производство, медицину и здравоохранение, социальное обеспечение, коммунальные услуги и другие важные информационные системы[33].

2.9. Подход Японии к определению основных понятий

В законодательстве Японии закреплено понятие кибербезопасности, под которой понимаются условия, при которых принимаются меры, необходимые для предотвращения утечки, потери или повреждения, а также для другого управления безопасностью

[30] Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан».

[31] Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 11.04.2019 г.).

[32] Cybersecurity Bill 2017 // URL: https://www.csa.gov.sg/~/media/csa/cybersecurity_ bill/draft_cybersecurity_bill_2017.ashx (дата обращения: 30.06.2019).

[33] National cyberspace security strategy (网络空间安全战略) December 2016 // URL: http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html (дата обращения: 30.06.2009).

информации, которая записывается, отправляется, передается или принимается с использованием электронного метода, магнитного метода или любого другого метода, не распознаваемого человеческими чувствами.

3. Принципы

3.1. Принципы: сравнительно-правовой анализ

Наиболее распространенными для исследуемых правопорядков принципами в сфере обеспечения безопасности КИИ являюся:

- законность (РФ, Казахстан, КНР);
- уважение прав и свобод человека и гражданина в информационной сфере (Казахстан, Япония);
- взаимодействие субъектов КИИ и ОГВ, при четком разграничении полномочий последних (РФ, США, Казахстан, Япония);
- приоритет предотвращения кибератак (РФ, Казахстан).

На основе комплексного анализа законодательства различных государств можно предложить следующий оптимальный набор принципов:

- законность;
- приоритет прав и свобод человека и гражданина при осуществлении правовых, организационных и технических мер защиты КИИ;
- пропорциональность (баланс интересов государства, общества, и частных лиц);
- риск-ориентированный подход при категорировании КИИ и установлении требований к субъектам КИИ;
- приоритет прогнозирования и предотвращения атак на объекты КИИ (превентивный приоритет);
- четкое разграничение полномочий ОГВ или создание единого регулятора;
- оперативное взаимодействие субъектов КИИ и уполномоченных ОГВ;
- транспарентность (определенность и доступность) предъявляемых к субъектам КИИ требований;
- непротиворечивость предъявляемых к субъектам КИИ требований;
- конфиденциальность и уважение бизнес-интересов;
- комплексный подход к вопросам кибербезопасности;
- учет интересов всех заинтересованных сторон (мультистейкхолдеризм);
- интеграция системы обеспечения национальной безопасности с международными системами безопасности;
- поощрение субъектов КИИ за исполнение требований в сфере защиты КИИ.

3.2. Подход ЕС к принципам регулирования в сфере ЖВУ: наднациональное регулирование, подход Германии и Соединенного Королевства

К конкретным институциональным принципам, которые относятся к отдельным аспектам регулирования в сфере КИИ в странах ЕС, необходимо, прежде всего, отнести принципы, относящиеся к принимаемым мерам безопасности по Директиве ЕС NIS, а именно:

- эффективность (effectiveness);
- совместимость (compatibility);

- пропорциональность рискам (proportionality);
- конкретность и понятность (concreteness);
- возможность проверки (verifiability)[34].

На основании комплексного анализа положений Директивы можно косвенно выделить следующие общие принципы регулирования КИИ в ЕС:

- приоритет прав и свобод, установленных Хартией Европейского Союза об основных правах[35] (указанное следует, в частности из п. 75 Преамбулы);
- субъектно-деятельностный подход (Директива концентрируется не на описании конкретных объектов КИИ, а на описании субъектов, сфер их деятельности);
- учет направленности деятельности (указанное следует, в частности из п. 65 Преамбулы);
- риск-ориентированный подход (это следует, в частности из п. 44 Преамбулы);
- конфиденциальность и уважение бизнес-интересов (вывод следует, в частности из ст. 14, 16);
- пропорциональность (указанное следует, в частности из п. 59, 74 Преамбулы).
- установление минимального уровня гарантий, с возможностью их повышения (принцип вытекает из ст. 5 Директивы);
- комплексный подход к вопросам кибербезопасности;
- учет интересов всех заинтересованных сторон.

3.3. Подход РФ к принципам регулирования в сфере КИИ

Принципы обеспечения безопасности КИИ содержатся в ст. 4 ФЗ О безопасности КИИ. Среди таковых необходимо отметить:

- принцип законности;
- принцип непрерывности и комплексности обеспечения безопасности критической информационной инфраструктуры;
- принцип взаимодействия ФОИВ и субъектов КИИ;
- приоритет предотвращения компьютерных атак.

3.4. Подход США к принципам регулирования в сфере КИИ

Законодательные акты США не выделяют, как таковые, принципы регулирования в сфере безопасности КИИ. При этом, один из ключевых документов - PPD-21[36] устанавливает три следующих стратегических императива, которые должны стимулировать правительство к укреплению безопасности и устойчивости критической инфраструктуры:

- уточнение функциональных отношений между федеральным правительством для продвижения национального единства усилий по укреплению безопасности и устойчивости критической инфраструктуры;

---

[34] Reference document on security measures for Operators of Essential Services CG Publication 01/2018. URL: http://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document___security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (дата обращения: 30.06.2019).

[35] Charter of Fundamental Rights of the European Union. 2012. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (дата обращения: 30.06.2019).

[36] Presidential Policy Directive - Critical Infrastructure Security and Resilience PPD-21. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (дата обращения: 21.05.2019).

- обеспечение эффективного обмена информацией путем определения базовых данных и системных требований для федерального правительства;
- внедрение функции интеграции и анализа для информирования о планировании и принятии операционных решений в отношении критически важной инфраструктуры.

3.5. Подход Казахстана к принципам регулирования в сфере КИИ

В законодательстве Казахстана непосредственно не закреплены принципы обеспечения безопасности КИИ. Возможно отметить общие принципы национальной безопасности, релевантные для сферы КИИ:

- соблюдение законности при осуществлении деятельности по обеспечению безопасности;
- приоритет прав и свобод человека и гражданина;
- оперативное взаимное информирование и согласованность действий сил обеспечения безопасности;
- приоритетность предупредительно-профилактических мер при обеспечении безопасности;
- своевременность и адекватность мер обеспечения безопасности масштабам и характеру нанесенного и (или) потенциального ущерба;
- соблюдение баланса интересов человека и гражданина, общества и государства, их взаимная ответственность;
- четкое разграничение полномочий государственных органов.

3.6. Подход КНР к принципам регулирования в сфере КИИ

В законодательстве Китая принципам регулирования КИИ уделено особое внимание. Вместе с тем, в отличие от ранее перечисленных подходов китайское законодательство в основном акцентирует внимание на международно-правовом аспекте.

Существует четыре основных принципа в регулирования указанной сферы[37]:

- уважение к сохранению суверенитета киберпространства. Суверенитет в киберпространстве неприкосновенен. Признается право стран выбирать свой собственный путь развития, модель управления сетью, публичную политику в Интернете и равное участие в международном управлении киберпространством. Сетевые вопросы в рамках суверенитета каждой страны являются обязанностью людей каждой страны. Каждая отдельная страна имеет право формулировать законы и нормативные акты, касающиеся киберпространства, в соответствии со своими национальными условиями и опираться на международный опыт, а также принимать необходимые меры для управления своими собственными информационными системами и сетевыми действиями на своей собственной территории. Национальные информационные системы и информационные ресурсы защищены от вторжения, вмешательства, атак и разрушений, гарантируют законные права и интересы граждан в киберпространстве, предотвращают и наказывают за распространение вредоносной информации, которая угрожает национальной безопасности и интересам;
- мирное использование киберпространства. Все страны должны соблюдать принцип Устава ООН о неприменении силы или угрозы применения силы. Страны должны

[37] Закон о кибербезопасности КНР URL: http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm (дата обращения: 01.07.2019).

совместно противостоять гонке вооружений в киберпространстве и предотвращать конфликты в киберпространстве;

- управление киберпространством в соответствии с законом. Китай провозглашает готовность всесторонне продвигать верховенство закона в киберпространстве, придерживаться принципа верховенства права, создавать сети в соответствии с законом и осуществлять доступ к Интернету в соответствии с законом, чтобы Интернет мог функционировать правильным образом на основе принципа верховенства права. Любая организация или частное лицо, которые пользуются свободой и осуществляют права в киберпространстве, должны соблюдать закон, уважать права других и нести ответственность за свои действия в Интернете;
- координация безопасности и развития сети.

Подход Японии к принципам регулирования в сфере КИИ

В сентябре 2015 г. Японский кабинет министров одобрил вторую «Стратегию кибербезопасности», которая весьма показательно демонстрирует, какую важность руководство страны придаёт вопросам кибербезопасности. Разработка стратегии 2015 г. велась на основе положений «Основного закона о кибербезопасности» 2014 г., который основывается на четырёх принципах, формирующих политику Японии в этой области:

- свободное перемещение информации;
- уважение к правам граждан;
- соблюдение интересов всех заинтересованных сторон;
- сотрудничество субъектов КИИ.

В Основном законе о кибербезопасности определяются принципы регулирования относительно операторов КИИ:

- операторы КИИ должны реализовать меры для КИИ под свою ответственность;
- необходимо развивать чувство безопасности в общественном и социальном развитии, укреплять устойчивость и международную конкурентоспособность посредством сотрудничества между правительством и частным сектором.

4. Предмет регулирования

4.1. Предмет регулирования: сравнительно-правовой анализ

В ходе проведенного анализа было выявлено несколько подходов к определению предмета регулирования в сфере КИИ (ЖВУ):

- объекты КИИ (РФ, Казахстан, Германия);
- субъекты и их деятельность (ЕС кроме Германии, Грузия, Сингапур, Китай, Япония).

Субъектно-деятельностный подход к определению предмета регулирования является более продвинутым (так как объект может принадлежать конкретному лицу, но не использоваться, следовательно, ущерб объекту не окажет существенного влияния). Вместе с тем, на ранних этапах развития соответствующего законодательства, с целью упрощения осуществления категорирования рекомендуется использовать объектный подход.

Дополнительно отметим, что вне зависимости от различий при определении объекта регулирования потенциальный конечный результат предполагается аналогичным.

4.2. Подход ЕС к предмету регулирования: наднациональное регулирование, подход Германии и Соединенного Королевства

Предметом регулирования Директивы NIS являются ОЖВУ и провайдеры цифровых услуг, а также непосредственно ЖВУ. Предмет регулирования британского статута № 506 аналогичен.

Предметом регулирования BSIG (Германия) являются объекты критическо-важных услуг и критическо-важные услуги.

4.3. Подход РФ к предмету регулирования

Предметом регулирования указанного закона являются объекты КИИ. Под объектом КИИ закон понимает:

- информационные системы;
- информационно-телекоммуникационные сети;
- автоматизированные системы управления субъектов критической информационной инфраструктуры.

Также закон выделяет категорию значимых объектов КИИ, под которыми понимаются объекты критической информационной инфраструктуры, которым присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры. К таким объектам предъявляются повышенные требования, по сравнению с обычными объектами КИИ. Если по результатам категорирования объект можно отнести к значимому, то собственнику необходимо будет реализовать систему безопасности для защиты данных объектов в соответствии с нормативными документами ФСТЭК.

4.4. Подход Грузии к предмету регулирования

Предметом регулирования законодательства Грузии в сфере КИИ являются субъекты КИИ.

4.5. Подход Казахстана к предмету регулирования

Предметом регулирования законодательства Казахстана в сфере КИИ являются объекты КИИ.

5. Критерии отнесения к КИИ/ категорирование

5.1. Критерии отнесения к КИИ. Категорирование объектов (услуг): сравнительно-правовой анализ

В правопорядках, в которых господствует объектный подход к КИИ (например, РФ, Германия, Казахстан) четко выделяются критерии отнесения объектов к КИИ и присвоения им определенной категории. Среди общих критериев можно назвать:

- объект относится к определенной сфере / имеет значимость для определенной сферы (социальная, политическая, экономическая, экологическая и другая);
- достижение предписанного НПА порогового значения определенного показателя, которое характеризует возможный ущерб (для РФ и Германии).

Подход РФ и Германии, в части установления конкретных критериев категорирования, точных пороговых значений для объектов КИИ, представляется наиболее удачным. При этом, дифференциация пороговых значений для отнесения объектов к разным категориям значимости, характерная для российского подхода представляется оптимальным решением в указанной области.

Без установления четких критериев, отдавая определение категории объекта на усмотрение государственного органа или самого лица – владельца объекта КИИ затруднительно добиться конкретного результата – защищенности объектов КИИ от потенциальных угроз. Расширение дискреционных полномочий ОГВ, вне четких критериев представляет собой коррупциогенный фактор. Расширение степени усмотрения бизнеса, вне установления четких критериев ведет к игнорированию публичных интересов, к достижению крайне низкого уровня защищенности объектов КИИ (в тех случаях, когда сама компания не считает необходимым предпринимать эффективные меры по их защите).

5.2. Подход ЕС к критериям определения ЖВУ: наднациональное регулирование, подход Германии и Соединенного Королевства

В Директиве NIS установлен субъектно-деятельностный подход, следовательно, внимание на объектах КИИ конкретно не акцентируется. Критерии отнесения объекта к КИИ не установлено. Категорирование производится в отношении ОЖВУ и их деятельности. Аналогичного подхода придерживается и британский статут № 506.

Вместе с тем, обратный подход можно встретить, например, в ФРГ. Так, согласно п. 10 раздела 2 Закона BSIG под объектами критической инфраструктуры понимаются объекты, установки или их части, которые:

- относятся к секторам энергетики, информационных технологий, телекоммуникаций, транспорта, дорожного движения, здравоохранения, водоснабжения, питания, финансов, страхования;
- имеют большое значение для функционирования сообщества, потому что отказ в их работе или ухудшение их функционирования приведет к значительному дефициту поставок или угрозе для общественной безопасности.

Конкретные объекты и виды деятельности установлены Указом об определении критических инфраструктур, в соответствии с Законом BSIG (ред. От 21.06.2017). Указ делит все объекты по критерию отнесения им к одной из соответствующих сфер: энергетики, водоснабжения, питания, информационных технологий и телекоммуникаций, здравоохранения, финансов, страхования, транспорта.

Указ определяет и критическо-важные услуги (то есть деятельность) для каждой сферы. Например, в сфере IT такие критически-важные услуги представлены: передачей голоса и данных, хранением и обработкой данных. В сфере IT объектами критической инфраструктуры являются: сети передачи данных, IXP, официальные DNS-серверы, центры обработки данных, сети доставки контента. При этом, для каждого вида и подвида объекта критической инфраструктуры определены так называемые «пороговые значения» по количеству пользователей, территории, по иным показателям. Только при соблюдении этих двух критериев: предметного и количественного, объект приобретает статус объекта критической инфраструктуры.

Выдержки из таблицы с примерами пороговых значений для сектора IT и телекоммуникаций приведены ниже.

