Стратегия правительства Канады в области корпоративной кибербезопасности

На этой странице

Послание Президента

Стратегия корпоративной кибербезопасности Правительства Канады

Безопасность канадцев является и всегда была нашим главным приоритетом. Канадцы полагаются на правительство Канады в предоставлении программ и услуг, многие из которых в современную эпоху становятся все более цифровыми. Как и многие государственные учреждения по всему миру, правительство было объектом кибератак, которые могут оказать значительное влияние на деятельность правительства и безопасность канадцев. Мы постоянно адаптируем меры безопасности и создаем инструменты, помогающие защитить наши системы и личную информацию канадцев.

Такие инструменты, как План управления мероприятиями по кибербезопасности правительства Канады, настольные учения и мониторинг безопасности правительственных веб-сайтов, являются упреждающими мерами, которые помогают США предвидеть киберсобытия и эффективно реагировать на них.

Сейчас мы предпринимаем дополнительные шаги для усиления нашего подхода и получения более четкой картины текущей киберзащиты в государственных органах. Эта первая в истории Стратегия корпоративной кибербезопасности правительства Канады, разработанная Секретариатом Совета казначейства Канады, канадским учреждением по обеспечению безопасности связи и общими службами Канады, представляет собой основанный на рисках общегосударственный подход, который улучшит сотрудничество между департаментами и повысит кибербезопасность в целом.

Эта стратегия кибербезопасности является первой в своем роде и свидетельствует о нашей приверженности обеспечению безопасности канадцев в эпоху цифровых технологий. Она сократит количество увольнений, выявит пробелы и будет включать круглогодичное тестирование и обзоры.

Это также улучшит методы подготовки правительства к кибератакам, реагирования на них и восстановления после них, одновременно способствуя формированию разнообразной рабочей силы с необходимыми навыками, знаниями и культурой для поддержки кибербезопасности. Государственная служба Канады является одной из лучших в мире, и эта стратегия поможет обеспечить нас кадрами, обладающими необходимыми инструментами для реагирования на сложные кибератаки.

Кибербезопасность - это постоянная работа, и эта стратегия будет регулярно пересматриваться и обновляться, чтобы соответствовать развивающимся угрозам.

Канадцы могут быть уверены, что правительство постоянно принимает решительные меры по защите их информации и реагированию на киберпространства, когда они все-таки происходят.

Я приглашаю вас ознакомиться со Стратегией, чтобы узнать больше о том, как правительство Канады укрепляет кибербезопасность во всех государственных структурах.

Достопочтенная Анита Ананд, председатель Правления Казначейства.

1. Введение

▶ В этом разделе

1.1 Контекст

Канадцы полагаются на государственные учреждения, такие как Правительство Канады (GC), в предоставлении программ и услуг. Государственные услуги, как важнейший сектор инфраструктуры, необходимы для здоровья, охраны и экономического благополучия канадцев. Растущий цифровой характер ГК и зависимость от информационных технологий означают, что ГК является привлекательной мишенью из-за наличия в ней личной информации, ценных исследовательских данных и другой конфиденциальной информации.

В результате события, связанные с кибербезопасностью, могут оказать значительное влияние на деятельность правительства либо в результате нарушения работы критически важных служб, либо в результате раскрытия секретной или личной информации. Этот значительный эффект может подвергнуть людей риску кражи личных данных или других видов мошенничества, что потенциально может подорвать доверие к государственным институтам и негативно повлиять на канадскую экономику и общество в целом. В *Национальной оценке киберугроз на 2023-24 гг.* подчеркивается значительный рост числа и изощренности субъектов киберугроз, которые пользуются зависимостью от технологий, подключенных к Интернету, для совершения вредоносных действий. Все более сложный ландшафт угроз в сочетании с быстрыми темпами технологических инноваций и внедрения еще больше усложнят понимание департаментами и агентствами GC рисков, с которыми они сталкиваются, и того, как они могут и должны защищать себя.

С этой целью, учитывая растущую изощренность и частоту кибератак, ГК должна сохранять бдительность и продолжать укреплять свою защиту для повышения устойчивости. Обеспечение конфиденциальности, целостности и доступности информации и сетей GC имеет важное значение для предоставления безопасных, надежных и пользующихся доверием цифровых услуг. Внедрение и поддержание устойчивой цифровой GC потребует лучшего понимания природы киберрисков наряду с действиями по модернизации и обеспечению безопасности систем для предотвращения кибератак и противодействия им. При возникновении кибернетических событий генеральный директор должен иметь возможность быстро обнаруживать эти события, чтобы минимизировать их влияние. Создание устойчивой системы кибербезопасности позволит ГК эффективно реагировать на киберпространства и своевременно восстанавливаться после них для поддержания непрерывного предоставления государственных программ и услуг.

1.2 Цель и сфера применения

Целью Стратегии кибербезопасности предприятия GC (Strategy) является:

- определите видение и стратегические цели для ГК, которые будут соответствовать меняющемуся ландшафту рисков кибербезопасности, повысят зрелость системы кибербезопасности и оптимизируют инвестиции ГК в кибербезопасность

- разработка будущего состояния кибербезопасности правительственных операций с поддерживающим управлением, надзором и четкими ролями и обязанностями
- определите инициативы и необходимые инвестиции для поддержки реализации Стратегии

Стратегия применяется к департаментам и агентствам, находящимся в ведении Совета казначейства, в частности, в соответствии с *Политикой в области обслуживания и цифровых технологий* и *Политикой государственной безопасности*. Кроме того, сфера применения Стратегии ориентирована на определенные информационные системы (Защищенные B) включительно, наряду с засекреченными (секретными) информационными системами, которые ориентированы на поддержку правительственных операций, уважая при этом уникальные потребности более широкой экосистемы засекреченных систем.

Хотя федеральные департаменты и агентства, не находящиеся в ведении Совета казначейства, в настоящее время не уполномочены применять и принимать требования и указания Совета Казначейства, им рекомендуется в максимально возможной степени следовать целям, изложенным в Стратегии, для улучшения состояния кибербезопасности во всех государственных учреждениях.

1.3 Текущая среда

Пилоты

> **Заявление Канады о цифровых амбициях**
>
> Обеспечить выполнение государственных функций в цифровую эпоху для всех канадцев. Это будет сделано путем предоставления модернизированных и доступных инструментов для поддержки предоставления услуг, которые отражают лучшее, что есть в Канаде в цифровом пространстве.

Как указано в *Цифровых амбициях Канады до 2022 года*, сегодняшний цифровой ландшафт отмечен беспрецедентными темпами и масштабами изменений. Быстрая технологическая, цифровая трансформация и преобразование данных в настоящее время являются частью повседневной жизни канадцев, революционизируя способы доступа к информации и услугам, а также то, как они живут, общаются и работают. Канадцы ожидают, что они будут доверять своему правительству и смогут получить доступ к любой государственной службе безопасным и доступным способом в любое время и с любого устройства. Однако выполнение этих ожиданий сопряжено с целым рядом проблем и соображений безопасности, которые необходимо учитывать в рамках постоянно меняющегося киберпространства, включая:

- **Предоставление цифровых услуг**
  - Канада сталкивается с постоянными и все более изощренными вредоносными кибератаками, которые угрожают государственному сектору и’ в конечном счете, безопасности и конфиденциальности канадцев.
  - По мере расширения внедрения цифровых технологий растут и возможности для взломов и потери данных. Рост объема оцифрованной личной информации и улучшение ее предоставления с помощью цифровых подходов должны сопровождаться мерами по обеспечению защиты частной жизни канадцев и возможности предоставления государственных услуг в условиях быстро меняющейся среды угроз.
  - Согласно Руководству по цифровым стандартам правительства Канады, сервисы должны создаваться с учетом потребностей пользователей. Это включает применение сбалансированного подхода к управлению рисками путем внедрения соответствующих мер конфиденциальности и безопасности, которые не вызывают затруднений и не являются бременем для пользователей.
- **Обязательства по охране окружающей среды, социальной сфере и управлению (ESG)**
  - Поскольку ГК все больше уделяет внимания ответственному и устойчивому предоставлению цифровых услуг, защита своих активов и личной информации канадцев является неотъемлемой частью

выполнения ГК социальной ответственности.

