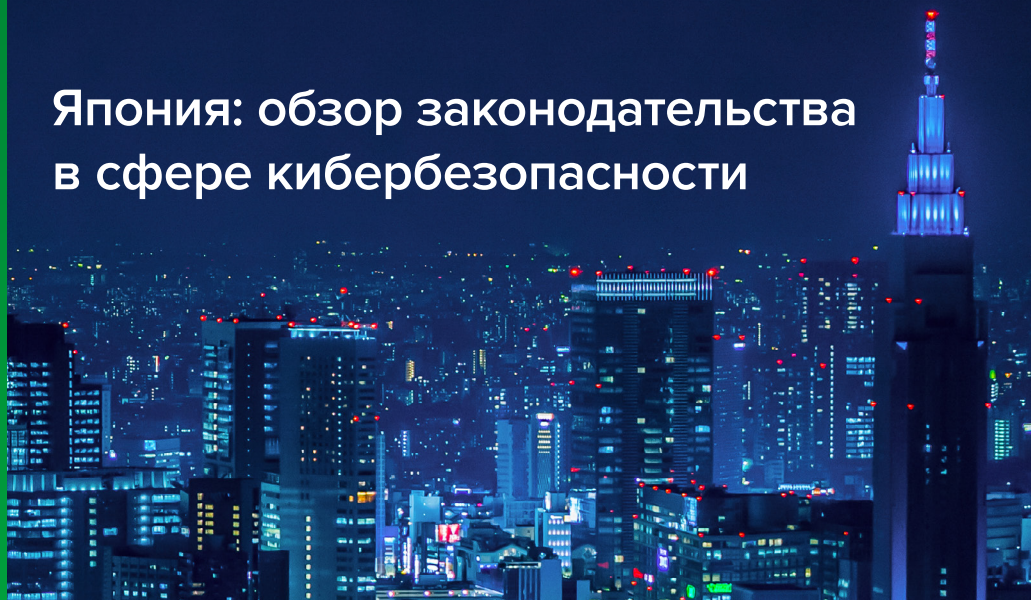
INFOWATCH®

Япония: обзор законодательства в сфере кибербезопасности



Оглавление

Аннотация

Представляем результат исследования сферы кибербезопасности Японии, в котором мы постарались дать общее представление об основных законодательных актах и органах власти, регулирующих данную область.

Наш интерес к Японии вызван тем, что она является одной из наиболее экономически развитых стран, в том числе в области информационных технологий и электронной промышленности, а также нашим соседом.

Обзор основан на анализе японских источников информации, опубликованных на японском и английском языках, а также данных Всемирного банка (World Bank), Международного союза электросвязи (МСЭ) и ряда других организаций. По возможности предпочтение отдавалось языку оригинала, а перевод производился с учётом российских определений.

Индексы и критерии

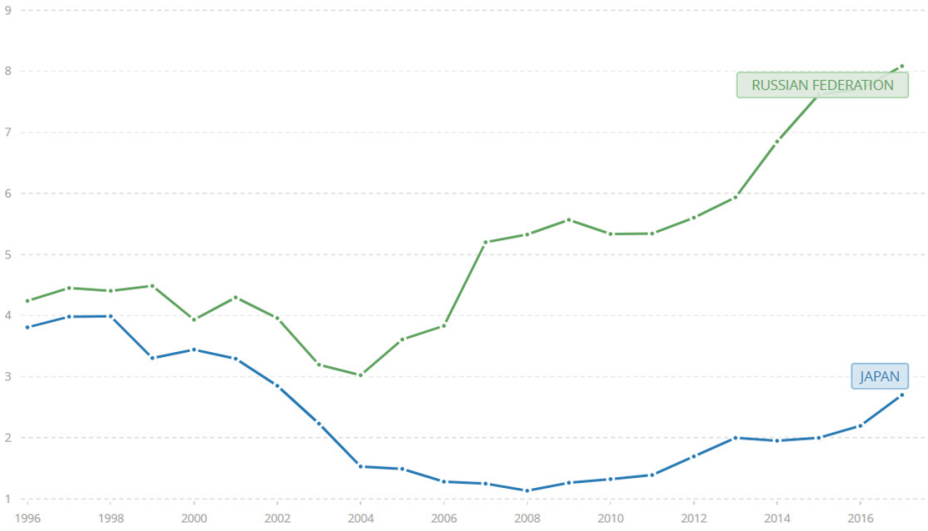
Экономика: ИКТ

Япония — страна с одним из самых высоких уровней вовлечённости населения в информационно-коммуникационные технологии (ИКТ). Ещё в 2017 показатель домашних хозяйств, у которых есть доступ в интернет, составил 97,2% . Это второе место в мире после Южной Кореи, показатель которой составил 99,2%. Показатель России составил 74,8%.

Япония также занимает 10 место в Индексе развития ИКТ [1] (последние данные доступны по состоянию на 2017)[2] Международного союза электросвязи (МСЭ). Для сравнения, Республика Корея находится на 2 месте, Сингапур — на 18, Россия — на 45.

Несмотря на высокие показатели, согласно исследованию «Japan cyber readness at a glance» [2] Потомакского института политических исследований (США), **доля экспорта товаров и услуг ИКТ из Японии** в 2012–2014 падала — с 5% до 3,3%. По данным Всемирного банка, показатели экспорта ИКТ-услуг из Японии (в % от общего объёма экспорта услуг) в 2013–2014 также незначительно снижались — с 1,998% до 1,953%, но к 2017 показатель экспорта вырос и составил уже порядка 2,7%. Наглядно показатели представлены на рисунке ниже (последние доступные данные — 2017):

Рисунок 1. Экспорт ИКТ-услуг из Японии и России (в % от общего объёма экспортируемых услуг), данные Всемирного банка [3]



Доступна также статистика по экспорту ИКТ-товаров из Японии. В этом показателе известные данные относятся к 2019. Результаты представлены на рисунке 2. Как видно, в 2012–2014 тоже наблюдался спад — с 9,1% до 8,4%. На 2019 данный показатель всё ещё находился примерно на уровне 8%.

