Сценарий деловой игры BCP/DR TLD-OPS

Версия 1.0.2

3 декабря 2019 года

Содержание

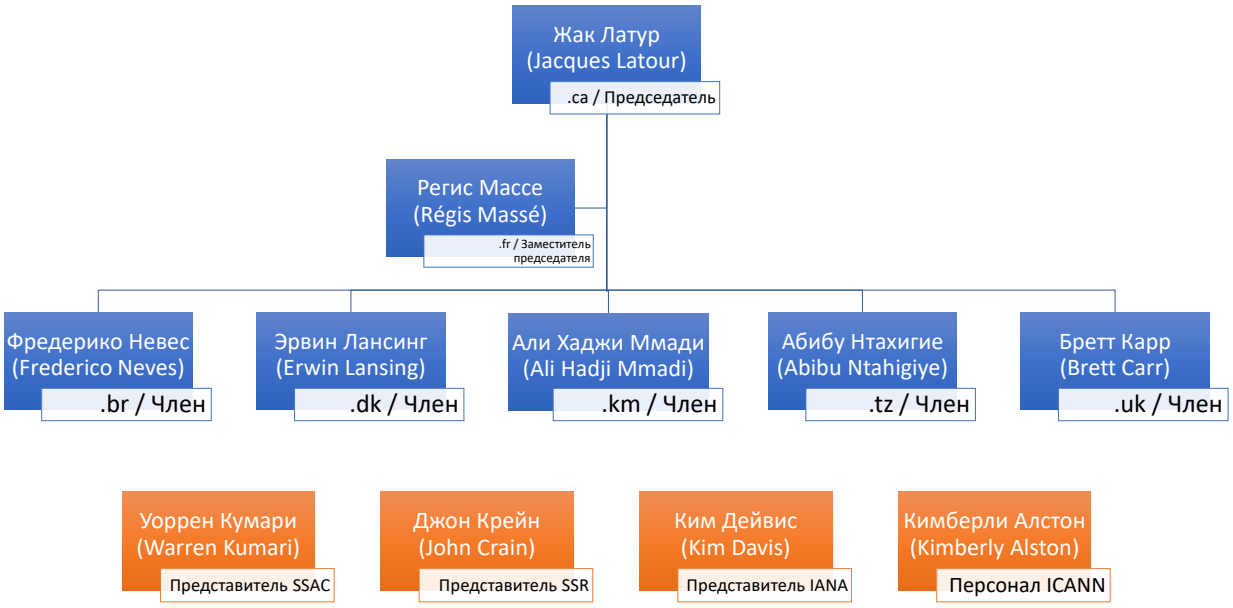
Введение

О TLD-OPS: коллективная безопасность и стабильность ccTLD

TLD-OPS — это созданное национальными доменами верхнего уровня в своих интересах сообщество для реагирования на инциденты, которое объединяет лиц, отвечающих за безопасность и стабильность работы своих ccTLD. Цель сообщества TLD-OPS состоит в том, чтобы дать возможность операторам ccTLD по всему миру обнаруживать и смягчать последствия инцидентов, которые могут повлиять на безопасность и стабильность сервисов ccTLD, например, DDOS-атак, заражения вредоносным ПО и фишинг-атак. Задача TLD-OPS — расширить спектр имеющихся у членов сообщества структур, процессов и средств реагирования на инциденты, но не заменять их. Сообщество TLD-OPS открыто для всех ccTLD, независимо от членства в ccNSO.

Описание: https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm

Особая благодарность Дирку Джамперцу (Dirk Jumpertz), менеджеру по безопасности EURid, за его выдающийся вклад в этот документ и проект.



Постоянный комитет TLD-OPS

Инструкция по использованию этого документа

Этот сценарий деловой игры призван служить практическим руководством для всех, кто хочет реализовать стратегию обеспечения непрерывности бизнеса небольшого оператора регистратуры. Его целевая аудитория — руководители высшего и среднего звена. Предполагается, что контрольный орган (Правление, представители государственной власти или любой другой орган) установил для оператора регистратуры обязательство и миссию повышать устойчивость к инцидентам через план обеспечения бесперебойной деятельности, предоставив финансовую поддержку.

Поскольку этот документ должен носить как можно более практический характер, в нем содержится ряд практических примеров в виде таблиц, которые можно скопировать и использовать на разных этапах разработки и реализации.

В нем также есть несколько примеров, которые могут использоваться в качестве шаблонов или идей при разработке планов обеспечения бесперебойной деятельности/аварийного восстановления.

Наконец, читатель периодически будет встречать в документе вставки «Действия», которые содержат практические предложения и советы: краткое описание действия с указанием лиц, которые должны его выполнить.

Что такое бесперебойная деятельность?

Бесперебойная деятельность — это способность организации после инцидента продолжать на приемлемых, заранее определенных уровнях поставку продуктов или оказание услуг, которые важны для бизнеса оператора регистратуры ccTLD и его заинтересованных сторон.

Обратите внимание, что бесперебойная деятельность связана не только с техническими инцидентами. Любой инцидент, который влияет на готовность организации к работе, может инициировать планы обеспечения бесперебойной деятельности. Поэтому организации важно понять, что может помешать готовности к работе.

Бесперебойная деятельность и аварийное восстановление

Планы обеспечения бесперебойной деятельности (BCP) и планы аварийного восстановления (DRP) взаимосвязаны, но не взаимозаменяемы, хотя, к примеру, при поиске шаблонов через Google результаты могут быть похожими. Первый представляет собой план действий, ориентированный на ведение бизнеса в период кризиса, а второй — его подмножество, которое включает процедуры восстановления жизненно важных для бизнеса систем в кратчайшие сроки.

Иными словами, план обеспечения бесперебойной деятельности будет содержать ссылки на ряд планов аварийного восстановления. В рамках настоящего документа мы разработаем планы обеспечения бесперебойной деятельности, содержащие план действий для конкретного сценария.

Как достичь этой цели?

Используя ряд рекомендаций стандарта ISO 22301 по обеспечению бесперебойной деятельности, можно создать глобальную концепцию, способствующую созданию, реализации и совершенствованию планов обеспечения бесперебойной деятельности.

Поскольку у администраторов доменов в мире ccTLD в основном одинаковая рабочая миссия, можно использовать общий упрощенный подход, в котором главное внимание уделяется практическим вопросам, а не на сложных, трудоемких и иногда теоретических методах разработки правильных планов обеспечения бесперебойной деятельности.

Связь со стандартом ISO/IEC 27001:2013

Стандарт ISO 27001 посвящен информационной безопасности, которая сводится к разработке, внедрению, мониторингу и совершенствованию средств контроля для сохранения уровней конфиденциальности, целостности и доступности, сокращенно обозначаемых как CIA. Для компании, предоставляющей IT-услуги, это в значительной степени пересекается с бесперебойностью деятельности.

Однако есть различие: стандарт ISO/IEC 27001 направлен на достижение требуемых уровней C, I и A в процессе обычной деятельности и предусматривает необходимые меры по смягчению негативного воздействия посредством технологии и процедур, тогда как ISO 22301 посвящен инцидентам, нарушающим деятельность организации, и предусматривает планы действий в случае таких инцидентов.