- Экологические проблемы подчеркивают необходимость минимизации углеродного следа, связанного с кибератаками и утечкой данных, поскольку эти инциденты часто приводят к значительному потреблению энергии.
- Эффективные методы обеспечения кибербезопасности демонстрируют приверженность управлению, поддерживая прозрачность, подотчетность и этичное поведение, а также укрепляя надежность GC среди канадцев.

- **Будущее работы**
  - Пандемия COVID-19 подчеркнула необходимость в более современных рабочих инструментах и практиках для поддержки гибридной рабочей среды. Через несколько дней после объявления пандемии в марте 2020 года большинство федеральных государственных служащих начали работать удаленно.
  - Поскольку были приняты меры для обеспечения возможности удаленной работы во время пандемии, потребовалось повысить толерантность к риску для обеспечения непрерывности работы правительства. Заглядывая в будущее, необходимо будет пересмотреть эту толерантность к рискам и связанные с ней меры по их снижению с учетом новой рабочей среды.
- **Модернизация технологий**
  - Технологии развиваются беспрецедентными темпами, регулярно внедряются новые инновации и усовершенствования (например, искусственный интеллект (ИИ), квантовые вычисления, блокчейн). Хотя такое быстрое развитие приносит много преимуществ и возможностей, оно также создает дополнительные векторы угроз и новые вызовы для кибербезопасности. Скорость технологических изменений означает, что меры безопасности, которые когда-то были эффективными, могут быстро устареть, что подчеркивает необходимость упреждающего и адаптивного подхода к кибербезопасности, при котором организации постоянно оценивают и совершенствуют свои меры безопасности, чтобы идти в ногу с постоянно меняющимся ландшафтом угроз. Скорость изменений вызывает трудности в надлежащем надзоре, создавая пробелы в подотчетности и ответственности за риски кибербезопасности.
  - Внедрение и интеграция устройств Интернета вещей (IoT) привело к конвергенции кибернетических и физических систем, что расширяет поле атаки там, где физическое воздействие может быть результатом вектора киберугроз или где кибернетическое воздействие может быть результатом вектора физической угрозы.
  - Способ предоставления и потребления услуг в области информационных технологий (ИТ) значительно изменился за последние годы и продолжает развиваться. Широкое использование мобильных устройств и внедрение облачных сервисов меняют технологическую среду GC и должны рассматриваться с точки зрения кибербезопасности.
  - Хотя традиционная модель безопасности, ориентированная на периметр, хорошо послужила GC, представление о том, что цифровые активы и пользователи в пределах определенной границы заслуживают доверия, не соответствует “новому цифровому миру”, где надежный периметр не может быть определен. Расширение возможностей подключения, риск внутренних угроз и необходимость защищать и хранить данные в различных собственных и сторонних хранилищах (например, в облаке) привели к появлению новых концепций безопасности, которые не основаны исключительно на подходе к обеспечению безопасности, ориентированном на периметр (то есть на нулевое доверие).
- **События в области кибербезопасности и инциденты, связанные с кибербезопасностью, продолжают влиять на правительство**

- С каждым годом увеличивается количество уязвимостей нулевого дня, которые требуют немедленных действий со стороны GC.
- Компромиссы в цепочке поставок (например, SolarWinds) оказывают влияние на GC и создают операционные риски при использовании сервисов сторонних производителей. Необходимо, чтобы учреждения критически важной инфраструктуры (то есть природные ресурсы, финансы, здравоохранение, телекоммуникации) были в центре внимания при обсуждении вопросов кибербезопасности и устойчивости во время анализа уязвимостей. ГК необходимо обеспечить, чтобы все мероприятия по кибербезопасности проводились совместно с этими важнейшими инфраструктурными учреждениями для обеспечения согласованного и коллективного подхода к кибербезопасности и устойчивости.
- Сложные киберинциденты [1], затрагивающие департаменты и агентства, демонстрируют, что GC продолжает оставаться мишенью, что обуславливает необходимость оперативного устранения любых недостатков архитектуры в информационных системах GC.
- Кибератаки и утечки данных также предоставляют мошенникам возможности использовать уязвимости и осуществлять мошеннические действия с использованием таких методов, как социальная инженерия, фишинг или перечисление украденных учетных данных, для получения несанкционированного доступа к системам, что потенциально может привести к краже личных данных или финансовому мошенничеству.

Прогресс на сегодняшний день

Таким образом, создание и поддержание государственной киберзащиты жизненно важно для защиты функций и услуг, от которых зависит канадское общество. За последнее десятилетие был достигнут прогресс в улучшении государственной системы кибербезопасности, благодаря тому, что в GC в некоторой степени были реализованы централизованные возможности обеспечения безопасности. Примеры включают:

- создание канадского подразделения общих служб (SSC) в рамках усилий по стандартизации инфраструктуры информационных технологий (ИТ) GC, включая интеграцию служб киберзащиты по периметру предприятия GC
- создание Канадского центра кибербезопасности (Cyber Centre) в составе Управления безопасности связи (CSE) для консолидации опыта работы в области кибербезопасности со всего федерального правительства и предоставления единого унифицированного источника экспертных рекомендаций, руководств, услуг и поддержки по оперативным вопросам кибербезопасности
- создание четких механизмов управления для поддержки разработки стратегической политики киберзащиты, эффективного управления инициативами в области информационной безопасности, затрагивающими деятельность всего правительства, и реагирования правительства на киберинциденты
- повышение доступности рекомендаций и других инструментов, а также внедрение минимальных требований к конфигурации в 2022 году в рамках *Политики в области обслуживания и цифровых технологий*, которая была первоначально опубликована в 2020 году, наряду с обновлением *Политики в области государственной безопасности* в 2019 году

Остаются пробелы

Несмотря на этот прогресс, сохраняются пробелы между текущим состоянием киберустойчивости правительства и тем, какой она должна быть. Эти пробелы включают:

- **Различные уровни кибернетической зрелости**
  - Инструмент самооценки кибернетической зрелости TBS (CMSA) был запущен осенью 2021 года для поддержки департаментов и агентств в оценке их зрелости в области кибербезопасности на основе

признанных передовых практик и основан на методологии, разработанной Национальным институтом стандартов и технологий (NIST) США в области кибербезопасности.

- Сравнение результатов 2021-22 годов по сравнению с результатами 2022-23 годов показывает, что департаменты и агентства добиваются незначительного прогресса в повышении своей кибернетической зрелости и что они остаются в среднем ниже целевого показателя наличия повторяющихся процессов для выявления угроз и реагирования на них в поддержку эффективной защиты от новых и зарождающихся угроз.

- **Отсутствие всесторонней осведомленности о рисках кибербезопасности**
  - Уровень возможностей, инвестиций и понимания безопасности в федеральных департаментах и агентствах остается непоследовательным. Размер и сложность цифрового имущества GC, включая наличие устаревших приложений и технологий, также значительно усложняют задачу.
  - Признавая потенциальную серьезность последствий для GC из-за недостатков в цепочке поставок, более широкое использование услуг сторонних производителей обусловило необходимость в более эффективных подходах и решениях для управления рисками сторонних производителей.
  - Способность защиты от возникающих уязвимостей и угроз дополнительно ограничивается наличием устаревших информационных систем GC. Это ограничение обусловливает необходимость продолжения усилий по управлению, модернизации или удалению таких систем, а также по внедрению необходимых мер предосторожности и постоянным инвестициям для обеспечения достаточной безопасности информационных систем GC на протяжении всего их жизненного цикла. Однако отслеживание и обслуживание технологических активов и данных (как локальных, так и в облаке) не являются всесторонне понятными или управляемыми, что ограничивает видимость и осведомленность о том, какие активы нуждаются в защите. Многие департаменты и агентства полагаются на ручные процессы, которые могут отнимать много времени, быть подверженными ошибкам и неэффективными. Ограничения в отношении ручных процессов особенно важны для многих активов, где требуется надлежащее отслеживание деталей конфигурации (например, точных криптографических алгоритмов и их параметров).