№.	Категория КВУ или объекта КВУ	Критерий	Пороговое значение
1.	**Голосовая связь и передача данных**		
1.1	Доступ		

1.1.1	Сети локального доступа, обеспечивающие общедоступные услуги телефонной связи и сетям передачи данных.	Число клиентов сети локального доступа	100 000 чел.
1.2.	Передача голосового сигнала и данных		
1.2.1	Передающие сети, поддерживающие общедоступные услуги телефонной связи и передачи данных, а также услуги доступа к Интернету (не включается пункт 1.1.1)	Количество пользователей соответствующей услуги	100 000 чел.
1.3	Обмен трафика		
1.3.1	Точки обмена трафиком (IXP) для общедоступных услуг телефонной связи, сервисов передачи данных и услуг доступа к Интернету	Среднегодовое количество подключенных АС (автономных систем)	300 АС
1.4.	Управление DNS		
1.4.1	DNS-резолверы, используемые для поддержки общедоступных услуг телефонной связи, сервисов передачи данных и услуг доступа к Интернету.	Количество DNS-запросов (среднегодовое)	2 500 000 запросов
1.4.2	Авторитативные доменные серверы DNS, используемые для поддержки общедоступных услуг телефонной связи, сервисов передачи данных и услуг доступа к Интернету.	Количество доменов, для которых сервер является авторитативным или на который делегирована доменная зона	250 000 доменов
2.	**Хранение и обработка данных**		
2.1	Инфраструктурные площадки для хранения данных		
2.1.1	Дата-центры	Законтрактованная мощность в МВт (по состоянию на 30 июня календарного года)	5 МВт
2.2.	Предоставление мощностей для размещения и хранения данных		
2.2.1	Серверные парки	Количество находящихся в эксплуатации серверов (среднегодовое)	25 000 серверов
2.2.2	Сети доставки контента (CDN)	Объем передаваемых данных (терабайт в год)	75 000 ТБ
2.3.	Выпуск цифровых сертификатов		

2.3.1	Удостоверяющие центры	Количество выпущенных квалифицированных цифровых сертификатов	500 000 сертификатов
		Количество сертификатов для аутентификации общедоступного сервера (серверные сертификаты, например, для веб-серверов, серверов электронной почты, облачных сертификатов (включая сертификаты TLS/SSL).	10 000 сертификатов

Стоит также отметить, что, противоположный немецкому (в части регулирования ОЖВУ, но не объектов КИИ) английский подход также устанавливает «пороговые значения» (для операторов жизненно-важных услуг). Так, например, для подсектора цифровой инфраструктуры, в отношении IXP установлено значение в 50 процентов доли соответствующего рынка. Следовательно, для того чтобы такой оператор подпадал под действие настоящего акта, необходимо соблюдение также предметного и количественного критериев.

5.3. Подход РФ к критериям определения объектов КИИ

ФЗ О безопасности КИИ в ст. 7 устанавливает основные требования к категорированию объектов КИИ.

Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

При категорировании учитываются следующие критерии:

- социальная значимость (возможный ущерб жизни и здоровью людей; прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи; отсутствие доступа к государственной услуге);
- политическая значимость (возможное причинение ущерба интересам РФ в вопросах внутренней и внешней политики);
- экономическая значимость (возможное причинение прямого и косвенного ущерба субъектам КИИ и (или) бюджетам Российской Федерации);
- экологическая значимость (воздействие на окружающую среду).
- значимость для обороны страны, безопасности государства и правопорядка.

С учетом этих критериев устанавливаются 3 категории значимости.

Конкретная категория значимости устанавливается субъектом КИИ, который образует специальную постоянно действующую комиссию по категорированию. Максимальный срок категорирования не должен превышать 1 год. Категорирование

проводится не реже чем один раз в пять лет. Субъект КИИ уведомляет об этом уполномоченный орган в течение 10 дней. Категория значимости может быть изменена.

Также предусмотрено определение категории значимости строящегося объекта.

В качестве исходных данных для категорирования принимаются:

- сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);
- осуществляемые процессы;
- состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;
- декларация промышленной безопасности опасного производственного объекта;
- сведения о взаимодействии (зависимости) объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры;
- угрозы безопасности информации[38].

Постановлением Правительства от 08.02.2018 № 127 также утвержден Перечень показателей критериев значимости объектов КИИ и их значений по 3 категориям.

Показатель		**Значение показателя**		
		III категория	**II категория**	**I категория**
I. Социальная значимость				
1.	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения оцениваемые:			
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	в пределах территории одного муниципального образования (численностью от 2 тыс. человек)	выход за пределы территории одного муниципального образования (численностью от 2 тыс. человек)	выход за пределы территории одного субъекта Российской Федерации или территории города

[38] Постановление Правительства РФ «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» от 08.02.2018 N 127 // СПС Консультант плюс.

		или одной внутригородской территории города федерального значения	или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	федерального значения
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 2, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:			
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	в пределах территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения

			Федерации или территории города федерального значения	
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 2, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
4.	Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи (тыс. человек)	более или равно 3, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее или равно 6
II. Политическая значимость				
6.	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения	прекращение или нарушение функционирования федерального органа государственной власти	прекращение или нарушение функционирования Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального

				Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации
7.	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	нарушение условий договора межведомственного характера (срыв переговоров или подписания)	нарушение условий межправительственного договора (срыв переговоров или подписания)	нарушение условий межгосударственного договора (срыв переговоров или подписания)
III. Экономическая значимость				
8.	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим	более или равно 1, но менее или равно 10	более 10, но менее или равно 20	более 20

	акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период)			
9.	Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
10.	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры,	более 3, но менее или равно 70	более 70, но менее или равно 120	более 120

	являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)			
IV. Экологическая значимость				
11.	Вредные воздействия на окружающую среду, оцениваемые:			
	а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	в пределах территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города	выход за пределы территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом вредных

		федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры	федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры	воздействий за пределы территории субъекта критической информационной инфраструктуры
	б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	более или равно 2, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
12.	Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра	прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта Российской Федерации или города федерального значения	прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации	прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента Российской Федерации, Правительства Российской Федерации,

				Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации
13.	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое:			
	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	более 0, но менее или равно 10	более 10, но менее или равно 15	более 15
	б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	более 0, но менее или равно 10	более 10, но менее или равно 40	более 40
14.	Прекращение или нарушение функционирования (невыполнение установленных показателей)	менее или равно 4, но более 2	менее или равно 2, но более 1	менее или равно 1

	информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемые в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)			

5.4. Подход США к критериям определения объектов КИИ

США не выделяют отдельных критериев отнесения к КИИ. Директива PPD-21 определяет, что под термином «все опасности» («all hazards») понимаются угроза или инцидент, природный или техногенный, который оправдывает действия по защите жизни, имущества, окружающей среды, здоровья и безопасности населения и минимизации сбоев в государственной, социальной или экономической деятельности.

Термин включает в себя стихийные бедствия, кибер-инциденты, промышленные аварии, пандемии, террористические акты, саботаж и разрушительную преступную деятельность, направленную на критически важную инфраструктуру.

На основании данного термина, а также определения «критической инфраструктуры» Директива PPD-21 определила 16 критических секторов инфраструктуры и установила соответствующие федеральные отраслевые агентства (Sector-Specific Agencies). В некоторых случаях совместные отраслевые агентства назначаются, когда эти департаменты разделяют роли и обязанности SSA. Критически важные сектора могут быть изменены, если этого потребуют объективные обстоятельства. По этим вопросам Министр национальной безопасности (Secretary of Homeland Security) должен периодически оценивать необходимость и утверждать изменения в критически важных секторах инфраструктуры и консультироваться с помощником Президента США по национальной безопасности и противодействию терроризму, прежде чем изменять критически важный сектор инфраструктуры или назначенное отраслевое агентство для этого сектора.

5.5. Подход Грузии к критериям определения объектов КИИ

Критерии категорирования объектов в грузинском законе не выделяются, однако определяются критерии категорирования субъектов КИИ. При составлении списка субъектов 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 и (или) 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.

5.6. Подход Казахстана к критериям определения объектов КИИ

В соответствии с Постановлением Правительства Республики Казахстан от 8 сентября 2016 года № 529 определяются следующие критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры:

- влияние объекта информационно-коммуникационной инфраструктуры на непрерывную эксплуатацию особо важных государственных объектов, при нарушении функционирования которого будет остановлена деятельность особо важных государственных объектов;
- влияние объекта информационно-коммуникационной инфраструктуры на непрерывную и безопасную эксплуатацию стратегических объектов, при нарушении функционирования которого будет остановлена деятельность стратегических объектов либо возникает угроза чрезвычайной ситуации техногенного характера;
- влияние объекта информационно-коммуникационной инфраструктуры на непрерывную и безопасную эксплуатацию объектов отраслей экономики, имеющих стратегическое значение, при нарушении функционирования которого будет остановлена деятельность объектов отраслей экономики, имеющих стратегическое значение, либо возникает угроза чрезвычайной ситуации техногенного характера;
- влияние объекта информационно-коммуникационной инфраструктуры на обеспечение устойчивого функционирования объекта информатизации «электронного правительства» и иных информационно-коммуникационных услуг, частичное или полное нарушение (прекращение) функционирования которых может привести к чрезвычайной ситуации социального характера[39].

6. Сферы обеспечения безопасности КИИ

6.1. Сферы обеспечения безопасности КИИ (ЖВУ): сравнительно-правовой анализ

Правопорядки ЕС, в частности Великобритании и Германии, а также РФ, США, Казахстан, Япония, Китай, Сингапур выделяют ряд сфер обеспечения безопасности КИИ (ЖВУ). Среди общих можно назвать:

1. транспорт (кроме КНР);
2. энергетика (кроме КНР);
3. здравоохранение (кроме Казахстана);
4. банковский сектор и финансовый рынок (кроме КНР и Казахстана);
5. IT и связь (кроме Казахстана);
6. водоснабжение и поставки питьевой воды (кроме Казахстана, РФ, КНР);
7. химическая промышленность (кроме Казахстана, Сингапура, Японии, ЕС).

Конкретный список сфер зависит от того, какие отрасли являются наиболее значимыми для указанного государства с экономической и социальной точек зрения.

[39] Постановление Правительства Республики Казахстан от 8 сентября 2016 года № 529.

6.2. Подход ЕС к сферам обеспечения безопасности ЖВУ: наднациональное регулирование, подход Германии и Соединенного Королевства

Директива NIS выделяет следующие основные сферы, в которых осуществляют деятельность ОЖВУ:

1. энергетика;
2. транспорт;
3. банковское дело;
4. финансовый рынок;
5. здравоохранение;
6. поставки питьевой воды;
7. цифровая инфраструктура.

Британский статут № 506 выделяет аналогичные сферы. Также британский статут выделяет и отдельные секторы, в рамках выделенных сфер.

Немецкий BSIG и соответствующий Указ выделяют дополнительно сферы: питания, IT и телеком.

6.3. Подход РФ к сферам обеспечения безопасности КИИ

ФЗ О безопасности КИИ выделяет 5 общих сфер: социальная, экономическая, политическая, экономическая, экологическая, безопасность и правопорядок.

Исходя из анализа ФЗ О безопасности КИИ можно выделить следующие конкретные секторы:

1) здравоохранение;
2) наука;
3) транспорт;
4) связь;
5) энергетика;
6) банковская сфера и финансовый рынок;
7) ТЭК;
8) атомная энергетика;
9) оборона;
10) ракетная промышленность;
11) горнодобыча;
12) металлургия;
13) химическая промышленность.

6.4. Подход США к сферам обеспечения безопасности КИИ

На сегодняшний день в США определены следующие критически важные сектора инфраструктуры:

1) химический сектор;
2) сектор коммерческих объектов;
3) сектор коммуникаций;
4) сектор критического производства;
5) плотины;
6) военно-промышленная база;
7) аварийно-спасательные службы;
8) энергетика;

9) финансовые услуги;
10) продовольствие и сельское хозяйство;
11) государственные учреждения;
12) здравоохранение и общественное здоровье;
13) информационные технологии;
14) ядерные реакторы, материалы и отходы;
15) транспортные системы;
16) системы водоснабжения, сбора и отведения сточных вод.

Кроме того, необходимо отметить две области, в которых также сосредоточены усилия по обеспечению безопасности КИИ, но которые при этом не относятся к конкретным секторам, а носят внеотраслевой характер — это кибербезопасность и безопасность информации.

Кибербезопасность не выделена как самостоятельный сектор инфраструктуры, подлежащий защите. Тем не менее, происходящие в последнее десятилетие киберинциденты затрагивали системы и данные как государственного, так и частного секторов США. Частота этих атак и их влияние на экономику США и, как следствие, высокая значимость, которую США придает вопросам кибербезопасности, привели к регулярному обсуждению данных проблем в Конгрессе США[40].

Информация о критической инфраструктуре защищается через принятие различных федеральных программ. Одним из ключевых актов в данной отрасли является Программа защищенной информации о критической инфраструктуре (PCII) в соответствии с Законом об информации о критической инфраструктуре (CII) 2002 года, целью которой явилась защита информации об инфраструктуре частного сектора, добровольно передаваемой правительству в целях внутренней безопасности.

6.5. Подход Казахстана к сферам обеспечения безопасности КИИ

В законодательстве Казахстана выделяются следующие сферы обеспечения безопасности КИИ:

1. государственные услуги;
2. транспорт;
3. нефтегазовая сфера;
4. космическая сфера;
5. энергетика;
6. металлургия.

6.6. Подход Сингапура к сферам обеспечения безопасности КИИ

Законодательство Сингапура в исследуемой сфере выделяет одиннадцать важнейших секторов основных услуг:

1. энергетика;
2. информационные коммуникации;
3. водоснабжение;

[40] Так, согласно Исследовательской службе Конгресса, Конгресс принял пять законов, связанных с кибербезопасностью, на 113-м Конгрессе и дополнительный закон на 114-м Конгрессе. Конгресс также провел 119 слушаний по вопросам, связанным с кибербезопасностью, в ходе 114-го Конгресса. Белый дом издал президентские действия по кибербезопасности, связанные с кибербезопасностью критической инфраструктуры, обменом информацией и санкциями в ответ на злонамеренную кибер-деятельность. Congressional Research Service. Cybersecurity: Selected Issues for the 115th Congress. URL. https://fas.org/sgp/crs/misc/R45127.pdf (дата обращения: 30.06.2019).

4. здравоохранение;
5. банковское дело и финансы;
6. охранные и аварийные службы;
7. авиация;
8. наземный транспорт;
9. морской транспорт;
10. правительство;
11. средства массовой информации.

6.7. Подход КНР к сферам обеспечения безопасности КИИ

Законодательство КНР в соответствующей сфере предусматривает следующие области регулирования КИИ:

- отрасли: здравоохранение, образование, социальное обеспечение и защита окружающей среды;
- информационные сети: радио и телевизионные сети, интернет; поставщики услуг, предоставляющие облачные вычисления, большие данные и другие крупные общедоступные информационные и сетевые услуги;
- научные исследования и производство: оборонная промышленность, тяжелая промышленность, нефтехимическая и пищевая и фармацевтическая промышленность;
- СМИ и новости: радиостанции, телевизионные станции и службы новостей.