Для понимания разницы между ISMS (Системой управления информационной безопасностью) и BCMS (Системой управления непрерывностью деятельности) полезно рассмотреть несколько наглядных примеров:

- *Чтобы повысить целостность и доступность, как правило, используется избыточное хранилище с RAID-защитой и дублированием (ISO/IEC 27001).*
- *Чтобы обеспечить минимальные потери при возникновении пожара, проводятся противопожарные учения (ISO 22301).*

· *Чтобы защитить ноутбуки, настольные компьютеры и мобильные устройства от киберугроз, устанавливается антивирусная защита конечных устройств (ISO/IEC 27001).*

· *В то же время, в состав планов обеспечения бесперебойной деятельности включаются отработанные процедуры на случай успешной атаки с использованием программы-вымогателя (ISO 22301).*

Сфера применения (настоящего документа)

Настоящий документ служит руководством по реализации основ обеспечения бесперебойной деятельности и аварийного восстановления небольших операторов регистратур.

Он должен способствовать получению ответов на следующие вопросы:

- Как определить рамки обеспечения бесперебойной деятельности?
- Как определить риски?
- Как сделать обеспечение бесперебойной деятельности неотъемлемой частью структуры компании?
- Что необходимо для эффективной стратегии обеспечения бесперебойной деятельности?
- Какие материалы жизненно важны?
- Как составить план обеспечения бесперебойной деятельности или план аварийного восстановления?
- Как проводить учения по обеспечению бесперебойной деятельности?
- Как вносить улучшения?

Ссылки на нормативные документы

В основе настоящего документа лежат:

- ISO 22301:2012 — Общественная безопасность. Системы менеджмента непрерывности бизнеса. Требования.
- ISO 31000:2009 — Управление рисками. Принципы и руководящие указания.
- ISO/IEC 27001:2013 — Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования

Термины и определения

В настоящем документе используются термины и определения из ISO 22301:2012.

Чтобы понять уровни требований, см. RFC2119.

Среда организации

Хотя у большинства ccTLD почти одинаковый портфель услуг и миссия, всегда есть существенная разница, которая будет задавать направление Стратегии обеспечения бесперебойной деятельности. В целом можно сказать, что рабочая миссия большинства ccTLD заключается в следующем:

- Управлять инфраструктурой DNS-серверов своего TLD.
- Управлять важными для ccTLD общедоступными службами. В частности, это корпоративный сайт и административная служба поиска, такая как WHOIS или RDAP.
- Управлять какими-либо регистрационными услугами, позволяющими выполнять прямую или косвенную регистрацию доменных имен. Это может быть интерфейс пользователя, такой как сайт, или выделенный межмашинный интерфейс, такой как EPP.
- И наконец, что не менее важно, регистратура управляет несколькими корпоративными системами поддержки деятельности, которые могут быть не слишком заметными извне, но необходимы для функционирования организации (например, электронная почта, интрасеть, файловый сервер и т. д.)

Цель этого первого этапа состоит в том, чтобы понять, кто полагается на организацию и, следовательно, имеет определенные ожидания, которые необходимо оправдать во время инцидента, и для кого организация должна выполнять свою миссию.

Понимание организации и ее среды

Первый этап верхнего уровня на пути создания эффективной стратегии обеспечения бесперебойной деятельности состоит в доскональном изучении бизнеса и заинтересованных сторон. У заинтересованных сторон есть конкретные ожидания, требования и сформулированные обязательства, которые необходимо принять во внимание в установленных пределах. Поэтому всегда полезно составить список заинтересованных сторон, описать их и, в конечном итоге, проанализировать их ожидания в отношении функциональной устойчивости и непрерывности деятельности. Для получения правильных данных желательно, чтобы эту работу выполнило

руководство. Столбец «Важность для BC» отражает связь ожидания с непрерывностью деятельности. Некоторые ожидания могут быть не связаны с ней, в то время как другие могут считаться очень важными. В этом смысле можно использовать для указания степени важности уровни ВЫСОКАЯ, СРЕДНЯЯ, НИЗКАЯ и Н/П. Пример: если ожидание считается очень важным в контексте бесперебойной деятельности, по сути, это означает, что у заинтересованной стороны большие ожидания. Фактически, если заинтересованная сторона может ожидать, что «это ВСЕГДА работает», то есть DNS всегда работает; тогда важность будет ВЫСОКОЙ.

В таблице ниже приведен неполный список **примеров**, которые могут помочь в этой работе. На практике желательно сначала просмотреть и обновить таблицу, определить круг заинтересованных сторон (для их опроса), постараться кратко сформулировать ожидания и, наконец, оценить их важность с точки зрения бесперебойной деятельности.

Заинтересованная сторона	**Ожидания**	**Важность для BC**
Государственная власть	Абсолютно безотказное функционирование DNS Целостность и достоверность данных регистратуры Доступность систем регистратуры Экспертный центр в области DNS Научные исследования и разработки в области DNS Злоупотребление доменными именами	ВЫСОКАЯ ВЫСОКАЯ ВЫСОКАЯ Н/П Н/П Н/П
ICANN	Регистрация ccTLD IANA	Н/П
Правление	Абсолютно безотказное функционирование DNS Целостность и достоверность данных регистратуры Доступность корпоративных систем	ВЫСОКАЯ ВЫСОКАЯ СРЕДНЯЯ
Широкая общественность	Доступность DNS Доступность регистрации доменов	ВЫСОКАЯ ВЫСОКАЯ
Группы c-CERT	Информация, относящаяся к безопасности Доступ к данным владельцев доменов	НИЗКАЯ Н/П
Сотрудники	Доступность корпоративных систем	ВЫСОКАЯ
Правоохранительные органы	Целостность регистрации доменов	НИЗКАЯ

Регистраторы	Доступность регистрации доменов	СРЕДНЯЯ
Владельцы доменов	Доступность разрешения доменов Целостность регистрации доменов	НИЗКАЯ НИЗКАЯ
Местный ISP	Разрешение доменов Поддержка DNSSEC	ВЫСОКАЯ Н/П
Сообщество администраторов резолверов	Доступ к файлам зон	Н/П

Таблица 1

Такой список поможет определить приоритеты высокого уровня с точки зрения бесперебойной деятельности.

Канал поставок

В современной предпринимательской среде организации полагаются на ряд партнеров, поставщиков, провайдеров услуг и т. д. Очевидно, что они оказывают важное влияние на стратегию обеспечения бесперебойной деятельности, и поэтому следует понимать зависимость организации от ее канала поставок. Ценным и необходимым видом деятельности является составление списка всех поставщиков, влияющих на выполнение рабочей миссии организации.

Для составления этого списка целесообразно запросить у финансового отдела список всех поставщиков с кратким описанием поставляемых товаров и услуг. Из этого списка можно определить, какие поставщики оказывают реальное влияние на функциональную устойчивость. Пример: поставщик центра обработки данных, очевидно, будет иметь ВЫСОКУЮ важность для BC; с другой стороны, поставщик мебели, такой как Ikea, будет менее важен.