- **Разрозненные подходы и отсутствие скоординированных инвестиций в различные средства обеспечения безопасности могут привести к несоответствиям, неэффективности и "слепым пятнам" в общей системе обеспечения безопасности GC**
  - Управление идентификацией, учетными данными и доступом (ICAM)
    - Управление цифровыми учетными данными таким образом, чтобы снизить риски для персонала, организационной и национальной безопасности, одновременно защищая целостность программы и обеспечивая надежное предоставление услуг, ориентированных на граждан, имеет первостепенное значение для GC. С этой целью требуется модернизировать текущие решения GC ICAM, чтобы гарантировать согласованное и совместное управление идентификацией в рамках GC как для внутренних, так и для внешних служб, а также повысить уровень надежности, необходимый для смягчения угроз аутентификации.
  - Мониторинг безопасности
    - Департаменты и агентства используют комбинацию различных инструментов, методов и сервисов для мониторинга своих систем, что может затруднить получение всестороннего представления о потенциальных угрозах безопасности и может привести к непреднамеренному дублированию или пробелам в мониторинге. Эта сложность обусловливает необходимость повышения прозрачности и доступа к данным для поддержки комплексного мониторинга, при котором департаменты и агентства могут анализировать данные со своих уникальных операционных позиций. Следует

учитывать, что многие отделы не обучены, не оснащены и не укомплектованы персоналом для поддержки этой функции.

- В то время как объем локальных служб ясен, поскольку он связан с мандатом (например, SSC поручено предоставлять услуги электронной почты, сети и центров обработки данных, а департаменты и агентства отвечают за конечные точки и приложения), быстрое внедрение облачных вычислений привело к отсутствию ясности в отношении ролей и обязанностей и степени распространения существующих ролей и обязанностей на облако. Из-за отсутствия ясности ожидалось, что департаменты и агентства будут управлять своими облачными средами, включая операции по обеспечению кибербезопасности. Это ожидание привело к дублированию усилий, непоследовательным подходам, отсутствию обмена разведданными и снижению прозрачности для GC enterprise в отношении анализа событий кибербезопасности и смягчения их последствий.

- Общие службы
  - Несмотря на то, что было получено финансирование для создания возможностей корпоративной кибербезопасности, не все эти возможности были полностью реализованы в рамках GC по разным причинам, включая каскадные подходы к реализации проектов и длительные процессы закупок.
  - В *Специальном отчете Комитета парламентариев по национальной безопасности и разведке о структуре и деятельности правительства Канады по защите своих систем и сетей от кибератак* подчеркивается всеобъемлющая проблема, когда правительством все чаще управляют горизонтально, в то время как его основополагающие полномочия остаются вертикальными, что создает значительные расхождения. В частности, политика Правления Казначейства, предназначенная для защиты государственных систем, применяется неравномерно, учитывая, что:
    - отдельные департаменты и агентства сохраняют значительную свободу действий в отношении того, использовать ли эту структуру или использовать конкретные защитные технологии
    - большое количество организаций, в частности Crown corporation и, возможно, некоторые другие государственные структуры, не обязаны придерживаться политики Совета казначейства или использовать систему киберзащиты
  - Хотя использование централизованных служб в государственных структурах помогло бы снизить корпоративные риски, существует необходимость в расширении обмена информацией для поддержки такого использования, включая усиление координации при разработке стратегических мероприятий, внедрении и эксплуатации. Эта потребность также усугубляется отсутствием стандартизированного отслеживания и управления услугами общих служб.

- **Традиционные модели архитектуры безопасности менее эффективны, поскольку пользователи и приложения теперь существуют за пределами традиционного сетевого периметра**
  - Растущая угроза сложных кибератак подчеркнула, что GC не может полагаться исключительно на обычные средства защиты по периметру для защиты критически важных систем и данных. Информационно-ориентированный подход, при котором отсутствует скрытое доверие и весь доступ проверяется (также называемый нулевым доверием) в сочетании с защитой сети на базе хоста и облака, позволит департаментам и агентствам быстро обнаруживать, изолировать угрозы такого типа и реагировать на них.

- **Несоответствие между традиционными подходами к оценке безопасности и гибкими методологиями предоставления услуг**
  - По мере того, как GC переходит к работе в более гибкой среде с использованием методов управления проектами и разработки, процессы оценки безопасности и авторизации (SA & A) в GC продолжают работать по каскадному принципу, основанному на соблюдении требований, что приводит к длительным задержкам в введении в действие решений для информационных систем. GC должен

перейти к подходу, основанному на оценке рисков и ориентированному на угрозы, который уменьшит трудности с гибкими методологиями предоставления услуг, сохраняя при этом баланс безопасности.

- **Слабые методы управления информацией**
  - Существующие процессы защиты данных выполняются вручную и не были всесторонне стандартизированы от создания до уничтожения. Кроме того, существует недостаточная осведомленность о надлежащих процедурах, связанных с обработкой и классификацией информации (например, недоклассификация или переклассификация), что приводит к непоследовательному применению в рамках GC.
  - Из-за устаревших ИТ-инструментов защита информации неадекватна, что может привести к увеличению инцидентов кибербезопасности или нарушений конфиденциальности, тем самым подрывая уверенность в безопасности управления информацией GC.
- **Незрелые методы управления событиями кибербезопасности**

> **Упражнения по киберсимуляции**
>
> Выполнение упражнений по киберсимуляции (также называемых настольными упражнениями) помогает повысить готовность, улучшить коммуникацию и принятие решений, а также обеспечить экономически эффективное обучение, которое повышает уверенность в реагировании на события, связанные с кибербезопасностью. В 2021-22 годах только 25% подразделений проводили учения по киберсимуляции.

  - Хотя GC улучшила централизованное управление мероприятиями по кибербезопасности благодаря созданию *Плана управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP), возможности каждого отдела ограничены, и не всегда ясно, какие услуги, предоставляемые на уровне предприятия, доступны. Более того, текущие решения, как правило, являются автономными и не имеют интеграции, автоматизации рабочего процесса и возможности генерировать уведомления о неисправностях для поддержки управления инцидентами кибербезопасности.
  - Департаменты и агентства сталкиваются с целым рядом значительных или кризисных событий различной сложности и масштаба. Они отвечают за идентификацию, планирование и восстановление, а также за восстановление своих критически важных служб, внутренних операций, информационных систем и вспомогательных приложений. Все эти обязанности становится все труднее выполнять из-за устаревания информационных систем и все более распределенного характера технологических активов. Необходимы достаточные ресурсы для обеспечения непрерывности критически важных служб и поддержки усилий по восстановлению после инцидентов.
- **Проблемы, связанные с людьми и культурой безопасности**
  - Глобальный спрос на специалистов в области кибербезопасности намного превышает предложение, что приводит к нехватке квалифицированных специалистов в этой области. Генеральный директор не застрахован от этого, поскольку вакантные должности в области кибербезопасности по-прежнему являются проблемой для департаментов и агентств в поиске персонала. Также необходимо установить модель подбора персонала для специалистов в области кибербезопасности правильного размера между департаментами и центральными агентствами, чтобы должности заполнялись на приоритетной основе. GC также имеет дополнительные уровни сложности из-за требований к допуску, профилей владения вторым языком и гибридной рабочей среды для многих ИТ-должностей.
  - Также существует общая нехватка обучения по кибербезопасности, доступного для персонала GC, как с точки зрения киберпространства (например, облачная безопасность, реагирование на инциденты, мониторинг безопасности, использование существующих инструментов кибербезопасности), так и с точки зрения персонала в целом. Чтобы свести к минимуму киберпространства, происходящие из-за

человеческой ошибки, крайне необходимо повысить квалификацию всего персонала, чтобы обеспечить лидерство и знания в области кибербезопасности во всей GC в целом.

- Инсайдеры, имеющие авторизованный доступ к конфиденциальным данным, могут представлять значительный риск для ГК в результате преднамеренного или непреднамеренного раскрытия или неправильного использования. Без модернизированных процессов проверки безопасности и непрерывного обеспечения безопасности сотрудников и подрядчиков, надежного доступа к ИТ-ресурсам и информации на основе идентификационных данных и надежных методов борьбы с мошенничеством возрастает риск инсайдерской угрозы.