Принимая во внимание вышеописанные факты, уже тогда правительство Японии начало предпринимать шаги по исправлению ситуации, сделало ставку на развитие ИКТ как двигателя, в перспективе способного вытянуть экономику из стагнации, в том числе за счёт развития рынка Интернета вещей (IoT).

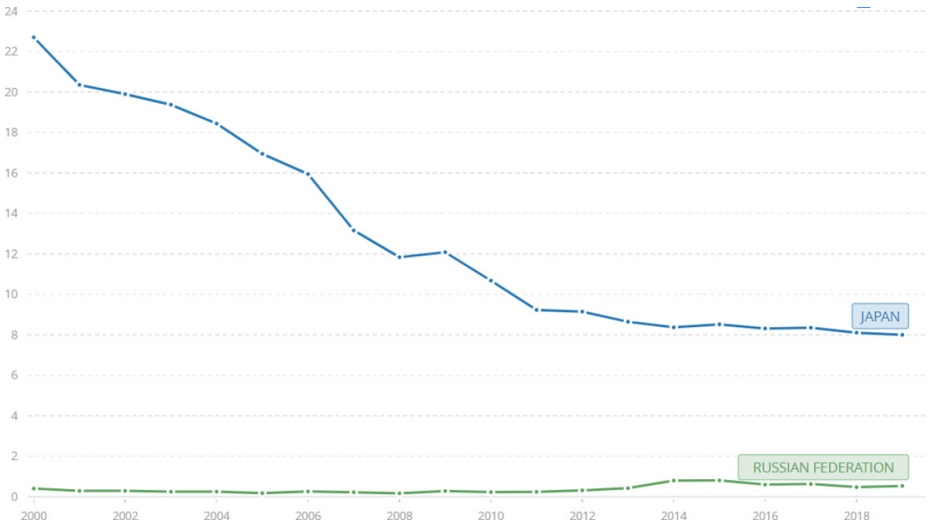
С тех пор правительство осуществляет активную работу для создания условий развития ИКТ-сектора в области создания передовой ИКТ-инфраструктуры, а также наращивая национальный потенциал в области кибербезопасности, поскольку развитие сектора, его экономический рост возможны лишь тогда, когда обеспечена безопасность инфраструктуры и данных.

---

1 ICT Development Index (IDI)

2 После 2017 у исследователей МСЭ возник вопрос о корректности данных расчетов, начата разработка новой методики, которая до сих пор не завершилась, поэтому индексы за 2018–2020 не выпускались

Рисунок 2. Экспорт ИКТ-товаров Японии и России (в % от общего объёма экспорта товаров), данные Всемирного банка [4]



Интересно, что несмотря на уровень развития Японии в области ИКТ, в самой стране не слишком охотно расстаются с традиционными методами финансовых расчётов и принимают цифровые технологии: например, по части платежей. До сих пор в большинстве небольших магазинов, ресторанов и даже вендинговых автоматах нельзя расплатиться банковской картой — необходимы наличные. Сравнительно недавно стали доступны бесконтактные платежи.

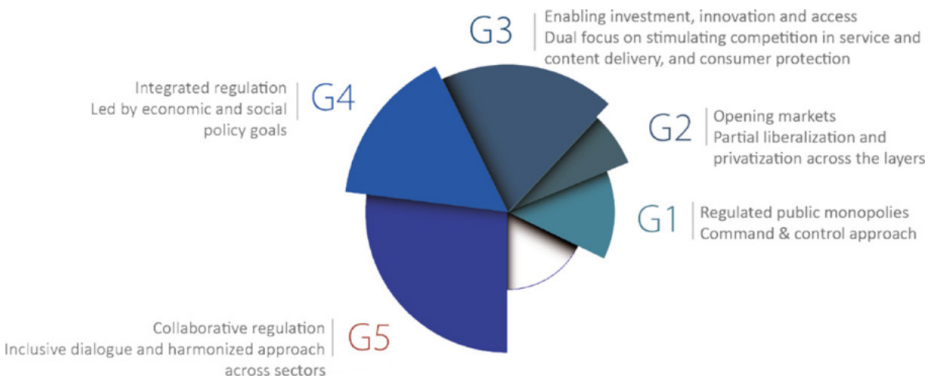
Концепция «поколений регулирования»

Международный союз электросвязи (МСЭ) разработал оригинальную методику для расчёта индекса развития нормативно-правовых баз в области информационно-коммуникационных технологий. По результатам его исследования в отчёте «Digital trends in Asia and the Pacific 2021» [5] отражено, что Япония относится к 16 передовым странам, имеющим целостную нормативно-правовую базу в области ИКТ.

Кроме того, с периодичностью раз в два года МСЭ выпускает отдельный отчёт «Global ICT Regulatory Outlook» (GIRO) [6], в котором оценивает уровень развития нормативно-правовых баз 193 стран. **Методика охватывает 25 критериев,** поэтому контрольный показатель рассматривает все аспекты регулирования в области ИКТ и помогает анализировать уровень зрелости современных нормативно-правовых баз. Данный показатель используется для оценки пробелов в законодательной базе, предлагает пути улучшения нормативно-правовой среды, позволяет отслеживать прогресс и предоставляет решения для достижения целей цифровой трансформации. Показатель также демонстрирует, как тесно уровень регулирования в сфере ИКТ связан с развитием рынка.

МСЭ введена концепция «поколений регулирования»: от стран категории G1 с подходом «командование и контроль» в правовом регулировании до стран категории G5, политика в области ИКТ которых основана на сотрудничестве между регуляторами.