В зависимости от последствий инцидента с поставщиком используются разные метки воздействия:

Воздействие	**Последствия**
КРИТИЧЕСКОЕ	Незамедлительные
СИЛЬНОЕ ВОЗДЕЙСТВИЕ	В течение недели или 7 дней
СРЕДНЕЕ ВОЗДЕЙСТВИЕ	В течение месяца или 30 дней
СЛАБОЕ ВОЗДЕЙСТВИЕ	Позже, чем через месяц или 30 дней

Таблица 2

В следующей таблице **приведен пример**, помогающий составить этот список поставщиков:

Поставщик (наименование)	**Описание**	**Важность для BC**	**Воздействие**
ISP	Интернет-провайдер	ВЫСОКАЯ	КРИТИЧЕСКОЕ
Обработчик кредитных карт	Организация, которая способствует обмену данными между продавцом и банком владельца карты	СРЕДНЯЯ — ВЫСОКАЯ	СИЛЬНОЕ ВОЗДЕЙСТВИЕ
Телефонная компания	Поставщик услуг телефонной связи	СРЕДНЯЯ	СРЕДНЕЕ ВОЗДЕЙСТВИЕ
Почтовая служба	Поставщик почтовых услуг	НИЗКАЯ	НИЗКАЯ
Энергетическая компания	Восстановление электроснабжения		
Компания по расчету заработной платы	Выплаты сотрудникам		
Компания по обслуживанию компьютеров	Покупка настольных компьютеров для сотрудников, серверов для служб		

Сетевые провайдеры/ISP			
Операторы сотовой связи			
Страховая компания			

Таблица 3

Определение рамок обеспечения бесперебойной деятельности

Непрерывность работы как краеугольный камень стратегии BC

Непрерывность работы охватывает все виды деятельности, которые необходимы для ведения «обычного бизнеса». Это подразумевает поддержку заинтересованных сторон, таких как регистраторы, владельцы доменов и широкая общественность с технической, коммерческой и юридической точек зрения. Это также подразумевает эксплуатацию всех технических служб регистрации и управления доменными именами, поддержку бизнеса и, что не менее важно, обеспечение доступности пространства имен TLD для всех пользователей интернета.

Значительную часть технологических последствий следует устранять с помощью стандартных инженерных методов, и поэтому усилия по обеспечению бесперебойной деятельности направлены на составление перечня инцидентов и их предполагаемых результатов применительно к эксплуатационной готовности. При этом определяются меры по смягчению ситуации посредством политики, процедур и, где необходимо, технологий.

Следовательно, определение рамок обеспечения бесперебойной деятельности сводится к следующему:

> Управление **профилактическими** и **корректирующими** мерами с помощью политики, процедур, испытаний и технологии с целью гарантировать **эксплуатационную готовность и непрерывность работы** при возникновении **инцидентов** как **технического**, так и **нетехнического** характера.

Руководство

Разработка и поддержание эффективной и действенной стратегии обеспечения бесперебойной деятельности — это постоянная работа, которая требует поддержки со стороны высшего руководства. Поэтому лучшим местом для защиты и поддержки инициатив, связанных с непрерывностью деятельности, является руководящий состав или даже правление.

Хотя для сохранения актуальности планов необходимы регулярные проверки, руководству также следует взять на себя инициативу по внедрению принципов обеспечения непрерывности детальности на всех уровнях (технологии, инжиниринг, закупки, основная деятельность и т. д.).

ДЕЙСТВИЕ: внедрение руководством как минимум годового цикла проверки и контроль за его осуществлением.

Планирование

В этом разделе дается ответ на вопрос о том, как разработать практические планы обеспечения бесперебойной деятельности, учитывающие угрозы и уязвимости, имеющие отношение к оператору регистратуры, а также воздействие на функциональную устойчивость организации.

Начнем с составления перечня угроз/опасностей, который поможет определить, в каких областях необходимо обеспечить бесперебойность деятельности. Обратите внимание, что некоторые угрозы сложно или даже невозможно смягчить или подготовиться к ним. Стоит изучить угрозу и оценить стратегические варианты. Возможно, результаты такой работы будут отражены не в плане обеспечения бесперебойной деятельности, а в стратегическом выборе[1] в более долгосрочной перспективе.

Чтобы перевести угрозы и опасности в реальные риски, необходимо понять влияние на эксплуатационную готовность и устойчивость. Для определения того, какие сценарии следует рассмотреть, может использоваться упрощенная методология оценки рисков. Исходя из этой оценки, ряд сценариев будет преобразован в тактические планы обеспечения бесперебойной деятельности, в то время как другие сценарии приведут к разработке стратегии обеспечения бесперебойной деятельности, которая может

[1] Типичным примером может служить политическая нестабильность, которую чрезвычайно трудно смягчить. Однако для ccTLD важно учитывать этот фактор в общей стратегии обеспечения бесперебойной деятельности.

использоваться в качестве исходных данных для контрольного органа и дальнейших стратегических решений.

Как только станет ясно, какие угрозы/опасности требуют разработки фактического плана обеспечения бесперебойной деятельности, этот план может быть составлен на основе общего шаблона. Затем этот шаблон следует использовать в качестве руководства для всех отделов при подготовке процедур, где это необходимо.

Составление перечня угроз/опасностей

Перечень угроз/опасностей представляет собой полезный список источников бедствий, которые могут оказать существенное влияние на функциональную устойчивость организации. Нижеприведенный список угроз составлен на основе книги «Управление непрерывностью бизнеса» (4-е издание) ISBN 978-1-931332-35-4 и дополнен с учетом недавних событий.

Изучая эти угрозы, организация должна оценить вероятность события на основе имеющихся статистических данных. Возможность (вероятность) наступления события масштабируется следующим образом:

1. Весьма вероятное: событие повторяется ежегодно или чаще
2. Вероятное: событие происходит в среднем каждые три года
3. Редкое: событие происходит раз в десять лет
4. Маловероятное: событие происходит раз в 50 лет или реже
5. OoS: вне сферы охвата — события не учитываются в рамках обеспечения бесперебойной деятельности

Вероятность определяется на основе не внутренней статистики, а соответствующей статистики по региону, стране, сфере бизнеса и окружающей среде[2]. Важно подчеркнуть необходимость оценки вероятности (таблицы 7 и 8) и воздействия (таблица 6) рисков с учетом текущих средств контроля безопасности. Угрозы определяются на основе статистики, без учета существующих конкретных средств контроля.

[2] Типичный пример: такие погодные явления, как торнадо, могут быть очень актуальными для некоторых регионов США, но не имеют никакого отношения к другим регионам.

Категория угрозы	Угроза	Приме-нимо	Вероятность
Стихийные бедствия	Пожар	☐	_____
	Наводнение	☐	_____
	Ураган/торнадо/тайфун	☐	_____
	Сложные метеоусловия	☐	_____
	Землетрясение	☐	_____
	Оползень/лавина	☐	_____
	Вулканическая активность	☐	_____
	Цунами	☐	_____
	Поражение молнией	☐	_____
	Проседание грунта	☐	_____
	Загрязнение	☐	_____
	Нашествие насекомых	☐	_____
	Грызуны	☐	_____
	_____		
Кадры и медицина	Потеря ключевого персонала	☐	_____
	Эпидемия	☐	_____
	Нехватка навыков/персонала	☐	_____
	Семейные вопросы	☐	_____
	Воровство	☐	_____
	Злоумышленное причинение вреда (саботаж)	☐	_____
	Вымогательство	☐	_____
	_____		_____
Цифровое пространство	DDOS	☐	_____
	Хакеры	☐	_____
	Потеря данных	☐	_____
	Программы-вымогатели	☐	_____
	Деятельность, связанная с информационными войнами	☐	_____
	_____		_____
Внешние факторы	Экономический спад	☐	_____
	Гражданское неповиновение	☐	_____
	Террористическая деятельность	☐	_____
	Война/вторжение	☐	_____
	Политическое вмешательство/политические изменения	☐	_____
	Противоправное проникновение	☐	_____
	Изменения/актуальность технологий	☐	_____
	_____	☐	_____
	_		

Финансовый	Проблемы с движением наличных	☐	_____
	средств/ликвидностью	☐	_____
	Нехватка капитала	☐	_____
	Финансовые преступления	☐	_____
	Безнадежный долг	☐	_____
	Процентный риск	☐	_____
	Валютный риск	☐	_____
	Казначейский риск	☐	_____
	_____		
Технологии и инфра-структура	Отказ сети — глобальный	☐	_____
	Электричество — прекращение электроснабжения	☐	_____
	Неисправности в питающей сети переменного тока	☐	_____
	Неисправности в центрах обработки данных	☐	_____
	Неисправности компонентов[3]	☐	_____
	_____	☐	_____
Сбой в системе поставок	Недопустимый уровень обслуживания	☐	_____
	Низкое качество	☐	_____
	Неполучение услуг	☐	_____
	Невыполнение обязательств в рамках	☐	_____
	аутсорсинга/контракта на поставку	☐	_____
	Отсутствие товаров на складе	☐	_____
	Утрата критически важных активов	☐	_____
	Зависимость от поставщика	☐	_____
	_____		

Таблица 4

Само собой разумеется, что оператор регистратуры должен сосредоточиться на угрозах, которые имеют отношение к его региону и бизнес-среде. Приведенный выше неполный список служит примером. Также можно начать с нескольких угроз/опасностей и расширить их список позже.