Решение этой постоянно меняющейся проблемы рисков кибербезопасности потребует от ГК задействовать свои коллективные силы для создания безопасных и устойчивых информационных систем. Эта сила будет поддерживаться политикой, ориентированной на конкретные действия, повышенной гибкостью и стратегическим планированием инвестиций, направленным на устранение пробелов, чтобы гарантировать, что канадцы по-прежнему уверены в том, что их данные защищены и что предоставление критически важных услуг будет бесперебойным.

2. Общегосударственный подход к обеспечению кибербезопасности правительственных операций

▶ В этом разделе

2.1 Видение

Обеспечение общегосударственного подхода к обеспечению кибербезопасности правительственных операций, который будет способствовать предоставлению государственных услуг в цифровую эпоху для всех канадцев, требует от ГК предоставления модернизированных и доступных инструментов, поддерживающих предоставление услуг. Кибербезопасность является основополагающим компонентом, обеспечивающим простое, безопасное и эффективное предоставление государственных услуг и льгот. Следовательно, ГК должен уделять приоритетное внимание усилиям по реализации своего общего видения:

> **Создание устойчивой GC мирового класса для снижения рисков кибербезопасности, чтобы федеральные департаменты и агентства могли обеспечить безопасное предоставление цифровых услуг.**

Для реализации этого видения Генеральный директор должен уделять приоритетное внимание усилиям по снижению рисков кибербезопасности, чтобы отделы и агентства ГК могли максимально использовать преимущества цифровых технологий. Это также означает согласованные усилия по оптимизации использования ресурсов, используя общие решения, где это возможно, для повышения согласованности и снижения вероятности неправильной настройки. Для этого GC потребуются правильная политика, люди, процессы и технологии для выявления известных и неизвестных или возникающих рисков и управления ими при поддержании пропорционального и эффективного уровня кибербезопасности во всех федеральных департаментах и агентствах.

Этот подход также позволит Генеральному директору перейти от позиции реагирования к проактивному подходу при выявлении и устранении уязвимостей в системе безопасности и пробелов в возможностях, не отставая при этом от быстро меняющегося ландшафта угроз. Кроме того, ГК должен сосредоточиться на защите конфиденциальных государственных данных и обеспечении защиты своих информационных систем независимо от их среды. Обеспечение конфиденциальности и безопасности с самого начала и использование

информационно-ориентированного подхода позволят предоставлять надежные услуги и поддерживать информационные системы, которые предоставляют доступ к защищенным активам доверенным и проверенным пользователям, устройствам и службам на основе "необходимости знать".

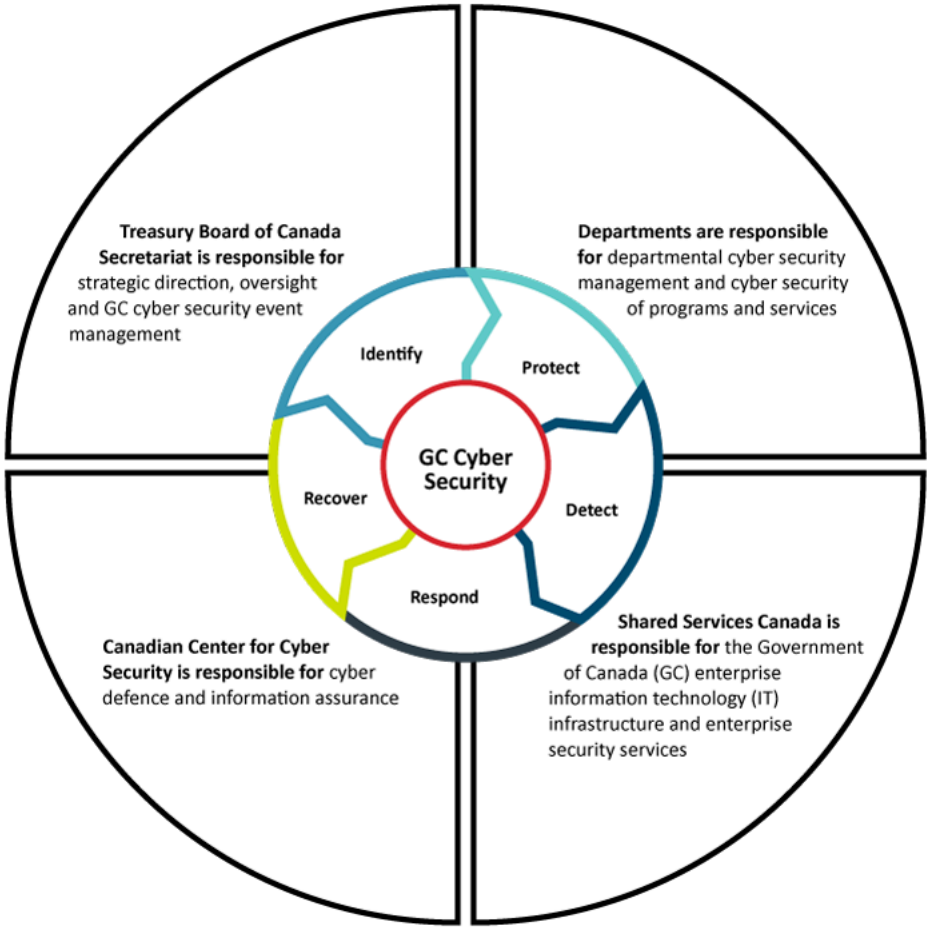
2.2 Ключевые заинтересованные стороны

Управление и координация кибербезопасности в рамках федерального правительства имеют решающее значение для обеспечения того, чтобы GC могла опережать киберугрозы и обеспечивать центральное руководство и поддержку, необходимые Канаде. Усиление управления и надзора будет необходимо для обеспечения сотрудничества и согласованности действий с департаментами и агентствами, которые играют ключевую роль в управлении кибербезопасностью. Каждая часть правительства играет свою роль в реализации концепции.

Чтобы добиться успеха, ключевые заинтересованные стороны должны тесно сотрудничать. К ключевым заинтересованным сторонам относятся:

- **Секретариат Совета казначейства Канады:** Политика и надзор, стратегическое руководство, управление мероприятиями GC по кибербезопасности
- **Учреждение по обеспечению безопасности связи и Канадский центр кибербезопасности:** киберзащита и обеспечение информации
- **Общие службы Канады:** корпоративная ИТ-инфраструктура GC и службы корпоративной безопасности
- **Департаменты и агентства:** Ведомственное управление кибербезопасностью, включая кибербезопасность ведомственных программ и служб

Рисунок 1: ключевые заинтересованные стороны



▶ Рисунок 1 - Текстовая версия

В централизованном порядке Трехсторонняя группа по информационной безопасности (Threatripadvisor), состоящая из Секретариата Совета казначейства Канады (TBS), Общих служб Канады (SSC) и Канадского центра кибербезопасности (Cyber Centre), играет важную роль в предоставлении консультаций, указаний, надзоре и указаний для реализации инициатив в области безопасности в масштабах GC, а также поддерживает департаменты и агентства, находящиеся в ведении Совета казначейства. Трехсторонняя организация продолжит свои усилия по координации оперативной деятельности в области кибербезопасности, изменяя способы обмена данными о кибербезопасности и информацией об угрозах, их использования и принятия мер в рамках государственных органов.

Департаменты и агентства несут ответственность за управление рисками кибербезопасности в своих программных областях; однако, поскольку правительство в целом применяет корпоративный подход к кибербезопасности, а программы и услуги становятся более интегрированными, крайне важно, чтобы рисками кибербезопасности эффективно и комплексно управлялись на уровне предприятия в соответствии с обязанностями, изложенными в инструментах политики Совета казначейства.