Рисунок 3. Концепция «поколений регулирования»



Лидирующая категория G5 — обширное понятие, оно означает фундаментальный сдвиг в способах регулирования, целостную политическую основу и объединение всех заинтересованных сторон, от политиков, отраслевых и межотраслевых регуляторов до небольших участников рынка. Совместное регулирование управляется путём лидерства, открытых диалогов и обсуждений, нежели путём командования и контроля.

Разница между поколениями представлена на рисунке 3.

Итоги исследования говорят о следующем:

- Только **8%** стран относятся к категории **G5**. Это страны, имеющие целостное правовое регулирование как основу, способствующую цифровой трансформации общества
- Немногим более четверти стран (**27%**) достигли уровня **G4**. Эти страны имеют интегрированный подход к регулированию ИКТ, руководствуются социальными и экономическими целями, имеют развитый ИКТ-рынок и низкий процент неподключённого к интернету населения
- Четверть из всех стран прошли лишь половину пути, добиваются устойчивого прогресса по укреплению политической и нормативной базы
- Более половины населения мира сосредоточено в странах категорий **G2 (29%)** и **G3 (26%)**, готовых совершить рывок ко всеобщему охвату цифровыми технологиями и в перспективе возглавить динамичные рынки ИКТ
- Почти 40% остаются в категориях **G1 (10%)** или **G2 (29%)**

Полный список стран категории G5 выглядит следующим образом:

Таблица 4. Страны пятого поколения регулирования

	Country	Region	ICT Regulatory Tracker Score	G5 Benchmark	Combined Score	GEN
1	Norway	Europe	95.5	39	134.5	G5
2	United Kingdom	Europe	95	37	132	G5
3	Singapore	Asia-Pacific	91.5	39	130.5	G5
4	Croatia	Europe	94	36	130	G5
5	Germany	Europe	93.5	36	129.5	G5
6	Romania	Europe	92	36	128	G5
7	Netherlands	Europe	93	35	128	G5
8	Kenya	Africa	87.5	37	124.5	G5
9	Estonia	Europe	87	37	124	G5
10	Sweden	Europe	89	35	124	G5
11	Brazil	Americas	88.5	35	123.5	G5
12	Morocco	Arab States	88.5	35	123.5	G5
13	Canada	Americas	85.5	37	122.5	G5
14	Spain	Europe	86	36	122	G5
15	Albania	Europe	83	35	118	G5
16	Japan	Asia-Pacific	72.5	37	109.5	G5

Global ICT Regulatory Outlook 2020

Как видно из таблицы выше, Япония замыкает список стран-лидеров и занимает 16 место. Отметим, что своё место она заняла при последнем расчёте индекса. Согласно предыдущим отчётам, она перешла в G5 сразу из категории G3.

Согласно данному исследованию, например, **Россия, Беларусь, Казахстан и Китай относятся к категории G2**, что означает, эти страны только готовы совершить скачок к цифровой трансформации. При этом исследователи и авторы индекса также отмечают, что страна из категории G2 способна сразу попасть в категорию G4 или G5.

Индекс киберготовности CIR 2.0

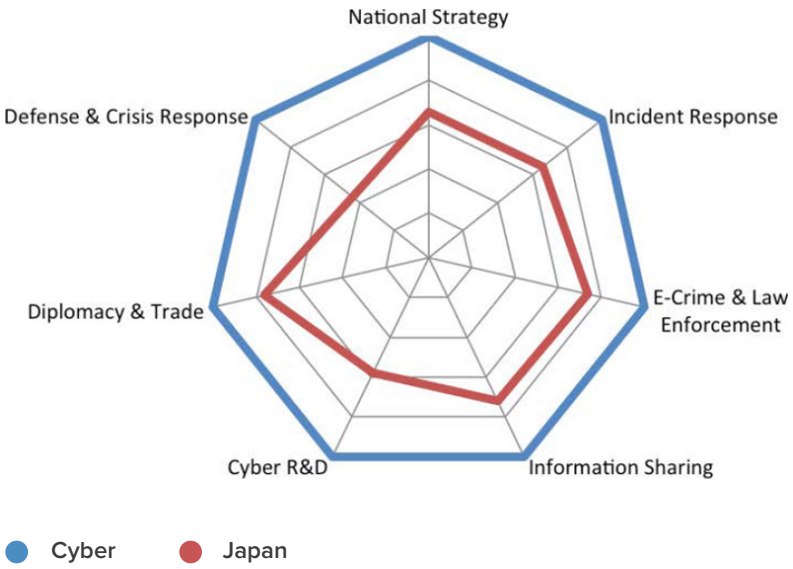
Потомакский институт политических исследований (США) разработал **индекс киберготовности — Cyber Readiness Index (CRI) 2.0.** Методология разработана специально для оценки уровня готовности стран к отражению киберугроз.

Данный индекс оценивает положение и возможности страны по 7 показателям:

1. Национальная стратегия
2. Реагирование на инциденты
3. Киберпреступность и охрана правопорядка
4. Обмен информацией
5. Инвестиции в исследования и разработки
6. Дипломатия и торговля
7. Оборона и кризисное реагирование

По оценке авторов индекса, на текущий момент ни одна из стран не находится в состоянии полной готовности к отражению киберугроз, однако **Япония соответствует требованиям шести из семи элементов**. Значения показателей отображены на рисунке ниже.

Рисунок 5. Оценка положения Японии по Индексу киберготовности



Таким образом, исходя из рисунка выше, можно оценить соответствие Японии требованиям:

- Национальная стратегия — более 60%
- Реагирование на инциденты — более 60%
- Киберпреступность и охрана правопорядка — почти на 80%
- Обмен информацией — почти на 80%
- Инвестиции в исследования и разработки — на 60%
- Дипломатия и торговля — на 80%
- Оборона и кризисное реагирование — чуть более 40%

В Японии кибератаки рассматриваются как одна из основных угроз национальной безопасности [7], поэтому кибербезопасности в стране уделено особое внимание: законодательная база, в том числе стратегия национальной кибербезопасности, тщательно пересматривается и постоянно обновляется. На правительственных ресурсах публикуются ежегодные отчёты о политике кибербезопасности страны (данные доступны с 2007).