6.8. Подход Японии к сферам обеспечения безопасности КИИ

В Японии выделяются следующие секторы:

1. информационные и коммуникационные технологии;
2. финансовый сектор;
3. авиация;
4. железнодорожное сообщение;
5. электричество;
6. газ;
7. деятельность Правительства и государственных служб (включая местные органы власти);
8. медицина;
9. водоснабжение;
10. логистика.

7. Невластные субъекты обеспечения безопасности КИИ, их правовой статус

7.1. Субъекты в сфере КИИ (ЖВУ), их правовой статус: сравнительно-правовой анализ

Наиболее развитыми правопорядками по критерию регулирования правового статуса субъектов КИИ (ОЖВУ) являются ЕС, РФ, Казахстан.

В ЕС субъекты делятся на 2 вида: ОЖВУ и провайдеры цифровых услуг. К последним предъявляются меньшие требования по обеспечению безопасности объекта.

В РФ Закон о КИИ разделяет субъектов на 2 вида: титульные владельцы объектов КИИ (лица которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети,

автоматизированные системы управления, функционирующие в обозначенных выше сферах) и лица, обеспечивающие взаимодействие систем и сетей. Владельцы объектов КИИ делятся на 2 вида: владельцы обычных объектов КИИ и значимых объектов 1,2 и 3 категории.

Среди обязанностей невластных субъектов, являющихся общими для указанных правопорядков, следует выделить:

- мониторинг угроз и управление рисками (в РФ данные обязанности осуществляются в процессе категорирования объекта КИИ);
- информирование уполномоченного органа о компьютерных инцидентах;
- взаимодействие с уполномоченными органами, предоставление им необходимой информации.

Особенностью российского подхода является обязанность субъектов КИИ по осуществлению категорирования объекта для определения его значимости и тех мер, которые необходимо предпринять для защиты такового от угроз.

Особенностью европейского подхода является необходимость подтверждения достаточности предпринятых мер путем проведения аудита безопасности и предоставления его результатов в уполномоченный орган (указанные меры проводятся на предварительной стадии в рамках российского подхода при осуществлении категорирования). В целом, европейский подход является воплощением принципа риск-ориентированности (целесообразность принимаемых мер защиты) и требует осуществления лишь минимально-необходимых мер в каждом конкретном случае.

Представляется разумным обратить внимание на дифференциацию субъектов по российской и европейской моделям. Основные обязанности могут быть восприняты из российского закона и адаптированы под нужды Киргизии. Риск-ориентированный подход применим, однако, он не должен вносить неопределенность в правовой статус субъектов КИИ.

7.2. Подход ЕС к определению ОЖВУ и провайдеров цифровых услуг: наднациональное регулирование, подход Германии и Соединенного Королевства

Директива выделяет две категории обязанных субъектов: ОЖВУ и провайдер цифровых услуг.

Под оператором жизненно важных услуг (OES) п. 4 ст. 1 Директивы NIS понимает государственные или частные предприятия в определенных сферах (энергетики, транспорта, банковского дела, финансового рынка, здравоохранения, поставок питьевой воды, цифровой инфраструктуры), которые: предоставляют услуги, являющиеся жизненно-важными с точки зрения поддержания важнейшей социальной и/или экономической деятельности; оказывают услуги, которые зависят от сетевых и информационных систем; возможный инцидент может оказать существенное негативное воздействие на оказание услуги.

Общая классификация таких инцидентов приводится координационной группой (CG). Также указанный орган предложил конкретные машиночитаемые теги, относящиеся к соответствующей классификации инцидентов, для использования в программном коде. Указанные теги будут использоваться для прикрепления к соответствующим файлам с

целью классификации природы и воздействия инцидента (в соответствии с разработанной таксономией)[41].

Критерий существенности негативного воздействия инцидента, в соответствии со ст. 6 Директивы NIS, определяются государствами-членами самостоятельно. При этом, нужно учитывать следующие межотраслевые факторы:

- количественный фактор (количество пользователей услуги, предоставляемой заинтересованной организацией);
- фактор отраслевой зависимости (зависимость других вышеуказанных отраслей, от услуги, предоставляемой этой организацией);
- фактор влияния инцидента (тяжесть и длительность влияния, которое инцидент может оказать на экономическую и социальную деятельность и общественную безопасность). В п. 27 Преамбулы Директивы ЕС 2016/1148 отмечено, что при оценке возможного воздействия инцидента на социально-экономическую деятельность или общественную безопасность с точки зрения его масштаба и продолжительности государства-члены ЕС также должны оценивать, сколько пройдет времени, прежде чем перерыв начнет оказывать отрицательное воздействие;
- рыночный фактор (доля, которую организация занимает на рынке организация). Преамбула в п. 26 содержит положение, согласно которому для определения значимости идентифицированного оператора жизненно-важных услуг в соответствующей отрасли государства-члены ЕС должны учитывать количество и размер указанных операторов, например, с точки зрения занимаемой доли рынка или объемов производства или поставляемых услуг, при этом на них не возлагается обязанность по раскрытию информации, позволяющей выявить идентифицированного оператора;
- территориальный фактор (географическое распространение области, на которую может оказать влияние инцидент);
- фактор взаимозаменяемости (влияние организации на поддержание необходимого уровня оказания услуги с учетом доступности альтернативных способов оказания указанной услуги).

Вышеуказанные межотраслевые факторы не являются исчерпывающими.

Государства-члены могут установить дополнительно и внутриотраслевые значения (п. 28 Преамбулы).

Более конкретные типы предприятий обозначены в Приложении 2 к Директиве NIS[42].

Также отметим, что, согласно п. 21 Преамбулы Директивы NIS, для целей идентификации операторов жизненно-важных услуг, применения к ним положений Директивы NIS, размещение организаций в государствах-членах ЕС подразумевает эффективное и реальное осуществление предпринимательской деятельности. Правовая форма указанной организации, будь то филиал или дочернее предприятие, обладающие правоспособностью, в данном случае не является определяющим фактором. Такой подход определения домицилия лица, в целом, характерен и для других директив. При этом, согласно п. 22 Преамбулы Директивы 2016/1148 операторы жизненно-важных услуг

[41] Cybersecurity Incident Taxonomy CG Publication 04/2018. URL: http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf (дата обращения: 30.06.2019).

[42] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Annex 2. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 30.06.2019).

должны отвечать особым требованиям в области обеспечения безопасности только в отношении тех услуг, которые считаются жизненно-важными. Таким образом, для целей идентификации операторов государства-члены ЕС должны установить список услуг, которые считаются таковыми.

Под провайдером цифровых услуг (DSP) ст. 1 Директивы понимает юридическое лицо, оказывающее цифровые услуги. Обоснование выделения такого субъекта состоит в том, что безопасность, стабильность и надежность указанных в Директиве типов цифровых услуг играет ключевую роль в нормальном функционировании многих предприятий – операторов жизненно-важных услуг (п. 48 Преамбулы). На взаимозависимость Операторов жизненно-важных услуг и Провайдеров цифровых услуг в конкретных отраслях обращает внимание и ENISA[43].

Понятие цифровых услуг дано в Директиве 2015/1535 Европейского Парламента и Совета ЕС от 9 сентября 2015 г. «О процедуре предоставления информации в области технических регламентов, а также правил оказания услуг в информационном обществе». В соответствии со ст. 1 указанной Директивы под цифровой услугой понимается любая услуга, соответствующая следующим признакам:

- по общему правилу, предоставляется за вознаграждение;
- предоставляется на расстоянии (услуга предоставляется без одновременного присутствия сторон);
- предоставляется электронными средствами (услуга первоначально отправляется и принимается в пункте назначения, с помощью электронного оборудования для обработки (включая цифровое сжатие) и хранение данных, а также полностью передается и принимается по проводам, по радио или оптическим каналам связи или другим электромагнитным средствам связи);
- предоставляется по индивидуальному запросу получателя услуг[44].

В соответствии с Приложением 3 к Директиве NIS, Директива охватывает понятием «провайдера цифровых услуг» только следующие категории таковых:

- интернет-магазин (При этом, в соответствии с п. 15 Преамбулы магазины приложений, функционирующие как онлайн-магазины, позволяющие осуществлять цифровую дистрибуцию приложений или программного обеспечения от имени третьих лиц, рассматриваются как вид интернет-магазинов);
- поисковик (при этом, в соответствии с п. 16 Преамбулы, определение онлайн-поисковой системы, содержащееся в настоящей Директиве, не должно охватывать поисковые функции, ограниченные содержанием определенного веб-сайта, независимо от того, предоставлена ли поисковая функция внешней поисковой системой или нет);
- сервис облачных вычислений[45].

Стоит также заметить, что возможно существование третьей категории субъектов – это такие организации, уведомляющие компетентные органы в добровольном порядке об инцидентах (оказывающих существенное влияние на предоставление ими услуг), которые

[43] Good practices on interdependencies between OES and DSPs. ENISA. 2018. URL: https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps (дата обращения: 30.06.2019).

[44] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535 (дата обращения: 30.06.2019).

[45] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Annex 3. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 30.06.2019).

не были отнесены ни к категории операторов жизненно-важных услуг, ни к провайдерам цифровых услуг (ст. 20 Директивы ЕС NIS). Обязательные уведомления (от ОЖВУ и провайдеров цифровых услуг) обрабатываются в приоритетном порядке. Добровольные уведомления обрабатываются только в том случае, если это не является экономически непропорциональным для государства-члена. Добровольное уведомление об инциденте, в отличие от обязательного, не налагает на лицо никаких обязанностей.

В целом, положения раздела 3 и 4 британского статута № 506 соответствуют вышеизложенному.

BSIG (Германия) и соответствующий Указ о мерах по обеспечению высокого общего уровня безопасности сетевых и информационных систем в Союзе (BSIGuaÄndG) содержат указания на тех же аналогичных субъектов, что и общее законодательство ЕС: операторов критической инфраструктуры и провайдеров цифровых услуг. Существенной разницы, за исключением названия, не выявлено.

Операторы жизненно важных услуг согласно ст.ст. 14, 15, 16 Директивы ЕС NIS несут следующие основные обязанности:

- принятие необходимых и пропорциональных технических и организационных мер, направленных на управление рисками, связанными с используемыми ими в процессе работы сетевыми и информационными системами. Как отмечено в п. 46 Преамбулы меры, направленные на управление рисками, включают в себя меры по определению любых рисков наступления инцидентов, по предотвращению, обнаружению и устранению инцидентов, а также по смягчению их последствий. Безопасность сетевых и информационных систем включает в себя безопасность хранения, передачи и обработки данных. Среди таких мер можно отметить: создание особой конфигурации системы, разделение систем, фильтрация трафика, использование криптографических средств защиты информации, введение аутентификации и идентификации в системе[46];
- принятие необходимых мер, направленных на предупреждение и минимизацию воздействия инцидентов, влияющих на безопасность сетевых и информационных систем, используемых для оказания жизненно важных услуг, с точки зрения их непрерывности;
- незамедлительное уведомление компетентного органа или CSIRT об инцидентах, оказывающих существенное воздействие на непрерывность оказываемых ими услуг. Уведомление должно содержать сведения, позволяющие компетентному органу или CSIRT определить наличие трансграничного воздействия инцидента. Уведомление не повышает ответственности уведомляющей стороны. При определении существенности, в соответствии с пп. a,b,c п. 4 ст. 14 Директивы ЕС NIS используются критерии: количества пользователей, пострадавших от сбоев в оказании жизненно-важной услуги; продолжительности инцидента; географическое распространение области, пострадавшей от инцидента. Процедура уведомления и конкретные примеры отражены в Руководстве по уведомлению операторами жизненно важных услуг об инцидентах 2018 года. Уведомление может быть направлено путем телефонного звонка, по электронной почте, путем заполнения онлайн формы, путем использования специального приложения. Можно привести два конкретных примера таких ситуаций, когда необходимо уведомление. В первом произошло отключение питания в регионе, что привело к невозможности работы информационных систем платежного шлюза, следовательно, люди по всей стране не могли

[46] Reference document on security measures for Operators of Essential Services CG Publication 01/2018. URL: http://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (дата обращения: 30.06.2019).

приобрести продукты. В качестве другого примера можно привести ситуацию, когда произошло разрушение контейнерного терминала порта из-за ошибок в обновлении ПО[47];

- предоставление компетентному органу информации, необходимой для проведения оценки безопасности сетевых и информационных систем, в том числе документально оформленных правил безопасности;
- предоставление компетентному органу доказательств эффективного применения правил безопасности, например, результатов аудита безопасности;
- уведомление о существенном влиянии инцидента, произошедшего с провайдером цифровых услуг, в случае использования услуг такого провайдера для оказания жизненно-важных услуг.

Провайдеры цифровых услуг, в свою очередь, в соответствии со ст. 16, 17 Директивы ЕС NIS обязаны:

- принимать необходимые пропорциональные технические и организационные меры, направленные на управление рисками. Указанные меры должны гарантировать уровень безопасности сетевых и информационных систем, соответствующий имеющимся рискам согласно уровню технического развития, с учетом, в частности: безопасности сетей и предприятий; управления инцидентами; управления устойчивостью бизнеса; мониторинга, аудит и тестирование; соответствия международным стандартам. Требования в области обеспечения безопасности и уведомления распространяются независимо от того, сами ли они осуществляют управление сетевыми и информационными системами или привлекают сторонних специалистов (п. 52 Преамбулы). Указанное предполагает наличие следующих элементов: систематического управления сетевыми и информационными системами, физическую безопасность, безопасность поставок, контроль доступа к системам[48];
- незамедлительно уведомлять компетентный орган или CSIRT об инцидентах, оказывающих существенное воздействие на оказание на территории Союза соответствующих услуг. При определении существенности во внимание принимаются: количество пользователей, пострадавших от инцидента, в частности, пользователей, использующих услугу для предоставления своих услуг; продолжительность инцидента; величина области, пострадавшей от инцидента, пострадавшей от инцидента; степень нарушения услуги; степень воздействия на экономическую и социальную деятельность. В части существенности воздействия Европейская комиссия предлагает исходить из следующих параметров: услуга, предоставляемая провайдером цифровых услуг, была недоступна в течение более 5 000 000 пользовательских часов; инцидент привел к потере целостности, подлинности или конфиденциальности хранимых, переданных или обработанных данных более 100 000 пользователей в Союзе; инцидент создал риск для общественной безопасности или привел к гибели людей; инцидент нанес материальный ущерб, по крайней мере одному пользователю в размере более 1 000 000 евро[49];

[47] Guidelines on notification of Operators of Essential Services incidents Formats and procedures CG Publication 05/2018. URL: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group (дата обращения: 30.06.2019).

[48] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0151&from=EN (дата обращения: 30.06.2019).

[49] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0151&from=EN (дата обращения: 30.06.2019).