ДЕЙСТВИЕ: возможно, координатор или менеджер по ВС захочет сосредоточиться на известных угрозах и опасностях и дополнять их перечень в рамках цикла регулярных проверок.

[3] Неисправности компонентов — это общий термин, обозначающий неисправные компьютерные системы, блоки питания, компьютерную память, диски и т. д. Можно включить это в план обеспечения бесперебойной деятельности или предположить, что такие риски по умолчанию смягчены при проектировании и разработке архитектуры инфраструктуры (то есть благодаря резервным источникам питания, дисковым системам RAID, использованию в серверах памяти ECC и т. д.).

Оценка рисков и управление ими

Что такое риск? Виды рисков.

Согласно стандарту ISO 31000, риск — это «влияние неопределенности на цели», что является очень общим и абстрактным определением высокого уровня. В контексте бесперебойной деятельности, функциональной устойчивости и непрерывности работы риск — это «воздействие инцидента на рабочую миссию оператора регистратуры ccTLD».

Если есть желание выполнить формальную, но простую оценку риска, можно использовать следующую таблицу:

Риск	**Описание**
Финансовый	Событие влечет для организации прямые и косвенные расходы. В зависимости от финансовой устойчивости организации допустимы определенные финансовые потери.
Операционный	Событие препятствует выполнению организацией ее рабочей миссии (то есть прерывается работа служб доменных имен).
Репутационный	Событие может нанести ущерб репутации, который прямо или косвенно повлияет на выполнение рабочей миссии.
Юридический	Событие вызывает юридические проблемы, которые могут привести к штрафам или даже уголовным приговорам.
Управленческий	Событие приводит к политическим последствиям и несоблюдению требований, результатом чего может стать расторжение концессионного договора или политическое вмешательство.
Человеческий	Событие наносит вред здоровью сотрудников (или членов их семей).

Таблица 5

Безусловно, у каждого риска свой уровень, в зависимости от которого этот риск можно принять во внимание при составлении планов обеспечения бесперебойной деятельности. Вот несколько примеров:

- Финансовые потери в размере 1 млн евро могут привести к банкротству оператора регистратуры.

- Событие, в результате которого отдельным лицам выносится уголовный приговор, неприемлемо для оператора регистратуры.
- Событие, которое приводит к телесным повреждениям сотрудников, является недопустимым.

Эта таблица не является исчерпывающей, и оператор регистратуры может решить, что и на каких уровнях использовать. В следующей таблице показаны пять уровней для каждого вида риска. Оператор регистратуры самостоятельно принимает решение о применимости этих уровней и фактических значений.

Вид	**НУЛЕВОЙ или Н/П**	**Низкий**	**Средний**	**Высокий**	**Критический**
Финансовый	Риск не существует или не применим	<1 000 долларов США	<10 000 долларов США	<100 000 долларов США	>100 000 долларов США
Операционный		Воздействует на человека	Воздействует на отдел	Воздействует на регистратуру	Воздействует на общественность
Репутационный		Внутренний	Группы пользователей (ICANN, CENTR)	Общественный	СМИ/политический
Юридический		Административное взыскание	Штраф <10 000 долларов США	Штраф <100 000 долларов США	Штраф >100 000 долларов США, личная ответственность или осуждение по уголовному делу

Управленческий[4]		Правление	Местные органы власти	Политический контроль	Прекращение деятельности регистратуры
Человеческий		Уровень не используется	Уровень не используется	Семья сотрудников	Причинение вреда здоровью

Таблица 6

Желательно использовать цветовую маркировку уровней, так как впоследствии это позволит создать визуальную тепловую карту всех применимых рисков в сопоставлении с возникшими рисками.

Простая оценка рисков/последствий для деятельности

Добавление различных рисков, как описано выше, в таблицу угроз/опасностей дает простое средство анализа последствий для деятельности.

Рассмотрим наглядный пример. Сценарий — DDOS-атаки на рабочую инфраструктуру ccTLD (включая, помимо прочего, сервер доменных имен TLD, а также регистрационные службы; предполагается, что у оператора регистратуры небольшая инфраструктура, в которой все службы объединены и для DNS не используется провайдер Anycast).

Категория угрозы	**Угроза**	**Применимо (Да/Нет)**	**Вероятность**
Цифровое пространство	DDOS	ДА	Очень высокая
Риски	**Уровень**		
Финансовый	СРЕДНЯЯ	DDOS-атака не влечет прямых затрат, так как не приводит к физическому уничтожению имущества. Основная статья расхода — кадровые ресурсы для борьбы с инцидентом. Конечно, это связано с косвенными расходами, поскольку во	

[4] Управленческие риски, возможно, являются самыми сложными и в то же время самыми конкретными видами рисков. Для некоторых регистратур этот риск может полностью отсутствовать. Это требует от руководства четкого определения и описания того, как регистратура зависит от внешних воздействий.

		время атаки не регистрируется ни одно доменное имя.
Операционный	КРИТИЧЕСКАЯ	TLD полностью недоступен или периодически доступен. Это оказывает огромное функциональное влияние на интернет. Точно так же это влияет на другие службы, такие как корпоративный сайт, общедоступную WHOIS и другие регистрационные службы.
Репутационный	ВЫСОКАЯ/ КРИТИЧЕСКАЯ	Инцидент будет замечен всеми пользователями интернета.
Юридический	ВЫСОКАЯ	После инцидента владельцы доменов и регистраторы могут подать иски о возмещении упущенной выгоды. (Это зависит от условий обслуживания и юрисдикции регистратуры.)
Управленческий	ВЫСОКАЯ	Поскольку большинство ccTLD можно считать операторами основных услуг (согласно директиве ЕС по NIS), есть все основания полагать, что от органов государственной власти поступит довольно много запросов.
Человеческий	НУЛЕВАЯ	Это событие не приведет к причинению сотрудникам прямого или косвенного ущерба.
RTO	Для DNS нулевое; эта служба должна функционировать постоянно. Доступ ко всем остальным службам, затронутым DDOS-атакой, должен быть восстановлен в течение рабочего дня.	
RPO	Для DNS допустимо снижение уровня обслуживания до 50% пропускной способности DNS-серверов; все остальные службы должны быть полностью доступны, допустимо снижение пропускной способности до 50%.	

Таблица 7

RTO или «Целевое время восстановления» определяет, как быстро должна быть восстановлена служба. Этот показатель отражает ожидания заинтересованных сторон и юридические или договорные обязательства. Обратите внимание, что для одной угрозы

или опасности могут быть определены разные значения RTO, так как это зависит от затрагиваемых служб.