Рассмотрим нормативно-правовую базу Японии в области кибербезопасности подробнее.

Определения в законодательстве Японии

Кибербезопасность

По аналогии с российскими определениями, термин «кибербезопасность»[3] 「サイバーセキュリティ」 в японском законодательстве можно перевести таким образом — это меры, которые необходимо предпринимать для управления информацией в целях обеспечения её безопасности, в том числе:

- Обеспечить превентивную защиту от утечек, модификации или удаления (утраты) данных, которые хранятся и передаются с помощью электромагнитных и других средств, не распознаваемых с помощью органов чувств человека
- Гарантировать защиту информационных систем и информационно-телекоммуникационных сетей (включая превентивные меры против умышленных действий в отношении компьютеров через информационную сеть или носителей информации, созданной с помощью электронных или магнитных средств)

Киберпреступление

Чтобы ратифицировать Будапештскую конвенцию о киберпреступлениях, в 2011–2012 Япония внесла изменения в свой Уголовный (с 14 июля 2011) и Уголовно-процессуальный (с 22 июня 2012) кодексы.

Криминализировано создание и распространение компьютерных вирусов, которые в Уголовном кодексе определены как «создание электромагнитных записей, содержащих несанкционированные команды». За данное нарушение предусмотрено наказание в виде лишения свободы сроком до 3 лет или штрафа размером до 500 000 иен (около $4500). За получение и хранение компьютерных вирусов полагается также наказание в виде лишения свободы сроком до 2 лет или штрафа размером до 300 000 иен (около $2700).

Криминализирована попытка стороннего вмешательства в работу компьютерных систем. За это кодекс предусматривает наказание в виде лишения свободы сроком до 5 лет или штрафа до 1 000 000 иен (около $9100). Например, преступлением будет считаться даже попытка взлома сети, заблокированная межсетевым экраном.

Кроме того, в законе «О запрете несанкционированного доступа» есть отдельная статья, которая состоит всего из одного предложения: **«Никто не должен заниматься несанкционированным доступом».**

В качестве сравнения: в России с 1 января 1997 в новом Уголовном кодексе существует 28 глава «Преступления в сфере компьютерной информации». 272 статья также предусматривает уголовную ответственность за несанкционированный доступ; 273 — за создание, использование и распространение вредоносных компьютерных программ, а 274 — за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. С 2018 введена статья 271.1, устанавливающая ответственность за вмешательство в деятельность и нанесение вреда КИИ Российской Федерации.

3 For the purposes of this Act, the term “Cybersecurity” means the necessary measures that are needed to be taken to safely manage information, such as prevention against the leak, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive functions (hereinafter in this section referred to as “Electronic or Magnetic Means”); and to guarantee the safety and reliability of information systems and information and telecommunications networks (including necessary preventive measures against malicious activities toward electronic computers through information network or storage media for information created by electronic or magnetic means (hereinafter referred to as “Electronic or Magnetic Storage Media”), and that those states are appropriately maintained.

Основные законодательные акты

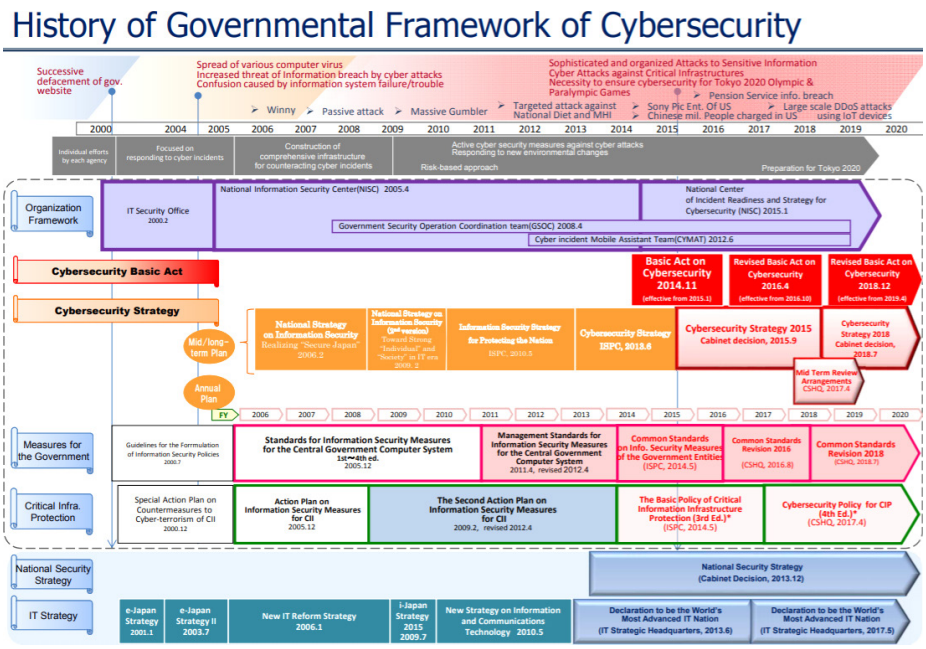
В Японии политику в области кибербезопасности определяет следующий законодательный акт:

Основной закон о кибербезопасности (№104, 2014) [8]. Законодательный акт основан на принципах, определённых в «Основном законе о формировании современного информационно-телекоммуникационного сетевого общества»

В ходе реализации его требований был создан **Стратегический штаб по обеспечению кибербезопасности**, а также в 2015 разработана **Стратегия кибербезопасности**, её актуальная версия опубликована в 2018. Данная стратегия устанавливает основные цели политики в области кибербезопасности, направлена на обеспечение кибербезопасности государственных структур, объектов критической информационной инфраструктуры и других, а редакция 2018 года содержит отдельный раздел, посвящённый кибербезопасности во время проведения Олимпийских и Паралимпийских игр в Токио, которые должны были состояться в 2020.