- предоставлять информацию, необходимую для проведения оценки безопасности их сетевых и информационных систем, в том числе документально оформленные правила безопасности;
- устранять любые несоответствия положениям ст. 16 Директивы ЕС NIS по требованию компетентного органа;
- назначить Представителя на территории ЕС. При этом, как отмечается в п. 65 Директивы, для того чтобы определить, оказывает ли провайдер цифровых услуг услуги на территории Союза, необходимо бесспорно установить, что провайдер цифровых услуг намерен предлагать свои услуги лицам в одном или нескольких государствах-членах ЕС. Только доступность в Союзе веб-сайта провайдера цифровых услуг или его посредника, его адреса электронной почты или иной контактной информации, а также использование языка, обычно используемого в третьей стране, в которой учрежден провайдер цифровых услуг, не является достаточным подтверждением указанных намерений. Однако такие факты, как использование языка или валюты, обычно используемых в одном или нескольких государствах-членах ЕС, с предоставлением возможности заказа услуг на указанном языке или упоминание находящихся в Союзе потребителей или пользователей, могут явно свидетельствовать о намерении провайдера цифровых услуг оказывать услуги на территории Союза.

В отношении имплементации положений Директивы ЕС NIS, применительно к провайдерам цифровых услуг, важно отметить, что:

- в отношении провайдеров цифровых услуг не действует правило, установленное ст. 3 Директивы ЕС NIS. То есть, государства не могут установить требования, превышающие изложенные в настоящей Директиве;
- в отличие от операторов жизненно-важных услуг, к провайдерам цифровых услуг могут быть приняты только надзорные меры последующего реагирования, в соответствии с п. 1 ст. 17 Директивы ЕС NIS. О предварительных мерах и об обязательных указаниях речи не идет;
- государства-члены ЕС не должны проводить идентификацию провайдеров цифровых услуг (п. 57 Преамбулы).

Более лояльное отношение к провайдерам цифровых услуг (light touch approach[50]) в Директиве NIS обосновывается тем, что на практике степень риска операторов жизненно-важных услуг, которые часто играют важную роль в поддержании ключевой социально-экономической деятельности, выше, чем степень риска провайдеров цифровых услуг (п. 49 Преамбулы).

Вместе с тем, не исключено применение более жестких требований к провайдерам цифровых услуг не на основании закона, но в силу договорных обязательств (п. 54 Преамбулы).

В рамках obiter dictum отметим, что в п. 51 Преамбулы содержится важное разъяснение-гарантия, согласно которому возложенные на операторов жизненно-важных услуг и провайдеров цифровых услуг технические и организационные меры не должны возлагать обязанности по проектированию, разработке или производству определенным образом медиапродуктов компании. Указанное означает, что государство не может обязать

[50] Paraskevi Kasse (Network and Information Security Officer). Update on the implementation of the NIS Directive // ENISA Presentation. URL: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/january-2018/2018-01-30-enisa-nisd.pdf (дата обращения: 30.06.2019).

бизнес вести дела определенным образом, неоправданно вмешиваясь в коммерческие процессы. То есть государство налагает публично-правовые обязанности, при этом, не вмешиваясь в коммерческую деятельность компании. Конкретные положения о «разделительной линии» между обязанностями субъекта ОЖВУ и коммерческой деятельностью не проводится.

Если говорить о соответствующих обязанностях в рамках конкретных государств-членов ЕС, то можно привести в пример опыт ФРГ. В Законе BSIG, а именно в разделах 8a, и 8c установлены обязанности операторов объектов критической инфраструктуры и к поставщикам цифрового контента. В целом, обязанности аналогичны вышеизложенным.

Положения раздела 3 и 4 британского статута № 506 в основном соответствуют вышеизложенному.

7.3. Подход РФ к определению субъектов КИИ

Согласно п. 33 Доктрины информационный безопасности РФ участниками системы обеспечения информационной безопасности являются, в том числе и собственники объектов критической информационной инфраструктуры; организации, эксплуатирующие такие объекты.

Закон о безопасности КИИ относит к субъектам КИИ лиц, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в обозначенных выше сферах, а именно:

- государственные органы;
- государственные учреждения;
- российские юридические лица;
- российские ИП.

Также к субъектам КИИ закон относит российских юридических лиц и (или) ИП, которые обеспечивают взаимодействие указанных систем или сетей.

Таким образом закон выделяет 2 вида субъектов КИИ (титульные владельцы и лица, обеспечивающие взаимодействие систем и сетей).

В обязанности субъектов (двух видов) входит:

- присвоение объекту категории значимости, если он удовлетворяет установленным критериям, и сообщение об этом в ФСТЭК. Форма направления сведений о результатах присвоения объекту КИИ одной из категорий значимости утверждена Приказом ФСТЭК № 236[51];
- информирование уполномоченного органа о компьютерных инцидентах (факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки). Информирование осуществляется через ГосСОПКА (государственная система обнаружения,

[51] Приказ ФСТЭК России «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» от 22.12.2017 N 236 // СПС Консультант плюс.

предупреждения и ликвидации последствий компьютерных атак) путем направления соответствующего сообщения, в том числе посредством сайта http://cert.gov.ru[52];

- оказание содействия должностным лицам ФСБ и ФСТЭК;
- обеспечение выполнения порядка, ТУ установки и эксплуатации специальных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- создание системы безопасности КИИ и обеспечение ее функционирования (предотвращение неправомерного доступа к информации), обрабатываемой значимым объектом КИИ; недопущение воздействия на технические средства обработки информации, в результате которого может быть прекращено функционирование значимого объекта КИИ; восстановление функционирования такого объекта; непрерывное взаимодействие с ГосСОПКА)[53];
- выполнение требований по обеспечению безопасности значимых объектов КИИ (принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры; установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры). Конкретные требования установлены Приказом ФСТЭК № 239[54].

В обязанности 1 вида субъектов дополнительно входит:

- соблюдение требований по обеспечению безопасности значимых объектов КИИ;
- выполнение предписаний должностных лиц ФСБ и ФСТЭК;
- реагирование на компьютерные инциденты в предусмотренном порядке;
- принятие мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ;
- обеспечение беспрепятственного доступа ФСБ и ФСТЭК к значимым объектам КИИ.

7.4. Подход США к определению субъектов КИИ

В соответствии с Директивой PPD-21 основная ответственность за защиту, реагирование и восстановление лежит на владельцах и операторах объектов критической инфраструктуры. Тем не менее, федеральное правительство оставляет открытой возможность вмешательства в тех областях, где владельцы и операторы не могут (или не хотят) предоставлять то, что федеральное правительство может счесть адекватной защитой или ответом. В частности, указывается на то, что «частные фирмы несут основную и существенную ответственность за устранение рисков для общественной безопасности, создаваемых их отраслями»[55]. Директива PPD-21 также указывает, хотя и менее определенно, на роль частного бизнеса: «владельцы и операторы имеют уникальные возможности для управления рисками, угрожающими их отдельным операциям и активам

[52] Приказ ФСБ России «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 24.07.2018 N 367 // СПС Консультант плюс.

[53] Приказ ФСТЭК России «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» от 21.12.2017 N 235 // СПС Консультант плюс.

[54] Приказ ФСТЭК России «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 N 239 // СПС Консультант плюс.

[55] White House, Office of Homeland Security, National Strategy for Homeland Security, стр. 33. URL: https://georgewbush-whitehouse.archives.gov/homeland/book/index.html (дата обращения: 30.06.2019).

и определения эффективных стратегий, чтобы сделать тех более безопасными и устойчивыми»[56].

7.5. Подход Грузии к определению субъектов КИИ

Субъект критической информационной системы представляет Агентству по обмену данными на рассмотрение правила информационной безопасности для внутрислужебного пользования. 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. Субъекты обязаны устранить выявленные недостатки в определенный срок.

7.6. Подход Казахстана к определению субъектов КИИ

Закон Казахстана в качестве субъектов КИИ выделяет владельцев критически важных объектов. Владелец критически важных объектов информационно-коммуникационной инфраструктуры обязан:

- осуществлять мониторинг обеспечения информационной безопасности объектов информатизации в порядке, определяемом уполномоченным органом в сфере обеспечения информационной безопасности;
- обеспечить подключение систем мониторинга обеспечения информационной безопасности к техническим средствам системы мониторинга обеспечения информационной безопасности Национального координационного центра информационной безопасности.
- оповещать Национальный координационный центр информационной безопасности об инцидентах информационной безопасности в порядке и сроки, которые определены правилами проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры, если иное не установлено законодательными актами Республики Казахстан;
- осуществлять передачу резервных копий электронных информационных ресурсов на единую платформу резервного хранения электронных информационных ресурсов в порядке и сроки, которые определены уполномоченным органом в сфере обеспечения информационной безопасности, если иное не установлено законодательными актами Республики Казахстан.

Владелец объекта информационно-коммуникационной инфраструктуры несет ответственность перед собственником или владельцем электронных информационных ресурсов, информационной системы за безопасность хранения и защиту электронных информационных ресурсов, защиту информационных систем, размещенных на принадлежащих ему объектах.

7.7. Подход КНР к определению субъектов КИИ

Операторы КИИ в КНР должны использовать только сетевые продукты и услуги, которые прошли процесс проверки национальной безопасности, хранить определенные

[56] White House, Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, February 12, 2013. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (дата обращения, 30.09.2019).

данные на территории Китая и проходить такие процедуры проверки безопасности, как выборочное тестирование и регулярные оценки.

Помимо некоторых из обязанностей операторов КИИ, предусмотренных Законом о кибербезопасности к таковым предъявляется ряд иных требований:

- квалификационное требование: «специалисты на ключевых должностях» должны подчиняться квалификационным требованиям;
- образование и обучение: операторы КИИ должны предоставлять программу обучения и подготовки в области кибербезопасности для общего персонала не менее чем на 1 рабочий день в год и не менее чем на 3 рабочих дня в год для «специалистов на ключевых должностях»;
- оценка безопасности: операторы КИИ обязаны установить процедуру оценки безопасности до того, как КИИ начнет работу и когда произойдут «существенные изменения»;
- сторонние поставщики услуг: операторы КИИ должны проводить тестирование безопасности любых сетевых систем, программного обеспечения или продуктов, разработанных сторонними поставщиками услуг, и любых сетевых продуктов, которые передаются оператору КИИ перед использованием;
- техническое обслуживание КИИ: оперативное обслуживание КИИ должно проводиться в Китае. Если техническое обслуживание должно проводиться дистанционно за пределами Китая для коммерческих нужд, операторы КИИ должны сначала сообщить об этом соответствующим надзорным органам.

8. Публичные органы в сфере обеспечения безопасности КИИ, их полномочия, взаимодействие между собой и с субъектами

8.1. Публичные органы в сфере обеспечения безопасности КИИ (ЖВУ), их полномочия, взаимодействие между собой и с субъектами: сравнительно-правовой анализ

Проанализированные акты различных юрисдикций представляют огромное многообразие несовпадающих (как по названию, так и по функциям, ОГВ, уполномоченных в сфере защиты КИИ) вариантов.

Нормативно-правовое регулирование в указанной сфере обычно осуществляет один или два органа:

- Президент и Правительство в РФ;
- Государственный совет в КНР;
- Правительство в Республике Казахстан;
- Министр национальной безопасности в США.

В отношении США важно сделать оговорку о том, что Министр национальной безопасности является далеко не единственным органом, осуществляющим нормативно-правовое регулирование. В каждой сфере (например, энергетики или связи) существуют свои органы, издающие свои обязательные к выполнению НПА. Рекордное многообразие органов и различных НПА в указанной сфере является спецификой американского регулирования, которое затрудняет имплементацию подобного подхода в иных юрисдикциях[57].

[57] Наделение различных органов власти полномочиями в сфере обеспечения безопасности КИИ позволяет, с одной стороны, создать всестороннее и сбалансированное регулирование в данной области. При этом, однако, такой подход требует существенных

Непосредственно контрольно-надзорные органы, наименования которых различны в исследуемых юрисдикциях, реализуют следующие основные функции:

- мониторинг инцидентов, хранение записей об инцидентах, проведение проверок;
- распространение предупреждений об опасности, подготовка методических рекомендаций об основных угрозах кибербезопасности;
- реагирование на инциденты, установление причин компьютерных инцидентов, помощь в их ликвидации;
- расследование, содействие расследованию преступлений в сфере кибербезопасности.

Особенностью европейской Директивы NIS является то, что она утверждает не только необходимые национальные органы по кибербезопасности, но уделяет внимание и международному сотрудничеству. Так, например, сеть CSIRTs публикует данные об основных инцидентах, имеющих важное значение для ЕС, в целом.

Японское регулирование, напротив, не упоминает конкретных уполномоченных национальных органов в указанной сфере и, в целом, не является развитым по данному вопросу.

Наиболее интересными представляются российский вариант (где непосредственными регуляторами являются ФСБ, ФСТЭК и НКЦКИ), а также Казахский (где регулятором является Комитет информационной безопасности РК и Национальный координационный центр информационной безопасности РК).

Перспективным, на наш взгляд, является выделение или создание одного органа по вопросам кибербезопасности, в целом, или безопасности КИИ в отдельности. Централизация, в таком случае, позволит более оперативно выявлять и реагировать на инциденты, о которых сообщили или не сообщили субъекты КИИ. В случае невозможности создания или наделения полномочиями по контролю в сфере КИИ одного органа, необходимо обеспечить взаимодействие по принципу одного окна. Принцип одного окна представляется наиболее удобным вариантом взаимодействия субъектов КИИ и государственных органов.

8.2. Подход ЕС к определению уполномоченных органов и их компетенции: наднациональное регулирование, подход Германии и Соединенного Королевства

В соответствии с п. 1 ст. 8 Директивы NIS каждое государство-член ЕС должно назначить один или несколько национальных компетентных органов, ответственных за безопасность сетевых и информационных систем (CA).

В силу п. 3 ст. 8 Директивы NIS каждое государство-член ЕС должно назначить единый национальный контактный пункт по вопросам безопасности сетевых и информационных систем (SPOC).

Согласно ст. 9 Директивы 2016/1148 каждое государство-член должно создать группы реагирования на инциденты, связанные с компьютерной безопасностью (CSIRTs). Основные требования и задачи таких групп обозначены в Приложении 1 к Директиве NIS. К числу основных задач таких групп можно отнести: мониторинг инцидентов на

расходов со стороны государства, поскольку каждое ведомство инициирует и реализует программы в рамках отдельных бюджетов, а также предъявляет высокие требования к уровню профессиональной подготовки штата в рамках каждого уполномоченного ведомства, что на практике может вызвать затруднения ввиду недостаточного количества высококвалифицированных специалистов в данной отрасли. Кроме того, представляется, что в подобной системе значительные усилия должны быть направлены на координацию совместных усилий нескольких уполномоченных органов государственной власти.

национальном уровне; распространение заблаговременных предупреждений, сигналов об опасности, сообщение и распространение информации среди заинтересованных сторон о рисках и об инцидентах; реагирование на инциденты; проведение динамического анализа рисков и инцидентов и поддержание ситуационной осведомленности; участие в сети CSIRTs[58].