Основываясь на ожиданиях и полномочиях, изложенных в *Политике государственной безопасности* и *Политике в области услуг и цифровых технологий*, роли и обязанности будут уточнены в рамках операционной модели target security и ее технологических вариаций. Прочные отношения сотрудничества между главными информационными директорами департамента (ИТ-директорами), главными сотрудниками службы безопасности департамента (ОГО) и назначенным должностным лицом по кибербезопасности (DOCS) будут необходимы для:

- реализация приоритетов и мероприятий GC в области кибербезопасности в рамках более широких ведомственных планов безопасности
- коллективно обеспечить управление рисками кибербезопасности в департаменте для поддержки управления общей ситуацией с рисками кибербезопасности

2.3 Стратегические цели

Для реализации концепции были установлены четыре стратегические цели наряду с сопутствующими ключевыми действиями. Целями являются:

- Четко сформулируйте риски кибербезопасности и их влияние на бизнес для эффективного, ориентированного на конкретные действия и подотчетного принятия решений
- Более эффективно предотвращайте кибератаки и сопротивляйтесь им, что ведет к большей защите информации и активов правительства Канады (GC).
- Укрепление возможностей и устойчивости во всем GC для активной подготовки к событиям кибербезопасности, реагирования на них и восстановления после них
- Формирование разнородной рабочей силы GC, обладающей необходимыми навыками, знаниями и культурой в области кибербезопасности

Эти стратегические цели более подробно описаны в разделе ниже. Кроме того, Приложение A: включает первоначальный набор ключевых показателей эффективности для оценки прогресса в выполнении определенных действий.

2.3.1 Цель 1: четко сформулировать риски кибербезопасности и их влияние на бизнес для эффективного, ориентированного на конкретные действия и подотчетного принятия решений.

Поскольку ландшафт киберугроз сложен, развивается и чрезвычайно изощрен, ГК необходимо углубить свое понимание ландшафта киберугроз, чтобы разработать более комплексные и многоуровневые средства защиты. Для управления рисками кибербезопасности федеральные департаменты и агентства будут иметь процессы управления рисками, руководство и подотчетность, обеспечивающие упреждающее и эффективное выявление, оценку и управление их рисками кибербезопасности. Многолетние ведомственные стратегии

кибербезопасности будут ежегодно представляться в Офис главного информационного директора (OCIO) TBS для утверждения. Благодаря такому подходу, основанному на оценке рисков, будет обеспечена достаточная общая видимость и доступ к данным для управления аналитикой, что позволит ГК эффективно управлять рисками кибербезопасности и измерять их в целом, а также согласовывать стратегии снижения рисков с целями всей ГК. Кроме того, Генеральный директор будет располагать механизмами, обеспечивающими быстрое выявление, оценку и управление уязвимостями по всему предприятию.

Ключевые действия и цели включают:

- **Планируйте и регулируйте устойчивое и интегрированное управление кибербезопасностью**
  - Определите общий подход, методологию, решения и инструменты для оценки состояния кибербезопасности GC, которые согласуются с политикой GC и контекстом управления ИТ и в которых применяется риск-ориентированный подход в соответствии с Канадским центром кибербезопасности (Cyber Centre) *Управление рисками ИТ-безопасности: подход на основе жизненного цикла* (ITSG-33).
  - Проводите независимые оценки, текущее (круглогодичное) тестирование и всесторонние обзоры состояния кибербезопасности подразделений, чтобы помочь выявить риски кибербезопасности и расставить приоритеты.
  - Усилить управление, связанное с цифровыми и технологическими гарантиями, в рамках общеорганизационного цикла планирования инвестиций в ИТ, чтобы обеспечить соответствие предложений о расходах на кибербезопасность приоритетам правительства и Стратегии.
  - Создать интегрированную платформу управления рисками, которая использует аналитические данные на основе данных для выявления, оценки и информирования о рисках кибербезопасности таким образом, чтобы:
    - находит отклик у высшего руководства
    - предоставляет практические рекомендации для улучшения устранения рисков, определения приоритетов инвестиций и направления ресурсов
    - обеспечивает гибкие подходы к обеспечению безопасности
  - Обеспечьте доступность ресурсов и поддержки для департаментов и агентств для улучшения их состояния кибербезопасности в соответствии со Стратегией и целевой операционной моделью безопасности (TSOM).
- **Улучшите понимание уязвимости в масштабах всей GC и улучшите управление уязвимостями**
  - Внедряйте инструменты для постоянного выявления, мониторинга и управления поверхностью атаки GC, используя существующие инструменты, где это возможно.
  - Разработайте точные инвентаризации активов и составьте карту взаимосвязей и зависимостей между активами, что также облегчит усилия по исправлению ошибок.
  - Проактивно устраняйте уязвимости инфраструктуры, систем и приложений, а также риски кибербезопасности, которые они представляют, с помощью программы управления уязвимостями GC Enterprise, чтобы гарантировать эффективное управление выявленными уязвимостями во всем цифровом пространстве GC, включая наращивание резервирования и расширение возможностей на основе оценок уязвимости наших сотрудников, процессов и технологий.
- **Улучшение управления рисками кибербезопасности сторонних производителей**
  - Принять меры по повышению прозрачности системы и управлению запасами в цепочках поставок программного обеспечения и оборудования для защиты информации и активов GC в рамках надежного подхода сторонних производителей к управлению рисками кибербезопасности.
  - Стандартизировать и усилить требования, положения и условия кибербезопасности с учетом рисков в контрактных соглашениях с внешними поставщиками и выполнять рутинную проверку соблюдения поставщиками договорных положений о безопасности.

Ожидаемый результат:

- **Кибербезопасность считается общегосударственной задачей, при которой риски в информационных системах GC постоянно отслеживаются, доводятся до сведения и устраняются эффективным и своевременным образом**

2.3.2 Цель 2: более эффективное предотвращение кибератак и противодействие им, что ведет к большей защите информации и активов GC

GC полагается на ряд технологий для выполнения своих функций и предоставления цифровых услуг, что принципиально требует комплексного подхода к обеспечению безопасности для обеспечения того, чтобы функции и сервисы последовательно и непрерывно соответствовали лучшим практикам и надежным стандартам. Более того, федеральные департаменты и агентства будут шире использовать общие возможности, инструменты и сервисы для решения общих проблем кибербезопасности, улучшая кибербезопасность во всем правительстве, а также повышая эффективность и соотношение цены и качества.

Ключевые действия и цели включают:

- **Ускорение внедрения современных архитектур кибербезопасности и приложений**
  - Модернизируйте общеорганизационные системы идентификации, учетных данных и управления доступом, включая повсеместное использование многофакторной аутентификации, для создания гибридной рабочей силы.
  - Модернизируйте приложения и методы доставки с использованием общих эталонных архитектур для безопасного предоставления цифровых услуг.
  - Внедрите комплексный подход с архитектурой безопасности и инженерными ресурсами, интегрированными в проекты, для обеспечения учета аспектов безопасности и потенциальных угроз системе.
  - Усовершенствуйте и стандартизируйте методы оценки безопасности и авторизации (SA & A) путем распространения результатов SA & A по всему предприятию, чтобы уменьшить дублирование усилий при оценке общих компонентов.
  - Продолжать расширять услуги киберзащиты для всех федеральных департаментов и агентств в максимально возможной степени.
  - Перевод систем GC на использование стандартизированной постквантовой криптографии для защиты от квантовой угрозы.
  - Улучшите способность GC предотвращать, обнаруживать, реагировать на мошеннические действия в отношении приложений GC и восстанавливать их после них.
- **Внедряйте безопасные, современные и доступные инструменты и устройства на рабочем месте**
  - По возможности предоставляйте общие и безопасные базовые решения для конечных точек, учитывающие конкретные потребности сотрудников GC, такие как мобильность, совместная работа и доступность. Сюда входят:
    - создание постоянно действующих средств защиты, соответствующих политике, директивам, стандартам и руководящим указаниям GC и легко проверяемых для повышения доверия между государственными органами
    - разработка простых в использовании профилей защиты и вспомогательных учебных пособий, в которых излагаются требования безопасности и набор необходимых мер предосторожности, которые позволят обеспечить надлежащую защиту активов в соответствии с категоризацией информации по безопасности и средой угроз
- **Усилить меры по защите данных**
  - Улучшите методы обеспечения информационной безопасности с помощью обновленной модели категоризации безопасности.
  - Установите автоматизированное применение политики безопасности данных для предотвращения несанкционированного доступа и потери данных.

- Улучшите управление инсайдерскими рисками и осведомленность о них для поддержки практики непрерывного обеспечения безопасности и последующего ухода.