Подробнее ретроспектива принятия законодательных актов в сфере кибербезопасности представлена на схеме ниже:

Рисунок 6. История государственной системы кибербезопасности



Рассмотрим примеры законодательных актов, в составе которых также уделено внимание кибербезопасности.

Основной закон о формировании современного информационно-телекоммуникационного сетевого общества (№144, 2000) [9]

Закон основывается на четырёх принципах политики Японии в этой области: свободное перемещение информации, уважение к правам граждан, соблюдение интересов всех заинтересованных сторон и их сотрудничество. Данный закон определяет «Общество передовых информационно-телекоммуникационных сетей» как общество, в котором доступно творческое и динамичное развитие во всех областях путём получения, совместного использования или передачи информации по всему миру в свободном и безопасном виде через интернет и другие современные информационно-телекоммуникационные сети.

Закон предписывает необходимость реализации мер по обеспечению кибербезопасности информационно-телекоммуникационных сетей, а также в новой редакции определяет круг полномочий Стратегического штаба по кибербезопасности.

Основной закон об использовании данных в государственном и частном секторе (№103, 2016) [10]	Законодательный акт определяет обязанности государства, местных общественных организаций и компаний, предусматривая основные принципы в отношении развития и использования данных государственного и частного сектора. Термин «данные государственного и частного сектора» означает информацию, записанную на электромагнитном носителе и используемую в государственных, муниципальных и административных органах.
Закон о защите персональных данных (№57, 2003) [11]	Закон направлен на защиту прав и интересов граждан и учитывает пользу персональных данных, в том числе то, что эффективное использование персональных данных способствует созданию новых отраслей, созданию динамичного экономического общества и повышению качества жизни населения Японии.
Закон о защите персональных данных, хранящихся в административных органах (№58, 2003) [12]	Закон защищает права и интересы граждан, а также обеспечивает беспрепятственное административное управление и эффективное использование персональных данных для создания новых отраслей, создания динамичного экономического общества и повышения качества жизни населения Японии путём установления стандартов обработки персональных данных, хранимых административными органами.
Закон об использовании номеров для идентификации личности при административных процедурах (№27, 2013) [13]	Данный законодательный акт определяет специальные положения для законов «О защите персональных данных, хранящихся в административных органах» и «О защите персональных данных» для безопасной обработки персональных данных административными органами.
Закон о запрете несанкционированного доступа к компьютерным данным (№128, 1999) [14]	Закон запрещает несанкционированный доступ и предусматривает меры наказания за его нарушение, а также меры по оказанию помощи со стороны Комиссии общественной безопасности (на уровне префектур) для предотвращения повторения подобных случаев. Цель состоит в предупреждении и предотвращении компьютерных преступлений через телекоммуникационные сети, а также поддержании порядка путём контроля доступа, и таким образом способствовать развитию передового информационного и телекоммуникационного общества.
Закон об электронной подписи и аутентификации (№102, 2000) [15]	Закон нацелен на содействие распространению обработки информации с помощью электронной подписи, тем самым способствуя улучшению жизни населения и развитию национальной экономики.

Помимо вышеописанных законов, кибербезопасности посвящена отдельная **статья закона о повышении конкурентоспособности в области промышленности** [16].

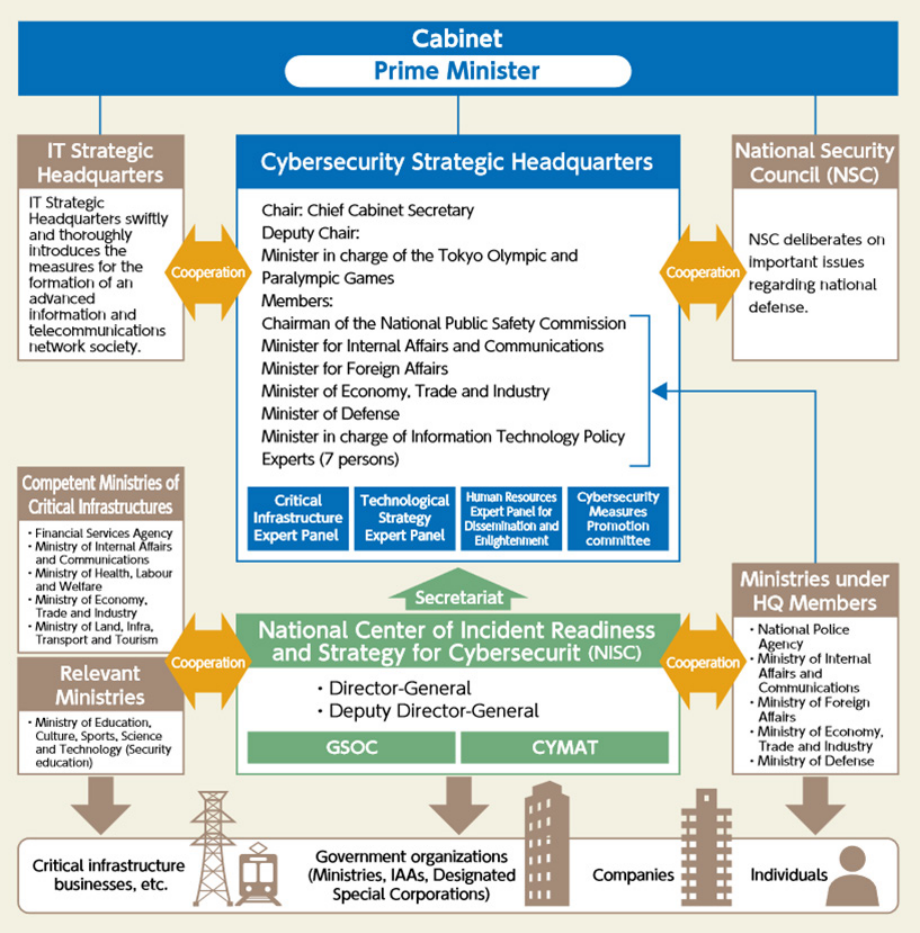
Кроме того, существуют законы об авторском праве, о недобросовестной конкуренции, о телекоммуникационной деятельности, а также закон об обработке информации (компьютерами) 1970 года, но в современных документах по его теме упоминаний не было найдено.