В качестве примера можно привести страны, где существует один орган, который одновременно выполняет функции SPOC, и CA, и CSIRT, например, Германия (Федеральный офис информационной безопасности)[59], Литва (Национальный Центр Кибербезопасности)[60].

Также можно привести страны, где производится разделение указанных органов, например: Франция, Испания, Соединенное королевство (Национальный центр кибербезопасности (NCSC) – контактный пункт; информационный комиссар (ICO) – компетентный орган для провайдеров цифровых услуг; Офис связи (OFCOM) – компетентный орган для ОЖВУ в сфере информационный инфраструктуры; Национальный центр кибербезопасности (NCSC) – CSIRT)[61].

Статьей 11 Директивы учреждается Группа по сотрудничеству для оказания поддержки и упрощения стратегического сотрудничества и обмена информацией между государствами-членами ЕС, укрепления доверия и уверенности, а также для достижения высокого уровня безопасности сетевых и информационных систем в Союзе (CG). В состав Группы по сотрудничеству входят представители государств-членов ЕС, Европейской Комиссии и ENISA. Этот орган подготавливает соответствующие отчеты по оценке накопленного опыта. Дополнительно укажем, что ENISA выпускает различные вспомогательные материалы, помогающие понять содержание директивы, например, Руководство по оценке соответствия операторов жизненно-важных услуг и провайдеров информационных услуг критериям безопасности, предъявляемым Директивой[62].

Статьей 12 Директивы учреждается сеть национальных CSIRTs (CSIRTs network). Этот орган подготавливает соответствующие отчеты по оценке накопленного опыта. Дополнительная функция указанного органа подчеркнута в п. 40 Преамбулы, согласно которому Секретариату сети CSIRTs рекомендуется поддерживать веб-сайт или создать отдельную страницу на существующем веб-сайте, на которых будет размещена в общем доступе информация об основных инцидентах, произошедших на территории Союза, особое внимание в которой будет обращено на интересы и потребности предприятий. Поощряется участие CSIRTs в сетях CSIRTs для размещения информации на добровольной основе на указанном веб-сайте, за исключением конфиденциальной и секретной информации.

В соответствии со ст. 23 Директивы ЕС NIS до 9 мая 2019 г. Европейская Комиссия передает в Европейский Парламент и Совет ЕС отчет, содержащий оценку единообразия

[58] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Annex 1. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 30.06.2019).

[59] Bundesamt für Sicherheit in der Informationstechnik. Official website. URL: https://www.bsi.bund.de (дата обращения: 30.06.2019).

[60] NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS. Official website. URL: https://www.nksc.lt/en/ (дата обращения: 30.06.2019).

[61] State-of-play of the transposition of the NIS Directive. EC official website. URL: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive (дата обращения: 30.06.2019).

[62] Guidelines on assessing DSP and OES compliance to the NISD security requirements. ENISA. 2018. URL: https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements (дата обращения: 30.06.2019).

подходов государств-членов ЕС к идентификации операторов жизненно-важных услуг. Отчет в открытых источниках до настоящего времени не опубликован.

8.3. Подход РФ к определению уполномоченных органов и их компетенции

Основные полномочия государственных органов и должностных лиц, в сфере защиты КИИ заключены в ст. 6 ФЗ О безопасности КИИ.

Президент Российской Федерации. Его основные функции сводятся к следующим:

- определение основных направлений государственной политики в области обеспечения безопасности КИИ;
- определение уполномоченных органов в сфере защиты КИИ;
- определение задач ГосСОПКА.

Правительство Российской Федерации устанавливает:

- показатели критериев значимости объектов КИИ, сроки категорирования;
- порядок осуществления государственного контроля в соответствующей сфере.

В рамках своих полномочий ФСТЭК[63]:

- утверждает порядок ведения реестра значимых объектов критической информационной инфраструктуры и ведет данный реестр[64];
- утверждает форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий[65];
- устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры[66];
- устанавливает требования к созданию систем безопасности и обеспечению их функционирования[67];
- осуществляет государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры (проводит плановые и внеплановые проверки), а также утверждает форму акта проверки, составляемого по итогам проведения указанного контроля[68]. Правила осуществления государственного контроля в указанной сфере утверждены Постановлением Правительства РФ от 17.02.2018 N 162[69].

В рамках своих полномочий ФСБ[70]:

- создает НКЦКИ;

---

[63] Указ Президента РФ «Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 N 1085 // СПС Консультант плюс.

[64] Приказ ФСТЭК России «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» от 06.12.2017 N 227 // СПС Консультант плюс.

[65] Приказ ФСТЭК России «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» от 22.12.2017 N 236 // СПС Консультант плюс.

[66] Приказ ФСТЭК России «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 N 239 // СПС Консультант плюс.

[67] Приказ ФСТЭК России «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» от 21.12.2017 N 235 // СПС Консультант плюс.

[68] Приказ ФСТЭК России «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 11.12.2017 N 229 // СПС Консультант плюс.

[69] Постановление Правительства РФ «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 17.02.2018 N 162 // // СПС Консультант плюс.

[70] Указ Президента РФ «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 22.12.2017 N 620; Указ Президента РФ «Вопросы Федеральной службы безопасности Российской Федерации» от 11.08.2003 N 960 // СПС Консультант плюс.

- координирует деятельность субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
- организует и проводит оценку безопасности критической информационной инфраструктуры;
- контролирует функционирование системы ГосСОПКА;
- разрабатывает методические рекомендации по обнаружению компьютерных атак[71];
- определяет перечень информации, предоставляемой в ГосСОПКА[72];
- утверждает порядок обмена информацией о компьютерных инцидентах между субъектами КИИ, между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, а также порядок получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения[73];
- организует установку на значимых объектах критической информационной инфраструктуры и в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
- устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Перечень видов средств и требований установлен в Приказе ФСБ № 196[74].

НКЦКИ:

- координирует мероприятия по реагированию на компьютерные инциденты и непосредственно участвует в таких мероприятиях;
- организует и осуществляет обмен информацией о компьютерных инцидентах;
- осуществляет методическое обеспечение деятельности субъектов КИИ по вопросам предупреждения компьютерных атак;
- участвует в обнаружении, предупреждении и ликвидации последствий компьютерных атак;
- осуществляет сбор, хранение и анализ информации о компьютерных инцидентах и компьютерных атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты;

---

[71] Указ Президента РФ «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 22.12.2017 N 620 // СПС Консультант плюс.

[72] Приказ ФСБ России «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 24.07.2018 N 367 // СПС Консультант плюс.

[73] Приказ ФСБ России «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» от 24.07.2018 N 368 // // СПС Консультант плюс.

[74] Приказ ФСБ России «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» от 06.05.2019 N 196 // // СПС Консультант плюс.

- определяет необходимые для организации взаимодействия форматы представления информации о компьютерных инцидентах в ГосСОПКА;
- определяет состав технических параметров компьютерного инцидента[75].

ФЗ О безопасности КИИ в ст. 5 также предусматривает создание ГосСОПКА, которая представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся: подразделения и должностные лица ФСБ; НКЦКИ; подразделения и должностные лица субъектов КИИ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

Основные задачи ГосСОПКА:

- прогнозирование ситуации в области обеспечения информационной безопасности;
- оссуществление контроля степени защищенности информационных ресурсов РФ от компьютерных атак;
- установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов РФ[76].

8.4. Подход США к определению уполномоченных органов и их компетенции

Директива PPD-21 распределяет роли и полномочии властных субъектов следующим образом.

Министр национальной безопасности обеспечивает стратегическое руководство, содействует общенациональному единству усилий и координирует общие федеральные усилия по обеспечению безопасности и устойчивости критически важной инфраструктуры страны. Выполняя обязанности, закрепленные в Законе о национальной безопасности 2002 года (Homeland Security Act of 2002) с внесенными в него поправками, Министр национальной безопасности:

- оценивает национальные возможности, возможности и проблемы в области защиты критически важной инфраструктуры;
- анализирует угрозы, уязвимости и потенциальные последствия всех угроз для критически важной инфраструктуры;
- определяет функции безопасности и устойчивости, которые необходимы для эффективного взаимодействия между государственным и частным секторами во всех критических секторах инфраструктуры;
- разрабатывает национальный план и показатели в координации с отраслевыми агентствами и другими партнерами по критически важной инфраструктуре;
- объединяет и координирует федеральные межсекторальные мероприятия по обеспечению безопасности и устойчивости;
- выявляет и анализирует ключевые взаимозависимости между важнейшими секторами инфраструктуры;

[75] Приказ ФСБ России «О Национальном координационном центре по компьютерным инцидентам» от 24.07.2018 N 366 // СПС Консультант плюс.

[76] Указ Президента РФ «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 22.12.2017 N 620 // // СПС Консультант плюс.

- сообщает об эффективности национальных усилий по укреплению безопасности и устойчивости страны для критически важной инфраструктуры.

Дополнительные обязанности Министра национальной безопасности включают:

- определение и определение приоритетности критически важной инфраструктуры с учетом физических и киберугроз, уязвимостей и последствий в координации с отраслевыми агентствами и другими федеральными департаментами и агентствами;
- поддержание национальных центров критической инфраструктуры, которые должны обеспечивать возможность информирования о ситуации, которая включает в себя интегрированную, действенную информацию о возникающих тенденциях, неизбежных угрозах и состоянии инцидентов, которые могут повлиять на критическую инфраструктуру;
- в координации с SSA и другими федеральными департаментами, и агентствами предоставление анализа, экспертных знаний и другой технической помощи владельцам и операторам критически важной инфраструктуры и облегчение доступа и обмена информации и разведывательными данными, необходимыми для усиления безопасности и устойчивости критически важной инфраструктуры;
- проведение всесторонней оценки уязвимости критической инфраструктуры страны в координации с отраслевыми агентствами и в сотрудничестве с организациями SLTT, владельцами и операторами критической инфраструктуры;
- координация действий федерального правительства в отношении значительных кибер или физических инцидентов, затрагивающих критически важную инфраструктуру, в соответствии с установленными законом органами;
- оказание поддержки Генеральному прокурору (Attorney General) и правоохранительным органам в их обязанностях по расследованию и преследованию угроз и атак на критически важную инфраструктуру;
- координация и использование опыта отраслевых агентств и других соответствующих федеральных департаментов и агентств для картографирования, визуализации, анализа и сортировки критической инфраструктуры с использованием коммерческих спутниковых и бортовых систем, а также существующих возможностей в других департаментах и агентствах; а также
- ежегодные отчеты о состоянии национальных критических инфраструктурных мероприятий, как того требует закон.

Каждый критически важный сектор инфраструктуры обладает уникальными характеристиками, операционными моделями и профилями рисков, которые получают поддержку от определенного отраслевого агентства (SSA) по конкретным секторам, которое обладает институциональными знаниями и специализированными знаниями об этом секторе.

Признавая существующие законодательные или регулирующие органы конкретных федеральных департаментов и агентств, и используя существующую осведомленность и взаимоотношения между секторами, отраслевые агентства должны выполнять обязанности в своих соответствующих секторах:

- в рамках более широких национальных усилий по укреплению безопасности и устойчивости критически важной инфраструктуры координировать свою деятельность с Министерством национальной безопасности (Department of Homeland Security, DHS) и другими соответствующими федеральными департаментами и агентствами и сотрудничать с владельцами и операторами критически важной инфраструктуры, где это необходимо, с

независимыми регулирующими органами, агентства, а также, при необходимости, с организациями SLTT для выполнения этой директивы;

- служить повседневным федеральным интерфейсом для динамической расстановки приоритетов и координации деятельности в конкретных секторах;
- выполнять обязанности по управлению инцидентами в соответствии с установленными законом полномочиями и другими соответствующими политиками, директивами или правилами;
- предоставлять, поддерживать или содействовать технической помощи и консультациям для этого сектора в целях выявления уязвимостей и, в случае необходимости, смягчения последствий инцидентов; а также
- поддерживать законодательные требования, предъявляемые к секретарю национальной безопасности, предоставляя на ежегодной основе критическую для конкретной отрасли информацию об инфраструктуре.

Перечисленные далее департаменты и агентства имеют специализированные или вспомогательные функции, связанные с обеспечением безопасности и устойчивости критической инфраструктуры, которые должны выполняться или совместно с другими федеральными департаментами, агентствами и независимыми регулирующими органами, в зависимости от обстоятельств.

Государственный департамент в координации с Министерством национальной безопасности, отраслевыми агентствами и другими федеральными департаментами и агентствами привлекает иностранные правительства и международные организации для укрепления безопасности и устойчивости критически важной инфраструктуры, расположенной за пределами Соединенных Штатов, и для содействия общему обмену лучшими практиками и опытом для обеспечения безопасности и устойчивости критически важной инфраструктуры, от которой зависит нация.

Министерство юстиции (Department of Justice, DOJ), включая Федеральное бюро расследований (Federal Bureau of Investigation, FBI), должно вести контртеррористические и контрразведывательные расследования и связанную с этим деятельность правоохранительных органов в критических секторах инфраструктуры. Министерство юстиции должно расследовать, препятствовать, преследовать по закону и иным образом уменьшать иностранные разведывательные, террористические и другие угрозы, а также фактические или попытки нападения или саботажа на критически важную инфраструктуру страны. ФБР также осуществляет сбор, анализ и распространение информации о киберугрозах на национальном уровне и несет ответственность за деятельность Национальной объединенной целевой группы по киберрасследованиям (National Cyber Investigative Joint Task Force, NCIJTF). NCIJTF выступает в качестве межведомственного национального координационного центра для координации, интеграции и обмена соответствующей информацией, связанной с расследованиями киберугроз, с представительством от Министерства национальной безопасности, Разведывательного Содружества (Intelligence Community, IC), Министерства обороны (Department of Defense, DOD) и других агентств, исходя из конкретных условий. Генеральный прокурор и министр внутренней безопасности должны сотрудничать друг с другом для выполнения своих задач в области критической инфраструктуры.

Министерство внутренних дел (Department of the Interior), в сотрудничестве с отраслевым агентством для сектора государственных учреждений (предприятий),

определяет, расставляет приоритеты и координирует усилия по обеспечению безопасности и устойчивости для национальных памятников и символов и включает меры по снижению риска для этих критически важных активов, а также содействует пользованию ими.

Министерство торговли (Department of Commerce, DOC) в сотрудничестве с Министерством национальной безопасности и другими соответствующими федеральными департаментами и агентствами должно привлекать частный сектор, исследовательские, академические и правительственные организации для повышения безопасности технологий и инструментов, связанных с киберсистемами, и содействовать развитию других усилий, связанных с критически важной инфраструктурой в целях обеспечения своевременной доступности промышленной продукции, материалов и услуг для удовлетворения требований национальной безопасности.