Ожидаемые результаты:

- **Стандартизированные и современные инструменты, устройства и общеорганизационные службы кибербезопасности развертываются и используются по всему GC**
- **Для обеспечения постоянной безопасности цифровых сервисов и защиты цифровых активов на протяжении всего их жизненного цикла применяется комплексный подход**

2.3.3 Цель 3: укрепление возможностей и устойчивости во всей GC для активной подготовки к событиям кибербезопасности, реагирования на них и восстановления после них

Даже при наличии надежных мер защиты и обнаружения инциденты кибербезопасности повлияют на GC. Поэтому важно, чтобы генеральный директор мог быстро реагировать на инциденты кибербезопасности, когда они все же происходят, для минимизации последствий и обеспечения непрерывности основных функций и услуг. Тестирование и реализация планов реагирования на инциденты как в организации, так и в государственных органах, а также создание возможностей для выявления уроков, извлеченных из инцидентов, и распространения информации об этом, является ключевой частью подхода. Комплексный подход к мониторингу с пропорциональными возможностями мониторинга безопасности, основанными на размере организации, бизнес-контексте и зрелости, поможет облегчить упреждающее обнаружение киберугроз. Кроме того, централизованный надзор и поддержка восстановления после наиболее серьезных инцидентов кибербезопасности обеспечат выявление и смягчение системных рисков.

Ключевые действия и цели включают:

- **Улучшите возможности мониторинга и обнаружения безопасности, чтобы обеспечить эффективные и адаптируемые варианты для департаментов и агентств**
  - Повысить четкость ролей и обязанностей, относящихся к мониторингу охвата, среди организаций, отделов и агентств, обслуживающих GC внутри предприятия.
  - Создайте архитектуру объединенного центра управления безопасностью (SOC), обеспечивающую охват, соизмеримый с оперативными потребностями департаментов и агентств, для повышения эффективности, сведения к минимуму дублирования усилий и обеспечения эффективной координации. В частности.:
    - Централизованный или командный SOC в Киберцентре, который контролирует всеобъемлющую инфраструктуру безопасности GC (включая локальные сети, облачные среды и другие конечные точки), где подразделения извлекают выгоду из экосистемы киберзащиты и получают доступ к своим данным через платформу аналитики безопасности.
    - Многофункциональный центр безопасности инфраструктуры и сетевых операций (ISNOC) в SSC для обеспечения эффективного сетевого мониторинга благополучия основных департаментов и агентств в рамках мандата SSC, наряду с кибербезопасностью общих решений, предоставляемых SSC, а также для поддержки Киберцентра и групп ведомственной безопасности.
    - Специализированные локальные SOC для отдельных департаментов и агентств, которые демонстрируют достаточную зрелость и которым требуются дополнительная наглядность и детализированные показатели в силу их уникальных мандатов или бизнес-потребностей, которые требуют усиленного мониторинга для поддержки кибербезопасности программ и предоставления услуг.
    - Управляемые сервисы SOC для департаментов и агентств, которые не обладают достаточной зрелостью в отношении возможностей мониторинга или ресурсов и которым требуется практическая поддержка в координации.

- Облегчение обмена журналами регистрации и другой важной информацией, хранящейся на уровне предприятия, для обеспечения департаментам и агентствам сквозной видимости потоков данных, поддерживающих их информационные системы, что позволит департаментам и агентствам выполнять свои соответствующие обязанности по обеспечению безопасности.

- **Повысить согласованность предприятия с *Планом управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP) для обеспечения лучшей подготовки к кибератакам, реагирования на них и восстановления после них**
  - Готовьте отделы за счет более эффективного планирования инцидентов и регулярных тренировок с использованием инструментов, которые позволяют проводить упрощенные упражнения по киберсимуляции (также называемые настольными упражнениями) и централизованно предоставлять отчеты о последующих действиях для поддержки расстановки приоритетов рекомендаций с учетом соображений GC в целом. Как минимум, департаменты и агентства будут проводить одно настольное киберучение на уровне заместителя министра каждый год.
  - Содействие сотрудничеству сообщества с помощью платформы управления реагированием на инциденты безопасности для автоматизации ответов на запросы департаментов и агентств о принятии мер и отчетности о них.
  - Разработайте дополнительные инструменты и шаблоны для улучшения мероприятий плана управления мероприятиями по кибербезопасности в департаменте и поддержки выполнения всеобъемлющей структуры GC CSEMP.
  - Создайте группы быстрого и масштабированного реагирования на инциденты и аварийного восстановления с различными наборами навыков для поддержки мероприятий по восстановлению в подразделениях.
- **Повысьте устойчивость критически важных служб GC с помощью усовершенствованных методов управления непрерывностью бизнеса**
  - Разработайте план обеспечения непрерывности бизнеса в масштабах GC, чтобы обеспечить скоординированный подход к управлению событиями, влияющими на множество критически важных служб, чтобы обеспечить непрерывное предоставление программ и услуг GC.

Ожидаемые результаты:

- **Сети, системы, приложения и конечные точки GC контролируются для обеспечения возможности пропорционального и сквозного обнаружения при соблюдении конфиденциальности**
- **Информационные системы GC и критически важные службы, пострадавшие от инцидентов кибербезопасности, быстро восстанавливаются и возобновляют работу с минимальными сбоями**

2.3.4 Цель 4: формирование разнообразной рабочей силы ГК, обладающей необходимыми навыками, знаниями и культурой в области кибербезопасности

Для достижения видения Стратегии и стратегических целей ГК должна культивировать культуру кибербезопасности, которая дает возможность ее сотрудникам учиться, задавать вопросы и бросать вызовы, чтобы способствовать постоянному совершенствованию. Содействие культурному сдвигу в области кибербезопасности во всем правительстве требует повышения осведомленности и знаний по кибербезопасности среди всего персонала GC, чтобы активно реагировать на риски кибербезопасности организации. Согласно документу правительства Канады "Цифровые стандарты: руководство по применению", меры безопасности не должны вызывать затруднений, чтобы не создавать нагрузки на пользователей. Использование надежной культуры кибербезопасности во всем GC повысит квалификацию киберпрофессионалов в GC и позволит GC привлекать, развивать и удерживать эти навыки, а также более эффективно обеспечивать устойчивый карьерный рост. Это также обеспечит повышенную осведомленность и бдительность среди всех сотрудников GC.

Ключевые действия и цели включают:

- **Развивайте навыки в области кибербезопасности**
  - Взаимодействуйте с соответствующими департаментами и агентствами для внедрения программ межфункционального обучения, позволяющих использовать различные обучающие решения, повышающие квалификацию сотрудников из разных отделов, имеющих разный уровень опыта в области кибербезопасности, с целью увеличения штата сотрудников и стратегического охвата для защиты активов GC.
  - Внедрите стандартизированное обязательное обучение по вопросам кибербезопасности в государственных органах для всего персонала GC.
- **Привлечение и удержание разнообразных специалистов в области кибербезопасности**
  - Установите стратегические партнерские отношения с учебными заведениями, отраслевыми группами и другими внешними организациями или сообществами для дальнейшего повышения квалификации и приобретения практического опыта, который может быть использован в GC.
  - Создать центр развития кибернетических кадров, который будет:
    - продвигайте культуру управления талантами, в рамках которой основной целью является набор и удержание кандидатов, обладающих необходимыми кибернетическими навыками и опытом.
    - сокращайте дублирование усилий, стимулируйте межведомственное сотрудничество и обмен знаниями для эффективного развития и удержания талантов и ресурсов.
    - поддержка установления четких путей карьерного роста для сотрудников, включая возможности для продвижения по службе и повышения ответственности, с приоритетным упором на продвижение инклюзивной культуры на рабочем месте путем использования общероссийских программ обеспечения равенства, разнообразия и инклюзивности.
- **Ускорьте прием на работу государственных служащих за счет преобразования системы проверки персонала на безопасность и обеспечения непрерывного контроля**
  - Модернизируйте проверку безопасности персонала за счет усиления политики, автоматизации и внедрения технологий.