Структура органов, реализующих политику в области кибербезопасности

Как было сказано выше, «Основной закон о кибербезопасности» определил создание органа, ответственного за политику в области кибербезопасности — **Стратегический штаб по обеспечению кибербезопасности**.

Стратегический штаб был создан при Кабинете министров в ноябре 2014 для эффективного и всестороннего продвижения политики по кибербезопасности. Это командный орган по вопросам национальной кибербезопасности, который также наделён полномочиями давать рекомендации в сфере кибербезопасности другим государственным учреждениям. Стратегический штаб возглавляется Главным секретарем кабинета министров Ёсихидэ Сугой. Заместитель — ответственный министр по Олимпийским и Паралимпийским играм.

Рисунок 7. Структура органов, реализующих политику в области кибербезопасности



В Стратегический штаб по обеспечению кибербезопасности также входят:

- Председатель национальной комиссии общественной безопасности
- Министр внутренних дел и коммуникаций
- Министр иностранных дел
- Министр экономики, торговли и промышленности
- Министр обороны
- Министр по политике в сфере информационных технологий
- 7 независимых экспертов
- Экспертная группа по критической инфраструктуре
- Экспертная группа по технологической стратегии
- Экспертная группа по распространению и просвещению (грамотности в сфере кибербезопасности среди населения)
- Комитет по продвижению (по распространению, применению мер кибербезопасности)

Согласно статьям «Основного закона о кибербезопасности» и «Основного закона о формировании современного информационно-телекоммуникационного сетевого общества», среди функций штаба указаны:

- Подготовка Стратегии кибербезопасности и содействие её реализации
- Разработка мер по кибербезопасности для административных органов и агентств
- Оценка мер противодействия инцидентам, связанных с кибербезопасностью
- Работа в тесном взаимодействии со Стратегическим штабом по продвижению общества передовых информационно-телекоммуникационных сетей по вопросам кибербезопасности
- Работа в тесной координации с Советом национальной безопасности по вопросам кибербезопасности в контексте национальной безопасности
- Подготовка проекта плана по развитию использования данных государственного и частного секторов и содействие его внедрению

В качестве секретариата штаб-квартиры выступает **Национальный центр готовности к инцидентам и стратегии кибербезопасности** (National center of Incident readiness and Strategy for Cybersecurity — **NISC**). Центр создан в 2015 на базе бывшего Национального центра информационной безопасности, действующего с 2005. NISC играет ведущую роль в качестве координационного центра по вопросам межведомственного сотрудничества и развития партнёрских отношений между производственным сектором, академическими кругами, а также государственным и частным секторами.

NISC координирует политику кибербезопасности и формулирует:

- Стратегию кибербезопасности. Стратегия кибербезопасности демонстрирует базовую позицию в отношении политики кибербезопасности, её целей и реализации на 3 года (2018–2020) внутри страны и за рубежом
- Политику кибербезопасности для защиты КИИ
- Единый стандарт мер информационной безопасности государственных органов
- План развития человеческих ресурсов в области кибербезопасности
- Стратегию исследований и разработок в области кибербезопасности и другие

Рисунок 8. Структура NISC (японский язык)

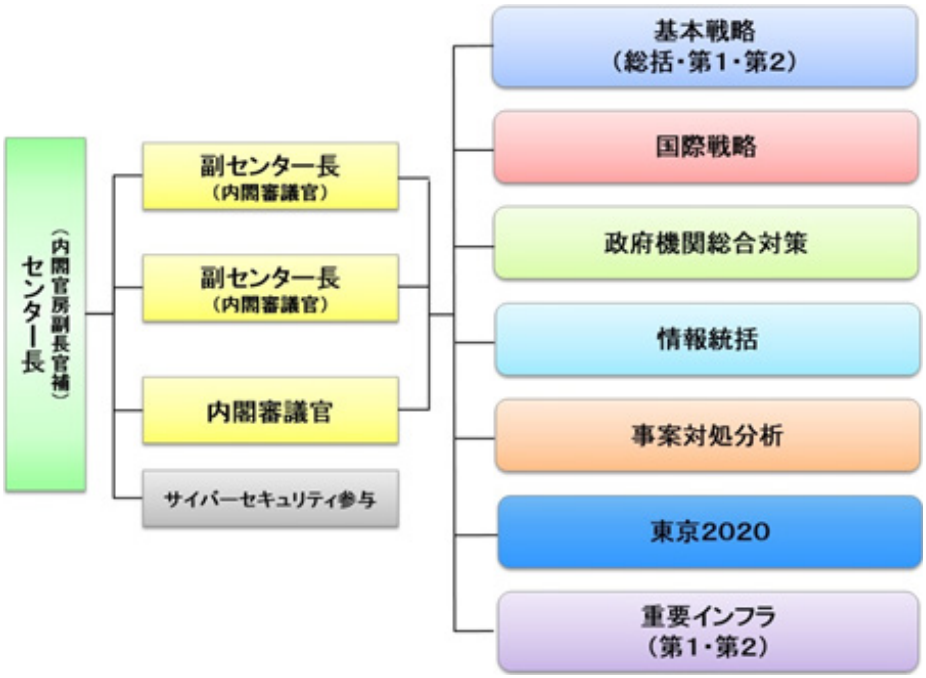
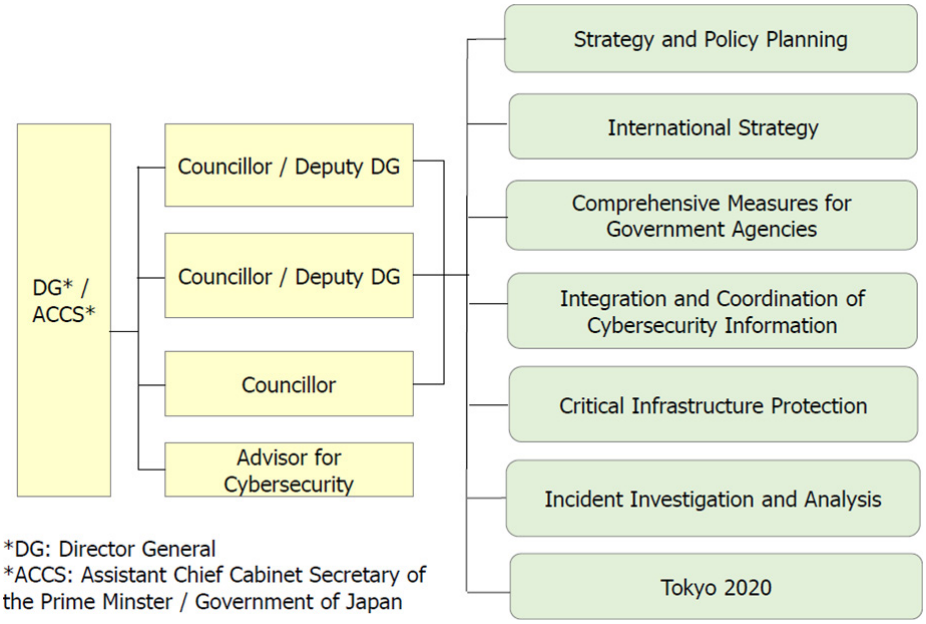