Разведывательное Содружество, возглавляемое Директором Национальной разведки (Director of National Intelligence, DNI), использует соответствующие полномочия и координационные механизмы для предоставления, при необходимости, оценок разведки в отношении угроз для критической инфраструктуры и координирует разведывательную и другую конфиденциальную или служебную информацию, связанную с критической инфраструктурой. Кроме того, надзор за политиками, директивами, стандартами и руководящими принципами защиты систем национальной безопасности должен осуществляться в соответствии с указаниями Президента США, применимым законодательством и в соответствии с этим указанием, осуществляемым под руководством глав агентств учреждений, которые имеют в управлении или осуществляют контроль над такими системами национальной безопасности.

Управление общих служб (General Services Administration) в консультации с Министерством обороны, Министерством национальной безопасности, другими департаментами и агентствами, в зависимости от обстоятельств, должна предоставлять или поддерживать общегосударственные контракты на системы критической инфраструктуры и обеспечивать, чтобы такие контракты включали права на аудит безопасности и отказоустойчивости критической инфраструктуры.

Комиссия по ядерному регулированию (Nuclear Regulatory Commission, NRC) обязана осуществлять надзор за защитой своими лицензиатами коммерческих ядерных энергетических реакторов и неэнергетических ядерных реакторов, используемых для исследований, испытаний и обучения; ядерных материалов в медицинских, промышленных и научных учреждениях, а также на объектах, которые производят ядерное топливо; и транспортировкой, хранением и утилизацией ядерных материалов и отходов. Комиссия по ядерному регулированию должна сотрудничать, насколько это возможно, с Министерством национальной безопасности, Министерством юстиции, Министерством энергетики (Department of Energy), Агентством по охране окружающей среды (Environmental Protection Agency) и другими федеральными департаментами и агентствами, в зависимости от обстоятельств, в укреплении безопасности и устойчивости критической инфраструктуры.

Федеральная комиссия по связи (Federal Communications Commission) в той мере, в которой это разрешено законом, должна использовать свои полномочия и опыт для сотрудничества с Министерством национальной безопасности и Государственным департаментом, а также с другими федеральными департаментами, агентствами и отраслевыми агентствами, в зависимости от обстоятельств, в: (1) определении и расстановке приоритетов коммуникационной инфраструктуры; (2) выявлении уязвимостей сектора связи и работа с отраслью и другими заинтересованными сторонами для устранения

этих уязвимостей; и (3) работе с заинтересованными сторонами, включая промышленность, и привлечение иностранных правительств и международных организаций к повышению безопасности и устойчивости критически важной инфраструктуры в секторе связи и содействие развитию и внедрению передового опыта, способствующего обеспечению безопасности и устойчивости критически важной инфраструктуры связи, от которой зависит США.

Федеральные департаменты и агентства должны своевременно предоставлять Министру национальной безопасности и национальным центрам критической инфраструктуры необходимую информацию для поддержки межотраслевого анализа и информирования о возможностях ситуационной осведомленности для критической инфраструктуры.

Министр национальной безопасности в координации с Управлением политики в области науки и техники (Office of Science and Technology Policy, OSTP), отраслевыми агентствами, Министерством торговли и другими федеральными департаментами и агентствами должен оказать содействие в согласовании тех федеральных и финансируемых из федерального бюджета мероприятий по исследованию и разработкам, которые направлены на укрепление безопасности и устойчивости критически важной инфраструктуры страны, в том числе:

- содействовать исследованиям и разработкам для обеспечения безопасного и отказоустойчивого проектирования и строительства критически важной инфраструктуры и более безопасных сопутствующих кибертехнологий;
- расширять возможности моделирования для определения потенциального воздействия на критическую инфраструктуру сценария инцидента или угрозы, а также каскадного воздействия на другие сектора;
- содействовать инициативам по стимулированию инвестиций в кибербезопасность и принятию важнейших функций проектирования инфраструктуры, которые повышают безопасность и устойчивость к любым угрозам; а также
- приоритиризировать усилия по поддержке стратегического руководства, изданного Министром национальной безопасности.

Следует отметить, что в структуре органов федеральной власти, вовлеченных в обеспечение безопасности КИИ, создаются специальные структуры, разрабатывающие методологические принципы и руководства и реализующие программы информационной поддержки в отдельных областях (группе областей), закрепленных за ними.

Так, Агентство по кибербезопасности и безопасности инфраструктуры (CISA)[77] является национальным консультантом по рискам, сотрудничая с партнерами в целях защиты от сегодняшних угроз и сотрудничая для создания более безопасной и устойчивой инфраструктуры в будущем. CISA сотрудничает с отраслями индустрии и правительством для понимания и управления рисками для критически важной инфраструктуры США.

CISA создает национальный потенциал для защиты от кибератак и работает с федеральным правительством по предоставлению инструментов кибербезопасности, служб реагирования на инциденты и возможностей оценки для защиты сетей «.gov», которые поддерживают основные операции партнерских департаментов и агентств.

CISA координирует усилия по обеспечению безопасности и устойчивости, используя надежные партнерские отношения между частным и государственным секторами, а также

[77] The Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.dhs.gov/CISA (дата: обращения: 30.06.2019).

предоставляет техническую помощь и оценки федеральным заинтересованным сторонам (стейкхолдерам), а также владельцам инфраструктуры и операторам по всей стране.

CISA проводит обширную общенациональную информационно-пропагандистскую работу по поддержке и расширению возможностей реагирования на чрезвычайные ситуации провайдеров (providers) и соответствующих государственных должностных лиц продолжать поддерживать связь в случае стихийных бедствий, террористических актов и других техногенных катастроф.

Организационно в рамках CISA действуют пять отделов - Кибербезопасности (Cybersecurity), Экстренная связь (Emergency Communications), Безопасность инфраструктуры (Infrastructure Security), Федеральная служба охраны (Federal Protective Service). Каждый из указанных отделов действует в соответствии с опредленными для них целями и задачами, и в рамках функционирования разрабатывает программы, информационные продукты, оказывает различного рода услуги[78].

Также, в Агентстве кибербезопасности и безопасности инфраструктуры (CISA) расположен Национальный центр управления рисками (NRMC) - центр планирования, анализа и сотрудничества, который занимается выявлением и устранением наиболее значительных рисков для критической инфраструктуры США.

Другим примером «консультирующего органа» может являться Национальный институт стандартов США и технологии (NIST)[79]. В 2013 году Указом Президента 13636 («Улучшение критической инфраструктуры кибербезопасности»[80]) Национальному институту стандартов США и технологии (NIST) было поручено возглавить разработку основ для минимизации рисков кибербезопасности для критической инфраструктуры, получения обратной связи от общественности и заинтересованных сторон частного сектора и инкорпорации лучших отраслевых практик в полной возможной мере. В рамках своей деятельности В 2014 году NIST опубликовал Основы кибербезопасности для защиты критической инфраструктуры (Cybersecurity Framework for Protecting Critical Infrastructure (NIST Framework), описывая его как «основанный на риске набор отраслевых стандартов и лучших практик, чтобы помочь организации управляют рисками кибербезопасности».

8.5. Подход Грузии к определению уполномоченных органов и их компетенции

Агентство по обмену данными (DEA) при Министерстве юстиции было создано в 2010 году. В его задачи входят разработка стандартов для электронного управления, инфраструктур обмена данными и информационно-коммуникационной сферы Грузии, а также реализация политики в области информационной безопасности. В компетенцию Агентства входит обеспечение кибербезопасности всей правительственной сети (за исключением ее военной части), включающей 36 объектов критической инфраструктуры. DEA устанавливает минимальные требования по информационной безопасности для критических информационных систем.

Под руководством DEA функционирует Компьютерная группа реагирования на чрезвычайные ситуации (CERT) – она отвечает за реагирование на киберинциденты и

[78] Так, отдел Кибербезопасности (Cyber Security Division) осуществляет деятельность по распространению информации, разрабатывает продукты в рамках национальной системы кибер-осведомленности, обеспечения безопасности федеральных сетей, защиты критической инфраструктуры, разрабатывает методологические принципы и руководства в указанных областях.

[79] U.S. National Institute of Standards and Technology (NIST). URL: https://www.nist.gov (дата обращения: 30.06.2019).

[80] Executive Order - Improving Critical Infrastructure Cybersecurity. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (дата обращения: 30.09.2019).

наблюдение за работоспособностью правительственной сети Грузии. CERT уполномочен требовать доступ к критическим информационным системам или активам.

Отдел по борьбе с киберпреступностью Центрального отделения криминальной полиции при МВД осуществляет уголовное преследование и расследование киберпреступлений Согласно Уголовному кодексу Грузии, неправомерный доступ к компьютерной информации, создание или распространение вредоносных программ, неправомерное использование компьютерных сетей и кибертерроризм считаются преступлениями.

В рамках Отдела функционирует круглосуточный контактный центр, в функции которого входит обмен информацией о киберпреступлениях с другими членами Конвенции Совета Европы о киберпреступности.

При Совете по государственной безопасности и управлению кризисами при главе кабинета министров был создан консультативный орган, который отвечает за кибербезопасность. Совет осуществляет руководство в сфере информационной безопасности, выявляет и предотвращает внутренние и внешние угрозы, а также координирует разработку национальной стратегии кибербезопасности. Это связано с тем, что закон Грузии «О порядке планирования и координации политики национальной безопасности» определяет информационную безопасность как составную часть национальной безопасности. Согласно документу, органами, отвечающими за планирование политики в области национальной безопасности, являются Совет национальной безопасности и Совет по государственной безопасности и управлению кризисами.

Бюро кибербезопасности занимается разработкой эффективных и надежных систем в области информационных и коммуникационных технологий для гражданских подразделений Минобороны и для структурных подразделений Генерального штаба. Компьютерная группа реагирования на чрезвычайные ситуации при Бюро осуществляет наблюдение и защиту критической инфраструктуры и инфраструктуры связи Минобороны от киберугроз и рисков.

Национальная комиссия Грузии по коммуникациям контролирует соответствие операторов действующему законодательству, а также распределение и присвоение частот, лицензирование и разрешение споров между операторами, в случае, когда стороны не могут достичь согласия по таким вопросам как тарифы и ставки взаимоподключения. Она также уполномочена работать с жалобами потребителей.

8.6. Подход Казахстана к определению уполномоченных органов и их компетенции

Правительство Республики Казахстан в сфере информатизации утверждает перечень критически важных объектов информационно-коммуникационной инфраструктуры, а также правила и критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры.

Уполномоченный орган в сфере обеспечения информационной безопасности РК осуществляет следующие полномочия:

- разрабатывает перечень критически важных объектов информационно-коммуникационной инфраструктуры, а также правила и критерии отнесения объектов

информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры;

- утверждает методику и правила проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности;
- утверждает правила проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры по согласованию с органами национальной безопасности;
- утверждает правила создания и обеспечения функционирования единой национальной резервной платформы хранения электронных информационных ресурсов, периодичность резервного копирования электронных информационных ресурсов критически важных объектов информационно-коммуникационной инфраструктуры.

В компетенцию национального координационного центра информационной безопасности РК входит:

- сбор, анализ и обобщение информации оперативных центров информационной безопасности об инцидентах информационной безопасности на объектах информационно-коммуникационной инфраструктуры «электронного правительства» и других критически важных объектах информационно-коммуникационной инфраструктуры;
- межотраслевая координация по вопросам мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства», казахстанского сегмента Интернета, а также критически важных объектов информационно-коммуникационной инфраструктуры, реагирование на инциденты информационной безопасности с проведением совместных мероприятий по обеспечению информационной безопасности в порядке, определяемом законодательством Республики Казахстан;
- создание и обеспечение функционирования единой национальной резервной платформы хранения электронных информационных ресурсов.

Комитет по информационной безопасности Министерства цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан осуществляет регулятивные, реализационные и контрольные функции, а также участвуют в выполнении стратегических функций Министерства в области обеспечения информационной безопасности в сфере информатизации.

Уполномоченный орган ежегодно не позднее 1 февраля направляет центральным государственным и местным исполнительным органам, собственникам (владельцам) стратегических объектов, особо важных государственных объектов, объектов отраслей экономики, имеющих стратегическое значение, запрос о имеющихся объектах информационно-коммуникационной инфраструктуры, соответствующих не менее одному из критериев.

Центральные государственные и местные исполнительные органы, собственники (владельцы) стратегических объектов, особо важных государственных объектов, объектов отраслей экономики, имеющих стратегическое значение, ежегодно не позднее 1 марта на основании запроса вносят на рассмотрение в уполномоченный орган предложения для

включения объектов информационно-коммуникационной инфраструктуры в перечень с приложением документов и иных материалов, обосновывающих такое соответствие.

В целях обеспечения безопасности страны уполномоченные органы в сфере обороны, гражданской защиты и органы национальной безопасности по собственной инициативе вносят на рассмотрение в уполномоченный орган предложения для включения объектов информационно-коммуникационной инфраструктуры в перечень и (или) исключения из него.

Уполномоченный орган для рассмотрения и анализа предложений центральных государственных и местных исполнительных органов, собственников (владельцев) стратегических объектов, особо важных государственных объектов, объектов отраслей экономики, имеющих стратегическое значение, формирует комиссию из числа специалистов общественных объединений в сфере информационной безопасности, а также должностных лиц, ответственных за обеспечение информационной безопасности, в уполномоченном органе, органах национальной безопасности, гражданской защиты и обороны. Далее принимается решение о включении или исключении конкретных объектов из Перечня. Владельцы исключенных объектов освобождаются от соответствующих обязанностей.

8.7. Подход Сингапура к определению уполномоченных органов и их компетенции

Национальные отраслевые контрольные или надзорные департаменты в соответствии с разделением компетенции, устанавливаемой Государственным советом, несут ответственность за руководство и надзор за работой КИИ в области безопасности в своих секторах и областях.

Национальный отдел кибербезопасности и информатизации отвечает за всестороннюю координацию работы по защите безопасности КИИ и связанной с этим работой по надзору и управлению.

Подразделения Государственного совета по общественной безопасности, государственной безопасности, административному управлению защитой государственной тайны, управлению государственным шифрованием в рамках своих соответствующих обязанностей несут ответственность за обеспечение кибербезопасности.

Соответствующие департаменты районных или вышестоящих местных народных правительств также проводят работу по обеспечению безопасности КИИ.

9. Экономическая модель регулирования

9.1. Сравнительно-правовой анализ предлагаемых экономических моделей распределения издержек по обеспечению безопасности КИИ (ЖВУ)

Финансово и организационно затратные обязанности, в основном, в одностороннем порядке возложены на субъектов КИИ (ОЖВУ).

В рамках формирования нового перспективного, прогрессивного подхода считаем целесообразным закрепить принцип пропорциональности (соразмерности рискам) возложения дополнительных обязанностей на хозяйствующих субъектов, с целью недопущения чрезмерного обременения последних. В качестве доступных опций предлагается субсидирование, компенсационные меры (в том числе и налоговые льготы).

В целом, вышеуказанные подходы РФ и ЕС к дифференциации субъектов в зависимости от значимости объектов КИИ (осуществляемой ими деятельности) и соразмерное возложение обязанностей представляются правильными. Аналогичную

дифференциацию объема обязанностей (в отношении АЭС, морских перевозчиков, производителей медикаментов и т.д.) предусматривают и анализируемые акты США. В некоторых сферах (например, в нефтегазовой и торговой) США использует рекомендательные нормы и поощрение.