RPO или «Целевая точка восстановления» определяет необходимый уровень восстановления служб. Она может принимать различные формы, такие как снижение производительности (например, сокращение числа доступных DNS-серверов, уменьшение пропускной способности сервера и т. д.), задержка при оказании услуг, восстановление данных до определенной точки и т. д.

RTO и RPO следует определять исключительно на основе бизнес-данных, а не на основе того, «что может произойти» в случае инцидента.

Такая оценка дает хорошее представление о том, что угрозу необходимо принять во внимание и обработать риск.

Готовность к принятию риска и его обработка

Грубо говоря, есть 5 способов работы с рисками:

1. Принять риск (ничего не делать).
2. Избежать риска (составить альтернативный план).
3. Снизить риск (изменить баланс).
4. Ограничить риск (минимизировать воздействие).
5. Передать риск (переложить его на кого-либо другого, воспользоваться страхованием).

Все планы обеспечения бесперебойной деятельности относятся к варианту 4, когда с помощью заранее определенных мер оказывается противодействие влиянию, а выполнение рабочей миссии восстанавливается до заранее определенного уровня.

С другой стороны, результаты оценки последствий для деятельности также следует принять во внимание, поскольку это может привести к предварительным мерам (вариант 3, снижение риска) и действиям по снижению риска и достижению RTO и RPO.

Давайте вернемся к предыдущему примеру и выясним, что можно сделать для снижения риска до приемлемого уровня.

Ясно, что в этом конкретном случае у DNS абсолютный приоритет, общедоступные службы, такие как корпоративный сайт и общедоступная функция WHOIS, находятся на втором месте, а последними по порядку, но не по важности, идут регистрационные службы.

Категория угрозы	**Угроза**	**Применимо (Да/Нет)**	**Вероятность**
Цифровое пространство	DDOS	ДА	Очень высокая
Снижение рисков			
Принять риск	Не применимо		
Избежать риска	Невозможно, DDOS-атаки инициируются неизвестными противниками.		
Снизить риск	Существующая инфраструктура не сможет гарантировать выполнение требований к ожидаемым RTO/RPO. Возможное решение заключается в использовании решения Anycast для DNS и/или сервисов очистки для остальных служб.		
Ограничить риск	Разработать план обеспечения бесперебойной деятельности в случае DDOS-атак (используя справочное руководство ccNSO по смягчению последствий DDOS-атак), включая дополнительные технические меры (такие как временное перемещение некоторых служб), план связи и план поддержки.		
Передать риск	Не применимо		

Таблица 8

При этом план обработки риска будет содержать различные действия, которые взяты из таблицы выше. Некоторые из них можно реализовать немедленно, другие могут потребовать дополнительного бюджета и дальнейшего утверждения и планирования.

План обработки рисков

При выполнении первоначальной оценки рисков/последствий для деятельности ряд сценариев приведет к неприемлемым уровням риска, или к пониманию того, что в настоящее время нельзя гарантировать выполнение ожиданий и требований в отношении RTO/RPO.

Этот пробел можно устранить благодаря конкретным мерам по снижению рисков. Такие меры должны быть внесены в план, называемый планом обработки рисков. План обработки рисков не входит в состав плана обеспечения бесперебойной деятельности, а существует параллельно. Он предусматривает дополнительные инвестиции, технологическую перестройку существующих служб и инфраструктуры, аутсорсинг определенных видов деятельности и т. д.

План обеспечения бесперебойной деятельности

Прежде чем можно будет составить план, потребуется разъяснить ряд терминов. Как уже упоминалось, BCP служит руководством и планом действий по преодолению кризиса, возникшего после конкретного инцидента.

На высоком уровне алгоритм преодоления кризиса почти всегда одинаков:

1. Оценка ситуации.
2. Сдерживание события.
3. Восстановление до заранее определенных уровней в пределах RTO (целевого времени восстановления) и RPO (целевой точки восстановления).
4. Завершение работы.

Обратите внимание, что окончание кризиса, отмеченное как завершение работы, не означает, что организация вернулась к ситуации «до инцидента». «Завершение работы» означает следующее: кризисная группа считает, что кризисная ситуация находится под контролем, служба восстановлена, организация может выполнять свою рабочую миссию. Это не означает, что ущерб полностью устранен.

Дополнительно проиллюстрировать и прояснить это можно на следующем примере: *в выходные дни вандалы уничтожили и разграбили головной офис регистратуры. IT-оборудование было украдено, мебель разломана. По существу, организация не может использовать свой офис для работы из-за повреждений и текущего расследования. Начинается выполнение плана BCP, согласно которому в случае недоступности офиса телефонные звонки перенаправляются на мобильные устройства, сотрудники информируются о необходимости оставаться дома и до дальнейшего уведомления работать на дому (подразумевается, что для удаленной работы нет препятствий). Кризисная группа вступает в первичные контакты с правоохранительными органами, страховыми компаниями и другими сторонами и обеспечивает выполнение вышеуказанного BCP. Как только это будет сделано, обслуживание будет восстановлено до приемлемого уровня, и организация сможет продолжить выполнение своей рабочей миссии. Кризисная группа выделяет ресурсы для дальнейшего исправления ситуации и возвращения офиса в прежнее состояние. В этот момент кризисная группа завершает работу и возвращается к своей обычной деятельности. Очевидно, что в небольшой организации функции будут совмещаться просто из-за ограниченности доступных ресурсов.*

Жизненно важные материалы — это набор информации (в цифровом или физическом виде), которая абсолютно необходима для того, чтобы справиться с инцидентом. К ней могут относиться контракты, контактные данные определенных сервисов (например, сетевых провайдеров, поставщиков услуг по очистке, арендодателя, органов власти и т. д.), логины и пароли, физические активы, такие как ключи и т. д. Не забудьте

надлежащим образом защитить эти важные материалы, и в то же время держать их в доступном во время кризиса месте.

План обеспечения бесперебойной деятельности: после определения сценариев с наибольшим риском наступает время составления плана. Можно принять решение о составлении подробного плана с описанием каждого действия во время бедствия. Хотя это вполне можно сделать, бедствия часто приводят к неожиданным сопутствующим событиям, которые мешают описать каждый шаг, который необходимо предпринять. Опыт подсказывает, что полезнее составить общее руководство с описанием существенных мер по преодолению кризисной ситуации. Такой план затем может использоваться во время обучения, тестирования и деловых игр.

Также следует оценить последствия сценария. Нет никакого смысла в том, чтобы составлять несколько одинаковых планов BC для разных сценариев. Типичный пример — инцидент, в результате которого офис становится недоступным. На самом деле, независимо от причины (пожар, забастовка, прекращение электроснабжения, наводнение, черная пятница) результат будет одинаковым. Это можно учесть в составе одного плана BC.

Представленный ниже шаблон компактен, и в нем отражены все рассмотренные ранее шаги по преодолению бедствия. Он также помогает сформулировать некоторые подготовительные задачи. **Обратите внимание, что импровизация во время кризиса — наихудший вариант развития событий.** Этот шаблон, в конечном итоге, является всего лишь памяткой, которая призвана помочь кризисной группе изучить ситуацию и подготовиться.