Рисунок 9. Структура NISC (английский язык)



Согласно рисунку выше, NISC состоит из семи групп (правая колонка):

1. **Группа планирования стратегии и политики**

   Зона ответственности: составление среднесрочного и долгосрочного плана политики по кибербезопасности, а также проведение исследований и анализа тенденций в области технологий кибербезопасности и т. д.

2. **Группа международной стратегии**

   Содействие международному сотрудничеству в области политики кибербезопасности.

3. **Группа разработки комплексных мер для государственных органов**

   NISC установил Общие стандарты мер информационной безопасности государственных органов, чтобы повысить уровень информационной безопасности для всех государственных учреждений и связанных с ними агентств в качестве базового стандарта. Основываясь на стандарте, NISC проверяет статус его внедрения во всех агентствах.

4. **Информационная группа по интеграции и координации в области кибербезопасности**

   NISC управляет государственной группой мониторинга в режиме реального времени — **GSOC** (Government Security Operation Coordination team). GSOC не только отслеживает злонамеренные сообщения, входящие или исходящие из государственных систем, но также работает как платформа для обмена информацией между государственными организациями.

5. **Группа по расследованию инцидентов**

   Анализ целевых писем и вредоносных программ, также расследование других случаев кибератак.

6. **Группа по Олимпиаде Токио — 2020**

   Продвижение мер по кибербезопасности Олимпийских и Паралимпийских игр в Токио в 2020.

7. **Группа по защите объектов критической информационной инфраструктуры**

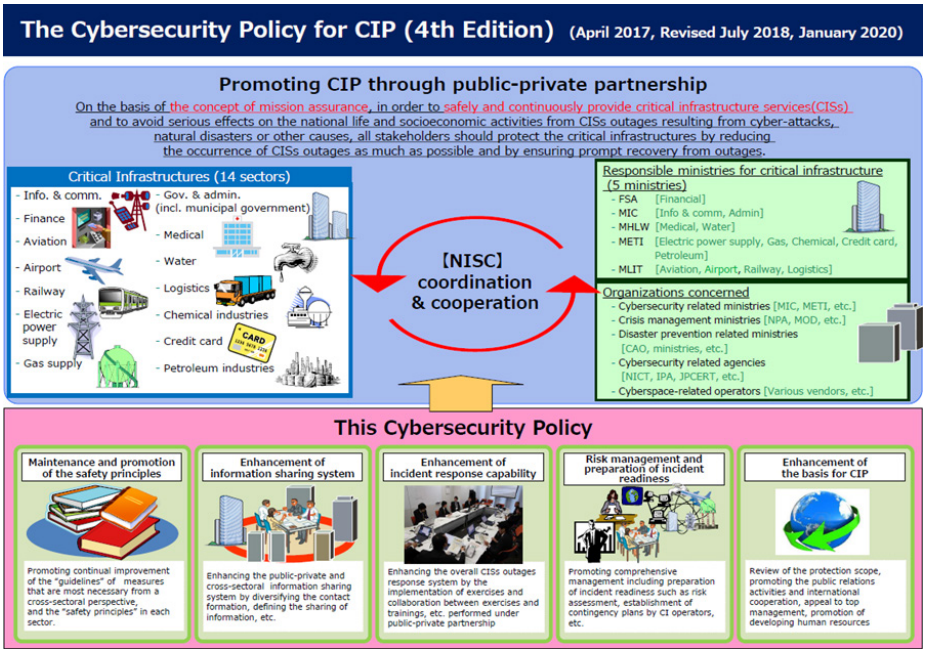
   Создание государственно-частного партнерства в области кибербезопасности на основе «Политики кибербезопасности для защиты объектов КИИ». Документ разработан в 2017 и последний раз пересмотрен в январе 2020. В документе 14 секторов определены как объекты КИИ: информационно-коммуникационные технологии, государственный и административный сектор, финансы и кредитные карты, авиация и аэропорты, железные дороги, электроснабжение, водоснабжение, логистика, медицина, транспортировка газа, нефтяная промышленность, химическая промышленность.