Представляется перспективным сочетание подхода РФ и США по данному вопросу для формирования экономической модели регулирования в сфере КИИ.

9.2. Подход ЕС к выработке экономической модели регулирования: наднациональное регулирование, подход Германии и Соединенного Королевства

Обязанность по исполнению требований закона распределена между компетентными органами и ОЖВУ, провайдерами цифровых услуг. Больше требований соответствующие НПА предъявляют к ОЖВУ (ОКИ). Так, ОЖВУ и провайдеры цифровых услуг за свой счет должны разработать и осуществить необходимые технические меры, проводить аудит безопасности, выявлять и сообщать об инцидентах. Обязанность публичных органов сводится к контролю и межгосударственному взаимодействию. Никакого возмещения или льгот при наложении новых обязанностей не предусматривается.

9.3. Подход РФ к выработке экономической модели регулирования

Обязанности по исполнению требований ФЗ О безопасности КИИ и подзаконных актов распределены между государственными органами и субъектами КИИ. Вместе с тем, существенное количество финансово затратных обязанностей возложено исключительно на субъектов КИИ, в том числе, частных лиц только в силу того, что их объект стал относиться к одной из категорий значимых объектов КИИ. Считаем целесообразным закрепить принцип пропорциональности возложения дополнительных обязанностей на хозяйствующих субъектов, с целью недопущения чрезмерного обременения последних. Возможно субсидирование, компенсационные меры (в том числе и налоговые льготы), поскольку регулирование в исследуемой области защищает не только интересы частных лиц, но и, в основном, публичные интересы (общественная безопасность).

9.4. Подход США к выработке экономической модели регулирования

По общему правилу, владельцы и операторы критически важной инфраструктуры должны работать с федеральным правительством на добровольной основе. Иными словами предполагается, что обмен информацией с федеральным правительством об оценках уязвимости, оценке рисков и принятии дополнительных защитных мер должен быть добровольным.

Однако в некоторых сферах предъявляются существенные обязательные требования к принимаемым мерам безопасности, например:

Атомные электростанции должны соответствовать очень специфическим стандартам для оценки их уязвимости к весьма специфическим типам атак и принимать необходимые меры для устранения этих уязвимостей. Комиссия по ядерному регулированию обеспечивает соблюдение этих норм.

Закон о безопасности морских перевозок (P.L. 107-295) требует, чтобы средства в портах и на некоторых судах проводились оценки уязвимости, а также разрабатывали и реализовывали планы безопасности (включая назначение сотрудника по безопасности, который отвечает за разработку и реализацию этих планов). Оценки уязвимости и планы безопасности рассматриваются Береговой охраной.

Закон о безопасности общественного здравоохранения и готовности к биотерроризму (P.L. 107-188) требует от общинных систем питьевого водоснабжения проведения оценок уязвимости и включения результатов этих оценок в свои планы реагирования на чрезвычайные ситуации. Оценки уязвимости должны быть представлены в Агентство по охране окружающей среды (EPA). Агентство по охране окружающей среды также должно получить сертификацию о том, что планы аварийного реагирования были соответствующим образом изменены, чтобы отразить оценки уязвимости.

Этот же закон также внес поправки в Федеральный закон о продуктах питания, медикаментах и косметике, требующий от всех учреждений, занимающихся производством, переработкой, упаковкой или хранением продуктов питания для потребления, регистрироваться в Министерстве здравоохранения и социальных служб. Кроме того, в Закон о пищевых продуктах и медикаментах были внесены поправки, в соответствии с которыми требуются нормативные акты, определяющие типы информации, которую эти учреждения должны регистрировать в течение определенного периода времени, чтобы определить, является ли пищевой продукт фальсифицированным и представляет собой опасность для общественного здравоохранения.

На другом конце спектра находятся такие секторы, как информационная и телекоммуникационная, нефтегазовая и коммерческая (то есть, торговые центры и офисные здания), где аналогичные меры (такие, как оценка уязвимости и другие) поощряются, но не являются обязательными.

Кроме того, внедрение на федеральном уровне более полного регулирования кибербезопасности критически важных объектов инфраструктуры сталкивается с трудностями. Так, администрация Президента Обамы столкнулась с тем, что отраслевые группы были обеспокоены соотношением дополнительных расходов и преимуществ, а также потенциальным дублированием требований к отчетности, связанных с дополнительными правилами[81].

10. Ответственность в сфере обеспечения безопасности КИИ

10.1. Сравнительно-правовой анализ подходов различных юрисдикций к вопросу ответственности в сфере КИИ (ЖВУ)

В большинстве анализируемых правопорядков предусмотрена ответственность за неисполнение обязанностей субъекта КИИ и за неправомерное воздействие на объекты КИИ. Основные виды ответственности в указанной сфере:

- уголовная (Германия, РФ, Грузия, Казахстан, Сингапур);
- административная (Германия, Великобритания, США, Казахстан, Сингапур, Китай, Япония).

В части административной ответственности, а именно размеров штрафов, считаем возможным обратиться к опыту Великобритании (с соразмерным уменьшением предусматриваемых штрафов до разумных пределов). Также целесообразным представляется подход Казахстана к дифференциации размера штрафа в зависимости от того, является и предприятие малым бизнесом или крупным. В вопросах уголовной ответственности возможно обратиться к российскому подходу и установить максимальную меру – 10 лет лишения свободы за неправомерное воздействие на объекты КИИ. К вопросу

[81] Congressional Research Service. Critical Infrastructures: Background, Policy, and Implementation. URL: https://fas.org/sgp/crs/homesec/RL30153.pdf (дата обращения: 21.05.2019г.).

установления уголовной ответственности также необходимо подходить дифференцированно (в зависимости от наступивших последствий). Следовательно, состав соответствующего преступления должен быть исключительно материальным. Вместе с тем, использование состава оставления в опасности также допустимо.

10.2. Подход ЕС к ответственности в сфере КИИ: наднациональное регулирование, подход Германии и Соединенного Королевства

Директива NIS не содержит конкретных норм об ответственности. Непосредственно исследуемые акты в Германии также не содержат норм об ответственности (однако указанное не значит, что таковая не установлена в соответствующем отраслевом законодательстве).

Для немецкого подхода характерно установление как административной, так и уголовной ответственности. Так, ст. 14 закона BSIG предусматривает ответственность в размере до 50 или до 100 тысяч евро, в зависимости от категории нарушения. При этом административное правонарушение может быть совершено как умышлено, так и по неосторожности.

В части уголовной ответственности в Германии согласно ч. 4 ст. 303 b Уголовного кодекса ФРГ содержит квалифицированный состав – компьютерный саботаж, который повлиял на снабжение населения ЖВУ (атака на критическую информационную инфраструктуру). За атаку на критическую информационную инфраструктуру предусматривается наказание в виде лишения свободы на срок от 6 месяцев до 10 лет[82].

Интересно, что выше обозначенный британский статут 2018 года содержит внушительные размеры штрафных санкций, налагаемых уполномоченным органом: до 1 миллиона фунтов за нарушение, которое не может привести к инциденту; 3,4 миллиона за существенное нарушение, 8,5 миллионов за существенное нарушение в течение длительного периода времени; 17 миллионов за нарушение, которое вызвало или могло вызвать угрозу жизни или ущерб экономике Соединенного Королевства.

10.3. Подход РФ к ответственности в сфере КИИ

Норма статьи 14 ФЗ О безопасности КИИ не содержит конкретных положений об ответственности за неисполнение требований законодательства в сфере защиты КИИ, а носит бланкетный характер.

Наказание за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации предусмотрено в ст. 274.1. УК РФ. Максимальное наказание по особо квалифицированному составу составляет 10 лет лишения свободы. Также возможно привлечение лица к административной ответственности за неисполнение законного предписания государственного органа.

10.4. Подход США к ответственности в сфере КИИ

Сложность модели регулирования КИИ, специфика правовой системы США, роль судебного прецедента – все это делает затруднительным исследование конкретных мер ответственности за те или иные нарушения в области обеспечения безопасности КИИ.

[82] Strafgesetzbuch (StGB) URL: https://www.gesetze-im-internet.de/stgb/index.html#BJNR001270871BJNE068403123 (дата обращения: 30.06.2019).

Следует отметить, что среди применяемых мер ответственности, могут применяться денежные штрафы, а также судебные запреты для принуждения к соблюдению или прекращения эксплуатации объекта, не соответствующего требованиям.

10.5. Подход Грузии к ответственности в сфере КИИ

Уголовный закон Грузии предусматривает в статьях 284, 324,1 уголовную ответственность за самовольное проникновение в компьютерную систему и за кибертерроризм, то есть противоправное завладение охраняемой законом компьютерной информацией, ее использование или угроза использованием, создающие опасность наступления тяжких последствий, совершенные в целях устрашения населения или (и) воздействия на орган власти. Других релевантных составов преступлений и проступков в исследуемой сфере законодательство Грузии не содержат.

10.6. Подход Казахстана к ответственности в сфере КИИ

Законодательство РК об административной ответственности в ст. 641 содержит ответственность за нарушения в сфере защиты КИИ. Ст. 205 УК РК также предусматривает уголовную ответственность за неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций.

10.7. Подход Сингапура к ответственности в сфере КИИ

Стороны, которые были уведомлены Комиссаром в качестве соответствующих владельцев КИИ, несут установленную Законом обязанность соблюдать кодексы и указания и сообщать об инцидентах Комиссару. Они также обязаны проводить регулярные проверки и оценки рисков для уязвимостей кибербезопасности. За несоблюдение этих обязательств предусмотрены значительные уголовные и гражданско-правовые санкции.

11. Выводы

На основании проведенного исследования можно сделать следующие общие выводы и предложить ряд рекомендаций по отдельным аспектам регулирования в сфере КИИ.

В части нормативно-правового регулирования вопросов защиты КИИ представляется перспективным обеспечить наличие главного акта по указанным вопросам (по аналогии с европейской Директивной NIS или российским ФЗ О безопасности КИИ). При этом российский подход представляется более перспективным, так как Директива, конечено, направлена на унификацию, однако, ФЗ является намного более «связывающим» регулированием, не допускающим отхождений. В Киргизии оптимальным было бы регулирование указанного вопроса на уровне закона и надлежащее обеспечение такового подзаконными НПА.

Терминологический аппарат может строиться в зависимости от выбранного подхода: через определение объектов КИИ или ЖВУ. При этом, вне зависимости от выбранной модели определенные термины должны быть отражены в соответствующем законе о безопасности КИИ, например: компьютерный инцидент или безопасность (объекта или услуги). В отношении некоторых терминов можно обратиться к зарубежному законодательству. Так, определение безопасности КИИ не через состояние полной защищенности, но через снижение рисков до приемлемого уровня, характерное для американского подхода. Вместе с тем, основной терминологический аппарат может быть заимствован из российского законодательства с включением ряда дополнительных

определений. При этом, отдельные определения необходимо заимствовать осторожно, не допуская терминологических коллизий. Любое заимствование должно проводиться с учётом уже существующих особенностей законодательства Киргизии в сфере информации и информационных технологий.

Большое внимание следует уделить принципам обеспечения безопасности КИИ, поскольку они определяют основы всей системы регулирования в сфере КИИ, являются ориентиром для толкования положений законодательства как субъектами КИИ, так и правоприменительными органами. Помимо закрепления общих принципов (таких как обеспечение законности и защиты прав и свобод) представляется важным ориентироваться на изложенный в общей части 3 раздела настоящего исследования расширенный перечень принципов регулирования сферы безопасности КИИ.

По предмету регулирования выделяются 2 подхода. Один регулирует объекты КИИ, а другой субъектов и их деятельность (ЖВУ). При этом объектный критерий является более удачным вариантом на стадии формирования системы безопасности КИИ, поскольку представляет собой четкий перечень категорий объектов, снижает степень усмотрения субъектов КИИ по вопросу категорирования и обеспечения безопасности, а также снижает коррупционные риски путем определения конкретных полномочий и прозрачных требований, предъявляемых уполномоченными органами. При этом, достигаемый результат в объектном подходе предполагается аналогичным результату, достигаемому субъектно-деятельностным подходом.

Выбор объектного подхода требует установления четких критериев категорирования объектов КИИ путем формирования конкретных «пороговых величин». В данном отношении возможно обратить внимание на «пороговые величины» для каждого сектора и категории объектов, сформулированные в российском и немецком законодательстве.

Одним из критериев для определения объектов КИИ являются сферы экономики, в которых обеспечивается безопасность КИИ. Конкретный перечень сфер зависит от основных критически-важных отраслей хозяйствования и социальной деятельности. Представляется разумным выделить сферы: транспорта; энергетики; здравоохранения; связи; водоснабжения. Вместе с тем, конкретный список сфер зависит от того, какие отрасли являются наиболее значимыми для Киргизии с экономической и социальной точек зрения.

Также необходимо обратить внимание на установление перечня обязанностей для субъектов КИИ. Основными обязанностями невластных субъектов являются: осуществление категорирования объектов, принятие необходимых мер безопасности, взаимодействие с уполномоченными органами, сообщение таковым об инцидентах. С одной стороны, можно предусмотреть конкретные обязанности по отнесению к конкретной категории объектов и для каждой категории установить перечень требуемых мер защиты (РФ, Казахстан). Обратный вариант представлен в европейском и американском законодательстве. Так, например, в соответствии с Директивой NIS, имплементирующие акты стран-членов должны реализовывать риск-ориентированный подход. Для Киргизии представляется разумным закрепить конкретные обязанности субъектов, при этом, в части обязанности по обеспечению безопасности объекта КИИ можно установить не только минимальный набор таковых, но и общее правило о принятии разумных и достаточных мер для обеспечения безопасности, даже если они не приведены в конкретном НПА.

Относительно выбора соответствующих регуляторов (уполномоченных органов в сфере КИИ) представляется перспективным либо создание одного единого органа по

вопросам кибербезопасности, либо наделение уже существующих органов соответствующими полномочиями при создании Национального Центра Кибербезопасности, который будет обеспечивать работу по принципу «одного окна». Огромное разнообразие органов, децентрализация полномочий в указанной сфере не содействуют транспарентности системы. Уполномоченный орган в сфере кибербезопасности, в частности, безопасности объектов КИИ, должен, как минимум, обеспечивать следующие функции: мониторинг инцидентов, хранение записей об инцидентах, проведение проверок (правильности осуществления категорирования и соблюдения мер безопасности КИИ); распространение предупреждений об опасности, подготовка методических рекомендаций об основных угрозах кибербезопасности; реагирование на инциденты, установление причин компьютерных инцидентов, помощь в их ликвидации; расследование, содействие расследованию преступлений в сфере кибербезопасности.