Ожидаемые результаты:

- **Культура кибербезопасности во всем GC, которая поощряет поведение, поддерживающее непрерывное обучение и совершенствование, с помощью пула кибер-талантов, стратегически распределяемых между государственными органами.**
- **Надежный режим проверки, который обеспечивает баланс между принятием решений на основе фактических данных и постоянными гарантиями для снижения рисков инсайдерских угроз и сокращением времени, необходимого для найма персонала**

2.4 Логическая модель

Следующая логическая модель была создана для иллюстрации ожидаемых результатов по ключевым входным данным и мероприятиям, а также результирующих результатов.

Таблица 1: логическая модель

Конечный результат	Безопасная и устойчивая Канада
Долгосрочный результат	Устойчивое правительство Канады мирового уровня (GC) для снижения рисков кибербезопасности и обеспечен услуг

Промежуточный результат (от 5 до 10 лет)	Департаменты и агентства используют аналитические данные для определения киберрисков и их влияния на бизнес, чтобы обеспечить эффективное и подотчетное принятие решений		Департаменты и агентства повышают общую кибернетическую зрелость, что приводит к повышению эффективности предотвращения кибератак и противодействия им	Департаменты и агентства создают возможности, необходимые для активной подготовки к событиям кибербезопасности, реагирования на них и восстановления после них	
Немедленный результат (от 2 до 5 лет)	Кибербезопасность - это общегосударственное мероприятие, при котором риски в информационных системах GC постоянно отслеживаются, доводятся до сведения и устраняются эффективным и своевременным образом	Стандартизированные и современные инструменты и устройства, а также общеорганизационные службы кибербезопасности развертываются и используются по всему GC	Для обеспечения постоянной безопасности цифровых сервисов и защиты цифровых активов на протяжении всего их жизненного цикла применяется комплексный подход	Сети, системы, приложения и конечные точки GC контролируются для обеспечения возможности пропорционального и сквозного обнаружения при соблюдении конфиденциальности	Информационные системы GC и критически важные службы, пострадавшие от инцидентов кибербезопасности, быстро восстанавливаются и возобновляют работу с минимальными сбоями
Результаты (2 года)	Интегрированная платформа управления рисками Программа управления уязвимостями Предприятия GC Стандартные положения о безопасности в контрактах для управления рисками сторонних производителей	Артефакты, инструменты и шаблоны архитектуры корпоративной безопасности GC Стратегия и дорожная карта GC по управлению идентификацией, учетными данными и доступом (ICAM) Учебные пособия по безопасности Внедрение служб корпоративной кибербезопасности	Артефакты реализации целевой операционной модели безопасности (TSOM) Разработка безопасных систем и методы моделирования угроз Платформа разработки, безопасности и эксплуатации (DevSecOps) Современная модель категоризации безопасности Политика защиты цифровых данных	Архитектура Федеративного центра управления безопасностью (SOC) Система непрерывного мониторинга Варианты использования мониторинга безопасности	Учебные пособия по Плану управления мероприятиями по кибербезопасности Правительства Канады (GC CSEMP) Платформа реагирования на инциденты безопасности Упрощенное киберсимулирование (настольные упражнения) Команда быстрого реагирования на инциденты Структура жизненного цикла для управления непрерывностью бизнеса подразделения

Деятельность (2 года)	Оптимизируйте управление, уточните ответственность, развивайте функциональные возможности и инструменты, а также измеряйте киберэффективность и зрелость	Создание базовых блоков, разработка рекомендаций и реализация гибких проектов	Внедрение безопасных систем и жизненных циклов разработки, а также разработка процессов безопасной операционной модели	Разработка требований и вариантов использования, уточнение ролей и обязанностей	Управляйте инцидентами, развивайте сотрудничество сообщества, а также разрабатывайте и тестируйте планы обеспечения непрерывности бизнеса и аварийного восстановления
Вклады (2 года)	Информация о человеческих и финансовых ресурсах от партнеров и заинтересованных сторон				

3. Подход к реализации

Для реализации видения и достижения стратегических целей операционная модель целевой безопасности (TSOM) имеет решающее значение для достижения эффективного подхода к проведению операций по обеспечению кибербезопасности, которые позволяют предоставлять цифровые услуги. Эта модель должна учитывать аспекты политики, людей, процессов и технологий, а также подход GC к управлению кибербезопасностью. Этот подход включает функции безопасности идентификации, защиты, обнаружения, реагирования и восстановления, которые представляют собой основные элементы целостной программы кибербезопасности. Этот подход также предоставляет департаментам и агентствам рекомендации по лучшему пониманию, управлению, снижению рисков кибербезопасности и информированию о них, а также дополняет существующие практики, изложенные в *Структуре управления рисками* и программе Киберцентра "*Управление рисками ИТ-безопасности: подход на основе жизненного цикла*" (ITSG-33).

Таким образом, TSOM является вспомогательным инструментом для поддержки практической реализации Стратегии и обеспечивает схему успешных операций по обеспечению кибербезопасности. TSOM иллюстрирует спектр процессов и действий в области безопасности, которые необходимы для обеспечения комплексной безопасности, и предоставляет разбивку заинтересованных сторон, которые либо несут ответственность за каждый процесс и действие, либо поддерживают их. Кроме того, TSOM предоставляет основу для уточнения ответственности и степени, в которой могут потребоваться дополнительные полномочия для достижения целевого состояния кибербезопасности правительственных операций.

Более того, TBS, SSC, CSE, а также департаменты и агентства будут использовать TSOM для руководства разработкой соответствующих ведомственных планов, которые согласуются с этой Стратегией. Ожидается, что эти планы будут включать комплексный подход к планированию инвестиций, который включает кибербезопасность и уделяет приоритетное внимание использованию общих решений и корпоративных сервисов в максимально возможной степени, где и когда они доступны. Ведомственные планы также поддерживают разработку ведомственных дорожных карт. Такие дорожные карты включают технологические карты, которые разрабатываются внутренними корпоративными сервисными организациями, такими как SSC, как ключевая заинтересованная сторона в предоставлении безопасных общих решений.

Мониторинг и оценка общей стратегии потребуются для обеспечения достижения видения и целей Стратегии. В то время как Трехсторонняя организация будет продолжать играть ключевую роль в управлении стратегическими инициативами и надзоре за ними, также потребуется более широкое управление для надзора и получения расширенных гарантий в отношении инвестиций в киберпространство. Это более широкое управление, которое будет основано на полномочиях TBS, связанных с надзором за расходованием средств, будет включать ранний анализ предложений по расходованию средств для обеспечения соответствия Стратегии и приоритетам правительства. Благодаря созданию улучшенных цифровых и технологических

гарантий правительство получит возможность действовать комплексно для содействия повторному использованию общих решений и технологий, а также для улучшения взаимодействия и эффективного совместного использования активов. Это приносит пользу правительству в целом, помогая обеспечить экономию и эффективность, повысить уверенность в предоставлении услуг, снизить риски, поддержать совершенствование возможностей и обеспечить улучшение результатов для GC.

4. Заключение

Хотя в последние годы GC добилась прогресса в повышении кибербезопасности, постоянно меняющаяся среда угроз и развитие технологий продвигаются еще быстрее. Во всех департаментах и агентствах требуется подтверждение приверженности делу надежного и прозрачного обслуживания канадцев таким образом, чтобы поддерживать и укреплять доверие к предоставлению безопасных цифровых услуг. Требуется соответствующий баланс между безопасностью, связанными с этим затратами и опытом работы конечного пользователя. Хотя безопасность имеет первостепенное значение, GC должен придерживаться сильной культуры киберрисков, чтобы гарантировать, что необходимые средства контроля безопасности, соизмеримые с конфиденциальностью и ценностью информации, реализованы экономически эффективным способом с минимальным воздействием на конечного пользователя.

Приложение A: ключевые показатели эффективности

В следующей таблице представлен предлагаемый набор ключевых показателей эффективности для мониторинга прогресса в достижении видения и стратегических целей, изложенных в Стратегии. Эти показатели будут дополнительно рассмотрены в рамках разработки вспомогательной системы управления эффективностью для Стратегии.