   Цели создания и внедрения документа:

   - Развитие и внедрение принципов безопасности

- Улучшение системы обмена информацией
- Повышение способности реагировать на инциденты
- Управление рисками и подготовка к реагированию на инциденты
- Создание основы защиты объектов критической информационной инфраструктуры

Рисунок 10. Политика кибербезопасности в отношении объектов КИИ



NISC и JPCERT / CC, в котором состоят коммерческие организации, работают вместе как **национальный CERT.** Всего в ассоциации состоит 83 организации. 6 компаний-учредителей:

1. JSOC Japan Security Operation Center (JSOC; LAC Co., Ltd.)
2. Hitachi Incident Response Team (HIRT)
3. IIJ group Security Coordination Team (IIJ-SECT)
4. Japan Computer Emergency Response Center (JPCERT / CC)
5. NTT Computer Security Incident Response and Readiness Coordination Team (NTT-CERT)
6. SoftBank teleCommunications Security Incident Response Team (SBCSIRT)

Вопросами кибербезопасности в Японии занимаются также следующие органы

- **Агентство поддержки кибербезопасности в промышленности** (Industrial Cybersecurity Promotion Agency, ICPA). Новый орган, подчинённый Министерству торговли и экономики, целью является защита объектов КИИ Японии от кибератак. Начало работу в 2017, полная функциональность должна была быть достигнута к 2020 для обеспечения кибербезопасности во время проведения Олимпийских игр.
- **Агентство содействия развитию в области ИКТ** (Information-Technology Promotion Agency, IPA). Национальный орган, ответственный за обмен информацией между правительством и бизнесом.
- В Национальном полицейском агентстве (NPA) создан **отдел по борьбе с высокотехнологичными преступлениями** (High-Tech Crime Technology Division) [17].

- **Японский центр по борьбе с киберпреступлениями** (Japan Cybercrime Control Center, JC3). Орган, который также занимается выявлением и нивелированием киберугроз. В сферу его ответственности входит сбор и анализ информации о киберугрозах, исследование и разработки мер по их устранению, разработка учебных программ [18].

- **Комиссия по защите персональных данных** (Personal Information Protection Commission, PIPC). Первый независимый орган по защите персональных данных, создан в 2014 [19]. В 2015 полномочия Комиссии были пересмотрены и теперь она отвечает за защиту персональных данных всего населения страны.

- **Партнёрство по обмену информации в области кибербезопасности** (Cyber Security Information Sharing Partnership of Japan, J-CSIP). Общественно-частное партнёрство, в рамках которого действует платформа для обмена информацией, а также сетевые инструменты реагирования на киберинциденты, которые могут повлиять на объекты КИИ [20].

- **Консультационная команда киберреагирования** (Cyber Rescue and Advice Team against targeted attack of Japan, J-CRAT). Орган также, как и J-CSIP, создан для защиты объектов КИИ от сложных целевых атак, помогает организациям принимать меры по предотвращению.

Силы самообороны Японии в 2020 создали **подразделение по кибербезопасности** (Cyber Defense Group), состоящее из 70 военнослужащих, к 2023 их количество планируется увеличить до 230 человек.

Список вышеперечисленных органов не полон, для обзора выбраны самые крупные, но это, в целом, позволяет сделать вывод о спланированной политике Японии в области кибербезопасности.

Заключение

Сферу обеспечения кибербезопасности в Японии регулирует порядка 10 министерств на базе 10 основных законодательных актов, в стране уже несколько лет как принята Стратегия кибербезопасности, которая обновляется в соответствии с новыми условиями (например, проведение Олимпийских игр). Все регуляторы взаимодействуют друг с другом, а опубликованные законы, регулирующие сферу, имеют прозрачную и лаконичную структуру — не случайно Япония вошла в число стран с самым высоким индексом регулирования нормативно-правовой сферы в данной области (категория G5).

Для обеспечения реализации политики в сфере кибербезопасности в Японии создано несколько органов (организаций, центров, отделов), занятых исключительно вопросами кибербезопасности, сделана ставка на обучение сотрудников и увеличение количества компетентных специалистов в Силах самообороны.

Уже в 2016 Японию оценивали как страну, практически полностью готовую к отражению киберугроз, но её руководство не останавливается на достигнутом и по настоящий день продолжает вести активную политику в данной сфере, соответствующую национальным приоритетам. Несмотря на то, что индекс киберготовности с 2016 не пересчитывался и не обновлялся, можно высказать обоснованное предположение, что уровень кибербезопасности страны повысился.

Источники

1 International Telecommunication Union. ICT Development Index, 2017

2 Cyber Readiness Index CIR 2.0

3 The World Bank. ICT service exports (% of service exports, BoP) — Japan, Russian Federation

4 The World Bank. ICT goods exports (% of total goods exports) — Japan, Russian Federation

5 International Telecommunication Union. Digital Trends in Asia Pacific 2021: 1, 2

6 ITU: Global ICT Regulatory Outlook 2020

7 Ministry of Defense: National Defense Program Guidelines for FY2019 and beyond (NDPG)

8 Основной закон о кибербезопасности Японии

9 Основной закон о формировании современного информационно-телекоммуникационного сетевого общества

10 Основной закон об использовании данных в государственном и частном секторе

11 Закон о защите персональных данных

12 Закон о защите персональных данных, хранящихся в административных органах

13 Закон об использовании номеров для идентификации личности при административных процедурах

14 Закон о запрете несанкционированного доступа к компьютерным данным

15 Закон об электронной подписи и аутентификации

16 Закон о повышении конкурентоспособности в области промышленности

17 National Police Agency

18 JC3: Japan Cybercryme Control Center

19 Personal Information Protection Commission

20 Information technology Promotion Agency