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ (ШАБЛОН)			
Ссылка:	[ССЫЛКА]	Вид угрозы	Затрагиваемые активы
Сценарий:	*Описание условий, которые служат толчком к приведению плана в действие. Это может быть событие, время, конкретное условие и т. д.*		
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:	*Когда план приводится в действие? Это может быть сделано сразу при обнаружении инцидента или через несколько часов.*		
RTO:	*Целевое время восстановления*		
RPO:	*Целевая точка восстановления*		
Кризисная группа:	*Кто входит в состав кризисной группы? Кто будет фактически заниматься преодолением последствий инцидента? Во избежание неоднозначного толкования указывайте имена сотрудников, партнеров, поставщиков.*		
Приоритеты:	*Каковы первоочередные задачи? Это следует толковать как последовательный список.*		
Оценка:	*Начальная стадия преодоления последствий инцидента — это оценка его масштабов. Опишите факторы, которые следует принять во внимание.*		
Сдерживание:	*Опишите порядок действий, направленных на предотвращение ухудшения ситуации.*		
Восстановление:	*Опишите порядок действий, направленных на восстановление минимальной эксплуатационной готовности, с учетом установленных выше приоритетов.*		

Завершение работы:	*После восстановления деятельности кризисная группа завершает работу и оставляет указания относительно дальнейших мер по возврату к состоянию, предшествовавшему инциденту.*
Коммуникация:	*Определите внутренний и внешний информационный обмен, включая сообщение, список адресатов и средства его доставки. Всегда начинайте с внутриорганизационных контактов.*
Жизненно важные материалы:	*Список ресурсов, которые необходимы для преодоления последствий инцидента. Это часть подготовительного этапа. План не содержит фактической информации и ограничен ссылками (подготовка материалов, поддержание их актуальности, точности и, по мере возможности, портативности — обязанность руководителей различных отделов и/или партнеров).*
Отчеты:	*Какие отчеты должны быть составлены во время и после кризиса. Эти отчеты полезны для сбора доказательств, извлечения уроков и отслеживания инцидента.*

Таблица 9

В приложении есть несколько примеров планов BC.

Поддержка

Ресурсы

Первоначальные усилия по созданию системы (управления) бесперебойной деятельностью могут занять довольно много времени. Однако вышеуказанная методика должна сделать эту задачу практически выполнимой для небольшой организации.

После определения необходимых ведомостей и списков эта деятельность становится более рациональной, поскольку необходимы только ежегодные проверки для уточнения планов с учетом изменения угроз и опасностей, например, кибератаки в начале 2000-х годов главным образом относились к области научной фантастики, а сегодня должны рассматриваться как явная и непосредственная опасность.

В небольшой организации лучше всего управлять успешной разработкой плана обеспечения бесперебойной деятельности на уровне руководства, и проекту необходимо оказать достаточную поддержку и внимание.

Нет никакой реальной необходимости назначать отдельного менеджера по бесперебойной деятельности, в некоторых случаях стратегия обеспечения бесперебойной деятельности может стать еще эффективнее, если включить это в обязанности всей организации.

Информированность

Успешная стратегия обеспечения бесперебойной деятельности требует информированности всей организации и понимания того, что каждый должен уделять внимание этим вопросам.

Следовательно, абсолютно необходимы регулярные заседания по повышению информированности.

Коммуникация

Как указано в шаблоне и примере планов обеспечения бесперебойной деятельности, коммуникация (внутренняя и внешняя) играет очень важную роль в кризисном управлении.

Поэтому очень важно:

1. Решить, какие средства связи будут использоваться. Пример: телефон, отправка SMS, передача сообщений, Twitter, электронная почта и т. д.
2. Подготовить шаблоны информационных сообщений (наскоро составленные сообщения могут реально подорвать авторитет организации во время кризиса).
3. Заранее определить и подготовить список тех, кому нужно отправить сообщение, например, «наши регистраторы» — недопустимое определение. Требуется ссылка на актуальный список адресов электронной почты.
4. Установить приоритеты и графики информационного обмена (например, публиковать в Твиттере новое сообщение каждые 60 минут, отправить электронное письмо в начале и в конце инцидента).
5. Оценить необходимость привлечения стороннего консультанта по связи в кризисной обстановке для содействия в определении стратегии и планов коммуникации, а также обучить людей взаимодействию со СМИ.

Приведение в действие

Когда BCP будет подготовлен, его следует включить в состав повседневной деятельности и штатных рабочих процедур. Это означает, что принципы обеспечения бесперебойной деятельности должны играть свою роль во всех технических, коммерческих и трудовых процессах.

Следовательно, бесперебойность деятельности важна в различных областях, таких как снабжение, правовая сфера, инженерно-конструкторские работы, ведение деятельности, коммуникации.

Вот несколько поясняющих примеров:

- Приобретение серверов и сетевого оборудования. В отправленном продавцам запросе предложений (RFP) упоминается о необходимости поставки **резервных источников питания** и сдвоенных **сетевых карт** для максимальной избыточности.
- Передача услуги на **внешний подряд**. В RFP явно указываются ожидаемые меры по обеспечению бесперебойной деятельности, которые ожидаются от поставщика услуг.

Отработка действий по обеспечению бесперебойной деятельности

Полезно разрабатывать планы, чтобы справиться с определенным сценарием бедствия, но без тестирования или тренировки, такой план остается *колоссом на глиняных ногах*.

Следовательно, тестирование и отработка планов BC — очень важная составляющая эффективной стратегии обеспечения бесперебойной деятельности. Подобно тому, как пожарные обучаются пожаротушению, кризисная группа должна потратить некоторое время на фактическое тестирование и отработку планов.

Это можно сделать двумя способами. Есть так называемые деловые игры или TTX и фактическое моделирование контролируемой ситуации.

Деловые игры (TTX)

Эти «теоретические учения» предназначены для проверки процедур и крайне полезны для тренировки групп. Они требуют относительно небольшой подготовки.

TTX может быть ролевой игрой, когда все участвующие стороны сидят за столом и исполняют свои роли. **Независимый распорядитель** будет вести группу по различным этапам сценария, включая в него случайные неожиданные дополнительные события.

Главный недостаток ТТХ — трудность создания у участников ощущения срочности и реальности.

ДЕЙСТВИЕ: важно, чтобы вся организация хотя бы раз в год знакомилась с планами обеспечения бесперебойной деятельности, критически оценивая их осуществимость. Планы ВС — это «живые документы», которые необходимо адаптировать к меняющимся условиям.

Моделирование

Планы обеспечения бесперебойной деятельности тестируются путем моделирования реальных жизненных ситуаций. Во время таких деловых игр проверяются ответные действия различных групп или партнеров для подтверждения эффективности работы групп, а также осуществимости планов.

Отрабатывая различные планы, группы запомнят, что они должны делать, если такое событие действительно произойдет.

Очевидно, что не всегда легко смоделировать инцидент (например, отключение электроснабжения в дата-центре), но могут быть предложены реалистичные сценарии.

Вот несколько примеров:

- Проникновение программы-вымогателя. Пользователь обращается в службу поддержки с вопросом, как ему поступить, поскольку на экране ноутбука отображается сообщение о его взломе и предлагается перевести биткоины в обмен на разблокирование компьютера. Цель такой деловой игры, проверить реакцию группы поддержки.
- Недоступность офиса в связи с нападением крыс. Очевидно, что нет никаких крыс, но цель состоит в том, чтобы проверить связь с сотрудниками.

Совершенствование

Для сохранения эффективности стратегии обеспечения бесперебойной деятельности важно пересматривать планы, оценку рисков, список заинтересованных сторон, список угроз и опасностей и т.д. хотя бы раз в год или после существенных изменений.

Такие изменения, как правило, происходят в результате многих действий:

- принятие новых законов;
- делегирование функций стороннему исполнителю;
- слияния и приобретения;
- новые услуги;

- изменение заинтересованных сторон;
- новые технологии;
- изменение характера угроз;
- инцидент;
- ...