Таблица A.1: стратегические цели, ключевые действия и ключевые показатели эффективности

Стратегическая цель	Ключевые действия	Ключевые показатели эффективности
Цель 1: четко сформулировать риски кибербезопасности и их влияние на бизнес для эффективного, ориентированного на конкретные действия и подотчетного принятия решений.	Планируйте и регулируйте устойчивое и интегрированное управление кибербезопасностью	• Процент изменений в нерешенных вопросах соблюдения политики для подразделений, завершивших самооценку
	Улучшите понимание уязвимости в масштабах всей GC и улучшите управление уязвимостями	• Улучшается понимание уязвимости в масштабах всей GC и устраняются уязвимости: (1) в ограниченной степени; (2) в умеренной степени; (3) в значительной степени
	Улучшение управления рисками кибербезопасности сторонних производителей	• Процент критически важных приложений GC, управляемых в рамках нового процесса визуализации цепочки поставок программного обеспечения и управления запасами • Процентная доля отобранных в рамках GC контрактов / подрядчиков с подтвержденным соблюдением договорных обязательств по кибербезопасности

Стратегическая цель	Ключевые действия	Ключевые показатели эффективности
Цель 2: более эффективное предотвращение кибератак и противодействие им, что приведет к большей защите информации и активов GC	Ускорение внедрения современных архитектур кибербезопасности и приложений	• Процент отделов, внедривших гибкий процесс SA & A. • Процент прогресса в завершении плана перехода GC на постквантовую криптографию • Процент подразделений, подключенных как минимум к 1 службе CCCS sensor services
	Внедряйте безопасные, современные и доступные инструменты и устройства на рабочем месте	• Безопасные, современные и доступные инструменты и устройства на рабочем месте используются (1) в ограниченной степени; (2) в умеренной степени; (3) в значительной степени
	Усилить меры по защите данных	• Процентная доля GC, использующих обновленный стандарт категоризации информационной безопасности
Цель 3: укрепление возможностей и устойчивости во всем GC для активной подготовки к событиям кибербезопасности, реагирования на них и восстановления после них	Улучшите возможности мониторинга и обнаружения безопасности, чтобы обеспечить эффективные и адаптируемые варианты для департаментов и агентств	• Процент подразделений, внедривших использование системы мониторинга и операций безопасности GC
	Усовершенствовать методы управления событиями кибербезопасности для подготовки к кибератакам, реагирования на них и восстановления после них	• Практика управления событиями кибербезопасности применяется во всех GC: (1) в ограниченной степени; (2) в умеренной степени; (3) в значительной степени
	Повысьте устойчивость критически важных служб GC с помощью усовершенствованных методов управления непрерывностью бизнеса	• Приложения, которые обеспечивают работу критически важных служб в рамках GC, понимаются: (1) в ограниченной степени; (2) в умеренной степени; (3) в значительной степени
Цель 4: формирование разнообразной рабочей силы ГК, обладающей необходимыми навыками, знаниями и культурой в области кибербезопасности	Развивайте навыки в области кибербезопасности	• Процент сотрудников GC, прошедших обязательное обучение по вопросам безопасности из года в год
	Привлечение и удержание разнообразных специалистов в области кибербезопасности	• Процент сокращения доли вакантных должностей в GC по кибербезопасности
	Ускорьте прием на работу государственных служащих за счет преобразования системы проверки персонала на безопасность и обеспечения непрерывного контроля	• Среднее время приема на работу новых государственных служащих

Приложение B: глоссарий

критически важная услуга или деятельность

Услуга или деятельность, нарушение которой может привести к высокой или очень высокой степени ущерба здоровью, безопасности или экономическому благополучию канадцев или эффективному функционированию правительства Канады.

(Источник: *Политика государственной безопасности*, Приложение B)

кибербезопасность

Кибербезопасность относится к безопасности передачи электронных данных и информации через киберпространство. Она охватывает технологии, процессы, практики, а также меры реагирования и смягчения последствий, предназначенные для защиты электронной информации, данных и информационной инфраструктуры от вреда, несанкционированного использования или сбоев в киберпространстве. Кибербезопасность дополняет ИТ-безопасность. Кибербезопасность вводит в действие средства контроля ИТ-безопасности, изложенные в подразделе B.2.3 Приложения B к *Директиве по управлению безопасностью*.

(Источник: *Руководство по обслуживанию и цифровым технологиям*, подраздел 4.6.1)

мероприятие по кибербезопасности

Любое событие, действие, бездействие или ситуация, которые могут нанести ущерб государственной безопасности, включая угрозы, уязвимости и инциденты.

Примеры мероприятий по обеспечению кибербезопасности:

- раскрытие новой уязвимости
- информация о том, что субъект угрозы может планировать вредоносную киберактивность против информационной системы GC
- попытки взлома периметра сети
- подозрительные или целевые электронные письма с вложениями / ссылками, которые не были обнаружены существующими средствами контроля безопасности
- подозрительная или несанкционированная сетевая активность, представляющая собой отклонение от базового уровня

(Источник: *План управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP), подраздел 1.5)

инцидент с кибербезопасностью

Любое событие (или совокупность событий), действие, бездействие или ситуация, которые привели к компрометации. Примеры инцидентов кибербезопасности включают:

- утечка данных или компрометация / искажение информации
- атаки со взломом учетных данных
- фишинговые кампании
- преднамеренное или случайное внедрение вредоносного ПО в сеть
- атаки типа "отказ в обслуживании"
- искажение или компрометация присутствия в Сети (включая несанкционированное использование учетных записей GC в социальных сетях)
- успешные попытки программ-вымогателей

(Источник: *План управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP), подраздел 1.5)

киберугрозы

Действие, направленное на подрыв безопасности информационной системы путем изменения конфиденциальности, целостности или доступности системы или содержащейся в ней информации.

(Источник: *План управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP), подраздел 1.5)

информационные технологии

Любое оборудование или система, которые используются для сбора, хранения, манипулирования, управления, перемещения, контроля, отображения, переключения, взаимообмена, передачи или приема информации или данных. Она включает в себя все вопросы, связанные с проектированием, разработкой, установкой и внедрением информационных систем и приложений.

(Источник: *Политика в области обслуживания и цифровых технологий*, Приложение A)

внутренняя угроза

Вредоносная угроза организации, исходящая от людей внутри организации, таких как сотрудники, бывшие сотрудники, подрядчики или деловые партнеры, которые владеют внутренней информацией, касающейся методов обеспечения безопасности организации, данных и компьютерных систем.

(Источник: *Национальная стратегия кибербезопасности*, Глоссарий рабочей тетради)

внутренние корпоративные службы

Услуга, предоставляемая департаментом правительства Канады другим департаментам правительства Канады, предназначенная для всего правительства.

(Источник: *Политика в отношении обслуживания и Digital*, Приложение A)

ИТ-безопасность

ИТ-безопасность - это дисциплина применения средств контроля безопасности, решений, инструментов и методик для защиты ИТ-активов от угроз, исходящих от взломов, на протяжении всего их жизненного цикла. ИТ-безопасность фокусируется на безопасности как электронных активов данных, так и физических ИТ-активов. Другими словами, она охватывает, например, безопасность файлов, которые хранятся на устройствах, безопасность систем, используемых для их хранения, и безопасность самих устройств.

(Источник: *Руководство по обслуживанию и цифровым технологиям*, подраздел 4.6.1)

уязвимость

Слабые места в информационной системе, процедурах системной безопасности, внутреннем контроле или реализации, которые могут быть использованы или спровоцированы источником угрозы.

(Источник: *План управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP), подраздел 1.5)

эксплойт нулевого дня

Атака, направленная против уязвимости нулевого дня.

(Источник: *План управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP), подраздел 1.5)

уязвимость нулевого дня

Уязвимость программного обеспечения, о которой еще не известно поставщику, и, следовательно, она не была устранена.

(Источник: *План управления мероприятиями по кибербезопасности правительства Канады* (GC CSEMP), подраздел 1.5)

Примечания

1 Министерство иностранных дел Канады подверглось “значительной” кибератаке, *National Post*, 24 января 2022 г.; Национальный исследовательский совет Канады пострадал от “киберинцидента”, *Globe and Mail*, 21 марта 2022 г.; DDoS-атаки блокируют веб-сайт премьер-министра Трюдо, *IT World Canada*, 11 апреля 2023 г.

Дата изменения:
2024-05-22