В части экономической модели регулирования необходимо избегать установления несоразмерно затратных требований к хозяйствующим субъектам – владельцам объектов КИИ. В настоящем случае перспективным представляется, во-первых, метод дифференциации и пропорциональности рискам (когда количество обязанностей зависит от категории значимости объекта и риска инцидента на конкретном объекте), во-вторых, принцип содействия (при котором субъект КИИ может обратиться в уполномоченный орган за помощью в осуществлении категорирования, а «корректировка» произведенного категорирования проводится органом без возложения штрафных санкций на хозяйствующий субъект), в-третьих, метод поощрения за выполнение экономически-затратных обязанностей субъекта КИИ.

Указанная сфера регулятивных предписаний требует также санкционного обеспечения. Так, рекомендуется установить административную ответственность за неисполнение обязанностей субъектами КИИ и уголовную за атаки на значимые объекты КИИ. По вопросам административной ответственности рекомендуется также обратиться к опыту Германии и Соединенного Королевства. Административные штрафы также должны быть соразмерны предполагаемым последствиям административного правонарушения. Дифференциацию можно проводить в зависимости от категории значимости и от срока, в который не была исполнена обязанность. В части уголовной ответственности ориентиром может выступить законодательство РФ. При этом, соответствующие составы преступлений должны быть материальными, а норма должна предусматривать квалифицированный и особо-квалифицированный составы, обеспечивая дифференциацию уголовной ответственности в зависимости от тяжести последствий кибератаки.

III. Приложения

Приложение 1: Сравнительно-правовая таблица по подходам к регулированию КИИ (ЖВУ)

Юрисдикция	**Ключевые термины**	**Принципы**	**Предмет регулирования**	**Критерии отнесения к объектам/ категории**	**Сферы**	**Субъекты**	**Публичные органы**	**Экономическая модель**	**Ответственность**
РФ	КИИ - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Безопасность КИИ - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.	Принцип законности Принцип непрерывности и комплексности обеспечения безопасности критической информационной инфраструктуры Принцип взаимодействия ФОИВ и субъектов КИИ Приоритет предотвращения компьютерных атак.	Объекты КИИ	Значимость: Социальная Экономическая Политическая Экологическая Обороны страны, безопасности, правопорядка	Социальная, Экономическая, Политическая, Экономическая, Экологическая, Безопасность и правопорядок	Лица, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в обозначенных выше сферах	Президент Правительство ФСБ ФСТЭК НКЦКИ	Обязанности по исполнению требований ФЗ О безопасности КИИ и подзаконных актов распределены между государственными органами и субъектами КИИ. Вместе с тем, существенное количество финансово затратных обязанностей было возложено исключительно на субъектов КИИ.	Уголовная, административная.

ЕС (наднациональный и национальный уровень)	ОЖВУ - государственное или частное предприятие, оказывающее услуги в определенных сферах (энергетики, транспорта, банковского дела, финансового рынка, здравоохранения, поставки питьевой воды, цифровой инфраструктуры), которые: предоставляют услуги, являющиеся жизненно-важными с точки зрения поддержания важнейшей социальной и/или экономической деятельности; оказывают услуги, которые зависят от сетевых и информационных систем; возможный инцидент может оказать существенное негативное воздействие на оказание услуги. Провайдер цифровых услуг -	Эффективность; Совместимость; Пропорциональность рискам; Конкретность и понятность Возможность проверки	Операторы жизненно-важных услуг и провайдеры цифровых услуг, а также ЖВУ	-	Энергетика; Транспорт; Банковское дело; Финансовый рынок; Здравоохранение; Поставки питьевой воды; Цифровая инфраструктура.	ОЖВУ Провайдеры цифровых услуг Основные обязанности: Принятие необходимых организационных и технических мер защиты Уведомление об инцидентах	Национальный компетентный орган, ответственный за безопасность сетевых и информационных систем (СА). Единый национальный контактный пункт по вопросам безопасности сетевых и информационных систем (SPOC). Группы реагирования на инциденты, связанные с компьютерной безопасностью (CSIRTs).	Обязанность по исполнению требований закона распределена между компетентными органами и ОЖВУ, провайдерами цифровых услуг. Больше требований соответствующие НПА предъявляют к ОЖВУ.	-

	юридическое лицо, оказывающее цифровые услуги (Интернет-магазин, поисковик, облачный сервис). Безопасность сетевых и информационных систем - способность сетевых и информационных систем на заданном уровне уверенности противостоять любым действиям, угрожающим доступности, достоверности, целостности или конфиденциальности хранимых, передаваемых или обрабатываемых данных или связанных с ними услуг, предлагаемых или доступных через указанные сетевые и информационные системы.								

Соединенное королевство	Аналогично ЕС	-	Аналогично ЕС	-	Энергетика; Транспорт; Здравоохранение; Поставки питьевой воды; Цифровая инфраструктура.	Аналогично ЕС	Национальный центр кибербезопасности (NCSC)– контактный пункт; Информационный комиссар (ICO) – компетентный орган для провайдеров цифровых услуг; Офис связи (OFCOM) – компетентный орган для ОЖВУ в сфере информационный инфраструктуры; Национальный центр кибербезопасности (NCSC) – CSIRT	Аналогично ЕС. В Доктрине отдельно подчеркивается обязанность органов управления организаций по выполнению требований.	До 1 миллиона фунтов за нарушение, которое не может привести к инциденту; 3,4 миллиона за существенное нарушение, 8,5 миллионов за существенное нарушение в течение длительного периода времени; 17 миллионов за нарушение, которое вызвало или могло вызвать угрозу жизни или ущерб экономике Соединенного Королевства
Германия	Объект критической инфраструктуры - объект, установка или ее часть, которая относятся к секторам энергетики, информационных технологий, телекоммуникаций, транспорта, дорожного движения, здравоохранения, водоснабжения, питания, финансов, страхования; имеет большое значение для	-	Объекты критическо-важных услуг и критическо-важные услуги.	Относятся к секторам энергетики, информационных технологий, телекоммуникаций, транспорта, дорожного движения, здравоохранения, водоснабжения, питания, финансов, страхования; Имеют большое значение для	Энергетика; Водный сектор; Питание; IT и телеком; Здравоохранение; Финансы и страхование; Транспортный сектор.	ОКИ Провайдеры цифровых услуг Обязанности аналогичны ЕС	Федеральный офис информационной безопасности	Обязанность по исполнению требований закона распределена между компетентными органами и ОКИ провайдерами цифровых услуг. Больше требований соответствующие НПА предъявляют к ОКИ.	Административная: до 50 или до 100 тысяч евро, в зависимости от категории нарушения Уголовная: Компьютерный саботаж, который повлиял на снабжение населения ЖВУ (атака на критическую информационную инфраструктуру) наказывается лишением свободы на срок от 6 месяцев до 10 лет.

	функционирования сообщества, потому что отказ в их работе или ухудшение их функционирования приведет к значительному дефициту поставок или угрозе для общественной безопасности.			функционирования сообщества, потому что отказ в их работе или ухудшение их функционирования приведет к значительному дефициту поставок или угрозе для общественной безопасности.					
США	Критическая инфраструктурак (critical infrastructure) - системы и активы, физические ли виртуальные, настолько жизненно важные для США, что нарушение функционирования или разрушение таких систем и активов окажет разрушительное влияние на безопасность, национальную экономическую безопасность, национальное здравоохранение или охрану здоровья или любое сочетание этих вопросов	Уточнение и уточнение функциональных отношений между федеральным правительством для продвижения национального единства усилий по укреплению безопасности и устойчивости критической инфраструктуры; Обеспечение эффективного обмена информацией путем определения базовых данных и системных требований для федерального	Деятельность и услуги в определенных секторах	Критерии не определены. Установлены шестнадцать критических секторов	Химический сектор Сектор коммерческих объектов Сектор коммуникаций Сектор критического производства: Плотины Военно-промышленная база Аварийно-спасательные службы Энергетика Финансовые	Владельцы и операторы критической инфраструктуры	Министр внутренней безопасности Отраслевые агентства по числу критических секторов Иные органы федеральной власти в пределах определенной для них компетенции	-	Сочетание уголовной и административной ответственности

	Ключевые активы – потенциальные цели, разрушение которых не ставит под угрозу жизненно важные системы, но может создать локальную катастрофу или серьезно повлиять на национальный моральный дух (например, национальные памятники, исторические достопримечательности, плотины, ядерные объекты, крупные торговые центры, в том числе, офисные здания и спортивные стадионы, где собирается большое количество людей. Устойчивость - означает способность подготовиться к изменяющимся условиям и адаптироваться к ним, а также выдерживать и быстро восстанавливаться после сбоев; включает в себя способность	правительства; а также Внедрение функции интеграции и анализа для информирования о планировании и принятии операционных решений в отношении критически важной инфраструктуры			услуги Продовольствие и сельское хозяйство Государственные учреждения Здравоохранение и общественное здоровье Информационные технологии Ядерные реакторы, материалы и отходы Транспортные системы Системы водоснабжения, сбора и отведения сточных вод				

	противостоять и восстанавливаться после преднамеренных атак, аварий или естественных угроз или инцидентов. Безопасность - снижене риска для критически важной инфраструктуры с помощью физических средств или защитных кибер-мер в отношении вторжений, атак или последствий стихийных бедствий или техногенных катастроф.								
Грузия	Информационная безопасность – деятельность, обеспечивающая соблюдение правил доступа, единства, аутентичности, конфиденциальности информации и информационных систем и их работы в течение длительного времени Критическая информационная система – информационная система, непрерывное	-	Субъекты КИИ	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	–	Субъект критической информационной системы	Группа помощи Агентства по обмену данными по реагированию на компьютерные инциденты Бюро кибербезопасности; Директор Бюро кибербезопасности; Группа помощи Бюро кибербезопасности по реагированию на компьютерные инциденты	-	Уголовная

	функционирование которой имеет важное значение для обороны или (и) экономической безопасности страны, нормального функционирования органов государственной власти или (и) общества. 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			(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.			Отдел по борьбе с киберпреступностью Центрального отделения криминальной полиции при МВД; Национальная комиссия Грузии по коммуникациям.		

Казахстан	Информационная безопасность в сфере информатизации - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз Критически важные объекты информационно-коммуникационной инфраструктуры - объекты информационно-коммуникационной инфраструктуры, в том числе информационно-коммуникационной инфраструктуры «электронного правительства», нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для	соблюдение законности при осуществлении деятельности по обеспечению национальной безопасности; приоритет прав и свобод человека и гражданина; оперативное взаимное информирование и согласованность действий сил обеспечения национальной безопасности; единство, взаимосвязь и сбалансированность всех видов национальной безопасности, оперативное изменение их приоритетности в зависимости от развития ситуации; приоритетность предупредительно-профилактических мер при обеспечении национальной безопасности;	Объекты КИИ	Влияние объекта информационно-коммуникационной инфраструктуры на непрерывную эксплуатацию особо важных государственных объектов, при нарушении функционирования которого будет остановлена деятельность особо важных государственных объектов. Влияние объекта информационно-коммуникационной инфраструктуры на непрерывную и безопасную эксплуатацию стратегических объектов, при нарушении функционирования которого будет остановлена деятельность стратегических объектов либо	Государственные услуги Транспорт Нефтегаз Космический сектор Энергетика Металлургия	Оперативные центры по информационной безопасности	Правительство Республики Казахстан в сфере информатизации. Комитет по информационной безопасности. Уполномоченный орган в сфере обеспечения информационной безопасности. Центральные государственные и местные исполнительные органы. Уполномоченные органы в сфере обороны, гражданской защиты и органы национальной безопасности.	-	Административная и уголовная ответственность.

	обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории; Информационная безопасность - состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны	своевременность и адекватность мер обеспечения национальной безопасности масштабам и характеру нанесенного и (или) потенциального ущерба национальной безопасности; соблюдение баланса интересов человека и гражданина, общества и государства, их взаимная ответственность; контролируемость реализации всей совокупности действий по защите национальной безопасности; интеграция системы обеспечения национальной безопасности с международными системами безопасности;		возникает угроза чрезвычайной ситуации техногенного характера. Влияние объекта информационно-коммуникационной инфраструктуры на непрерывную и безопасную эксплуатацию объектов отраслей экономики, имеющих стратегическое значение, при нарушении функционирования которого будет остановлена деятельность объектов отраслей экономики, имеющих стратегическое значение, либо возникает угроза чрезвычайной ситуации техногенного характера.					

		четкое разграничение полномочий государственных органов.		Влияние объекта информационно-коммуникационной инфраструктуры на обеспечение устойчивого функционирования объекта информатизации "электронного правительства" и иных информационно-коммуникационных услуг, частичное или полное нарушение (прекращение) функционирования которых может привести к чрезвычайной ситуации социального характера.					

Сингапур	КИИ - компьютер или компьютерная система, которая необходима для непрерывного предоставления основных услуг, связанных с утратой или изнурительными воздействиями на национальную безопасность, оборону, международные отношения, экономику, общественного здравоохранения, общественной безопасности или общественного порядка Сингапура.	-	-	-	Энергетика; Информационные коммуникации; Водоснабжение; Здравоохранение; Банковское дело и финансы; Охранные и аварийные службы; Авиация; Наземный транспорт; Морской транспорт; Правительство; Средства массовой информации.	-	Национальные отраслевые контрольные или надзорные департаменты; Национальный отдел кибербезопасности и информатизации; Подразделения Государственного совета по общественной безопасности, государственной безопасности, административному управлению защитой государственной тайны, управлению государственным шифрованием	-	Уголовная и ГПО
КНР	КИИ относится к национальной безопасности, национальной экономике и средствам существования людей, в сферах, включающих информационные сети, энергетику, финансы, транспорт, образование, научные	Уважение к сохранению суверенитета киберпространства. Мирное использование киберпространства Управление киберпространством в	-	-	Отрасли: здравоохранение, образование, социальное обеспечение и защита окружающей среды; Информационные сети: радио и телевизионные сети, интернет; поставщики услуг, предоставляющие	Операторы КИИ	-	-	-

	исследования, охрану водных ресурсов, промышленное производство, медицину и здравоохранение, социальное обеспечение, коммунальные услуги и другие важные информационные системы.	соответствии с законом Координация безопасности и развития сети			облачные вычисления, большие данные и другие крупные общедоступные информационные и сетевые услуги; Научные исследования и производство: оборонная промышленность, крупная промышленность оборудования, нефтехимическая и пищевая и фармацевтическая промышленность; СМИ и новости: радиостанции, телевизионные станции и службы новостей.				
Япония	Кибербезопасность - условия, при которых принимаются меры, необходимые для предотвращения утечки, потери или повреждения, а также для другого управления безопасностью информации, которая записывается, отправляется, передается или	Свободное перемещение информации; Уважение к правам граждан; Соблюдение интересов всех заинтересованных сторон; Сотрудничество субъектов КИИ.	-	-	Информационные и коммуникационные технологии; Финансовый сектор; Авиация; Железнодорожное сообщение; Электричество; Газ;	-	-	-	-

	принимается с использованием электронного метода, магнитного метода или любого другого метода, не распознаваемого человеческими чувствами.				Правительство и государственные службы (включая местные органы власти); Медицина; Водоснабжение; Логистика.				