Приложение: Краткое описание задач

В этом приложении суммируются различные задачи, описанные в настоящем документе. Оно может использоваться в качестве контрольного списка, способствующего реализации.

1. Составьте список всех **заинтересованных сторон** и их ожиданий; определите, какие ожидания относятся к бесперебойной деятельности (таблица 1)
2. Составьте список всех **поставщиков** с указанием поставляемых товаров и услуг; определите их важность с точки зрения бесперебойной деятельности и степень влияния (таблица 3)
3. Воспользуйтесь таблицей 4, чтобы составить **перечень угроз и опасностей**; выделите среди них применимые и укажите их вероятность
4. Воспользуйтесь таблицей 5, чтобы определить, какие **риски** имеют отношение к организации; воспользуйтесь таблицей 6, чтобы определить разные уровни для каждого риска.
5. Возьмите перечень угроз и опасностей (таблица 4) и скопируйте применимые угрозы и опасности в **оценку последствий для деятельности** (таблица 7). Можно обобщить данные из всех таблиц в виде тепловых карт, где уровни риска имеют цветовую маркировку, как показано в примере ниже:

Категория угрозы	**Угроза**	**Финансовый**	**Операционный**	**Репутационный**	**Юридический**	**Управленческий**	**Человеческий**
Цифровое пространство	DDOS	Средний	Критический	Высокий/ Критический	Высокий	Высокий	Нулевой

6. Расширьте таблицу 7, которая использовалась для простой оценки последствий для деятельности, и добавьте к ней **обработку рисков** (таблица 8). Ряд угроз будет приводить к недопустимому риску, если его не смягчить; соответственно, в результате составляется план обработки рисков, который содержит меры по снижению риска. Это не подразумевает полного устранения рисков, на самом деле речь идет только об их снижении.
7. Составьте **планы обеспечения бесперебойной деятельности,** используя таблицу 9 как шаблон для тех угроз и опасностей, которые считаются реальной угрозой с высокой степенью воздействия на организацию.

Приложение: Пример плана обеспечения бесперебойной деятельности

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ (ШАБЛОН)			
Ссылка:	[ССЫЛКА]	Вид угрозы	Затрагиваемые активы
Сценарий:	*Описание условий, которые служат толчком к приведению плана в действие. Это может быть событие, время, конкретное условие и т. д.*		
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:	*Когда план приводится в действие? Это может быть сделано сразу при обнаружении инцидента или через несколько часов.*		
RTO:	*Целевое время восстановления*		
RPO:	*Целевая точка восстановления*		
Кризисная группа:	*Кто входит в состав кризисной группы? Кто будет фактически заниматься преодолением последствий инцидента? Во избежание неоднозначного толкования указывайте имена сотрудников, партнеров, поставщиков.*		
Приоритеты:	*Каковы первоочередные задачи? Это следует толковать как последовательный список.*		
Оценка:	*Начальная стадия преодоления последствий инцидента — это оценка его масштабов. Опишите факторы, которые следует принять во внимание.*		

Сдерживание:	*Опишите порядок действий, направленных на предотвращение ухудшения ситуации.*
Восстановление:	*Опишите порядок действий, направленных на восстановление минимальной эксплуатационной готовности, с учетом установленных выше приоритетов.*
Завершение работы:	*После восстановления деятельности кризисная группа завершает работу и оставляет указания относительно дальнейших мер по возврату к состоянию, предшествовавшему инциденту.*
Коммуникация:	*Определите внутренний и внешний информационный обмен, включая сообщение, список адресатов и средства его доставки. Всегда начинайте с внутриорганизационных контактов.*
Жизненно важные материалы:	*Список ресурсов, которые необходимы для преодоления последствий инцидента. Это часть подготовительного этапа. План не содержит фактической информации и ограничен ссылками (подготовка материалов, поддержание их актуальности, точности и, по мере возможности, портативности — обязанность руководителей различных отделов и/или партнеров).*
Отчеты:	*Какие отчеты должны быть составлены во время и после кризиса. Эти отчеты полезны для сбора доказательств, извлечения уроков и отслеживания инцидента.*

ЦИФРОВОЕ ПРОСТРАНСТВО: ДЕЙСТВИЯ ХАКЕРОВ

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ			
Ссылка:	BCP-xxx.yy	ЦИФРОВОЕ ПРОСТРАНСТВО: ДЕЙСТВИЯ ХАКЕРОВ	Глобальный
Сценарий:	Есть доказательства того, что инфраструктура регистратуры была взломана и скомпрометирована. Сторонний злоумышленник установил программное обеспечение, создал учетные записи, средства удаленного доступа и т. д., чтобы проникнуть в систему регистратуры. Могла произойти утечка данных (требующих особенного внимания). .		
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:	СРАЗУ ПОСЛЕ ОБНАРУЖЕНИЯ		
RTO:	24 часа		
RPO:	Потеря данных за 24 часа		
Кризисная группа:	Менеджер юридического отдела – +CC 123 55 88 – ivan.horvat@registry.tld Менеджер технического отдела – +CC 123 44 55 – juan.perez@registry.tld Менеджер по ВС – +CC 123 33 66 – jane.doe@registry.tld Генеральный директор – +CC 123 56 44 – yamado.toro@registry.tld		
Приоритеты:	Защита доступности и целостности DNS-серверов и зоны TLD. Изоляция инфраструктуры DNS-серверов в случае необходимости. Изоляция взломанных систем. Сбор доказательств.		
Оценка:	Если найдено доказательство утечки данных, также привести в действие BCP для утечки данных.		

	Оценить, какие системы скомпрометированы, и составить их список. Какие службы подверглись воздействию? Оказано ли воздействие на DNS, регистрационную платформу, внутренние системы, сайт? Перепроверить инфраструктуру DNS-серверов. Не смог ли хакер закрепить свое присутствие в системе? Присутствует ли хакер в момент обнаружения? Необходима ли внешняя помощь компаний, специализирующихся на инцидентах в цифровом пространстве (существуют ли такие государственные субъекты)?
Сдерживание:	Удостовериться, что инфраструктура DNS-серверов защищена, и изолировать DNS-серверы от затронутой области. Отключить затронутые системы. Не пытаться восстановить или исправить скомпрометированные системы или бороться со злоумышленником. Сосредоточить усилия на изоляции скомпрометированных систем. Постараться собрать доказательства; не нарушать целостности полученных доказательств
Восстановление:	Затронутые системы необходимо восстановить и развернуть повторно. Если скомпрометировано оборудование конечного пользователя, развертываются новые системы.
Завершение работы:	После изоляции и отключения скомпрометированных систем и возобновления работы служб путем восстановления и повторного развертывания систем кризисная группа создает команду для выполнения следующих действий: 1. Обращение в правоохранительные органы и подача иска. 2. Проверка того, что скомпрометированные системы хранятся в безопасном месте, а журналы событий оставлены в качестве доказательств. Анализ целостности основной базы данных (есть ли следы изменений?).

Коммуникация:	Только внутренние контакты Первичное информирование всех о компрометации систем и изоляции скомпрометированных систем. Подчеркнуть, что дальнейшие контакты с внешним миром будут осуществляться непосредственно через менеджера по связям с общественностью, менеджера юридического отдела. Внешняя коммуникация: Проинформировать заинтересованные стороны (правление, органы власти). Проинформировать регистраторов в случае отключения систем (то есть сайта, WHOIS, EPP) и сообщать им о предпринятых дальнейших шагах. Проинформировать правоохранительные органы.
Жизненно важные материалы:	Документация по инфраструктуре и настройке. Хранилище паролей для доступа к различным системам. Развертывание и установка инфраструктуры, необходимой для развертывания новой инфраструктуры. Списки контактов для рассылки сообщений (регистраторы, сотрудники)
Отчеты:	Составить отчет об инциденте: что было обнаружено, какие меры приняты, какие доказательства собраны. Заняться этим во время преодоления кризисной ситуации, а не задним числом.

ВНЕШНИЙ ИНЦИДЕНТ: ТЕРРОРИСТИЧЕСКИЙ АКТ

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ			
Ссылка:	BCP-xxx.yy	ВНЕШНИЙ ИНЦИДЕНТ: ТЕРРОРИСТИЧЕСКИЙ АКТ	Офис
Сценарий:	Рядом с корпоративным офисом (офисами) регистратуры был совершен террористический акт. «Рядом» означает в том же городе или в радиусе 25 км. Этот план действует круглосуточно семь дней в неделю.		
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:	СРАЗУ		
RTO:	Не определено		
RPO:	Не определено		
Кризисная группа:	Ответственный за офис – +CC 123 44 55 – jan.modaal@registry.tld Менеджер отдела кадров – +CC 123 66 23 – maija.meikalainen@registry.tld Менеджер по BC – +CC 123 33 66 – jane.doe@registry.tld Генеральный директор – +CC 123 56 44 – yamado.toro@registry.tld		
Приоритеты:	Безопасность сотрудников.		
Оценка:	В зависимости от серьезности террористического акта его последствия могут создать проблемы (прекращение работы общественного транспорта, развертывание групп СОБР и т. д.). Прежде всего, необходимо обеспечить безопасность сотрудников и их семей. Поскольку регистратура поддерживает возможность работы на дому, сотрудники не должны оставаться в офисе или приезжать в офис.		

Сдерживание:	Если позволяет ситуация, офис будет немедленно закрыт, а сотрудники отправлены по домам. Если террористический акт произошел слишком близко от офиса, сотрудникам рекомендуется оставаться на местах и выполнять указания, поступившие от правоохранительных органов и из официальных источников.
Восстановление:	Ответственный за офис проверяет, что все сотрудники найдены и проинформированы. Он сообщает всем сотрудникам, что офис закрыт и вход в него запрещен до последующего уведомления. Ответственный за офис сообщает о ситуации менеджеру отдела кадров или менеджеру по BC. При необходимости, менеджер отдела кадров или менеджер по BC информируют соответствующие отделы и руководителей о необходимости принять меры.
Завершение работы:	Ответственный за офис выполняет указания, поступившие от правоохранительных органов и из официальных источников, и сообщает сотрудникам, когда офис будет вновь открыт.
Коммуникация:	<u>Только внутренние контакты</u> Первичное информирование сотрудников ответственным за офис лицом устно или путем отправки SMS-сообщений. Последующая отправка сообщений по электронной почте ответственным за офис лицом, менеджером отдела кадров или менеджером по BC.
Жизненно важные материалы:	Список сотрудников с номерами телефонов и адресами электронной почты.
Отчеты:	Отчет о том, что все сотрудники найдены и проинформированы.

ЦИФРОВОЕ ПРОСТРАНСТВО: ПРОГРАММА-ВЫМОГАТЕЛЬ

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ			
Ссылка:	BCP-xxx.yy	ЦИФРОВОЕ ПРОСТРАНСТВО: ПРОГРАММА-ВЫМОГАТЕЛЬ	Офисное оборудование и устройства конечного пользователя
Сценарий:	Заражение программой-вымогателем привело к блокированию нескольких ноутбуков, на которых установлена MS Windows, что сделало их непригодными для использования. Область заражения локализована в одном офисе или распространяется по всей организации.		
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:	СРАЗУ ПОСЛЕ ОБНАРУЖЕНИЯ		
RTO:	В течение рабочего дня.		
RPO:	Потеря данных за один рабочий день.		
Кризисная группа:	Менеджер технического отдела – +CC 123 44 55 – juan.perez@registry.tld Менеджер по BC – +CC 123 33 66 – jane.doe@registry.tld Генеральный директор – +CC 123 56 44 – yamado.toro@registry.tld		
Приоритеты:	Защита доступности и целостности инфраструктуры Windows Server. Изоляция зараженных систем. Восстановление зараженных систем.		
Оценка:	Распространяется ли заражение? Какое устройство было заражено первым? Можно ли изолировать зараженные устройства?		
Сдерживание:	Изолировать зараженные машины (т.е. разорвать сетевые соединения с дата-центром).		

	Отключить незараженные системы дистанционно или, если это представляется невозможным, дать указание пользователям отключить свои системы.
Восстановление:	Зараженные системы следует считать утраченными и требующими повторной установки. Возможно, некоторые сотрудники в течение нескольких дней будут работать без подключения к сети.
Завершение работы:	Кризисная команда создает команду для выполнения следующих действий: 1. Идентификация программы-вымогателя и проверка подписей или использование других методов обнаружения. 2. Определение источника заражения... какое устройство было заражено первым? 3. Создание в месте заражения изолированных сетевых сред (проводной и беспроводной); незараженные системы должны быть запущены и перепроверены, чтобы убедиться в том, что они действительно не заражены вредоносным ПО; 4. Составление плана переустановки программного обеспечения на зараженные ноутбуки. Для удаленных офисов это может оказаться проблемой, которая приведет к необходимости отправки инженера на объект. 5. Подача официального иска в правоохранительные органы или другие органы власти в зависимости от юридических обязательств/рекомендаций.
Коммуникация:	<u>Только внутренние контакты</u> Сообщить всем сотрудникам о проникновении программы-вымогателя и дать им указание (по электронной почте, по телефону или путем передачи сообщений) немедленно отключить свои ноутбуки (Windows).
Жизненно важные материалы:	Документация по инфраструктуре и настройке. Хранилище паролей для доступа к различным системам. Списки контактов для рассылки сообщений (сотрудники).
Отчеты:	Составить отчет об инциденте: что было обнаружено, какие меры приняты, какие доказательства собраны. Заняться этим во время преодоления кризисной ситуации, а **не** задним числом.

Приложение: Семинар

График проведения семинара

	Описание	Время в минутах	Докладчик
1	Презентация руководства - Раздать документ плана DR/BCP	45	
2	Ответы на вопросы, касающиеся руководства	15	
3	Заполнение форм: BIA – BCP - с учетом специфики своего ccTLD - раздать шаблон плана DR/BCP	45	
4	Обсуждение результатов заполнения форм	30	
5	Создание групп (не более 5) - раздать карточки, регистратура ОК и план BCP на случай хакерской атаки	5	
6	Ознакомление с карточками	10	
7	5 раундов деловых игр (TTX)	60	
8	Подведение итогов деловой игры	30	

(240 минут)

Презентация и обучение заполнению форм

Проведите 45-минутную презентацию + 15 минут для ответа на вопросы о документе, чтобы выделить главные темы.

В течение этих 45 участникам предоставляется возможность

1. Составить список заинтересованных сторон и записать их ожидания
2. Проанализировать перечень угроз и определить, какие из них необходимо учесть?
3. Оценить, какие риски важны для организации и определить их уровни.
4. Выбрать угрозу и оценить соответствующие последствия для деятельности (BIA)
5. Составить для этой угрозы план обеспечения бесперебойной деятельности (BCP); перечислить жизненно важные материалы

Список заинтересованных сторон

Включенные в этот список заинтересованные стороны служат всего лишь примером. Не стесняйтесь добавлять заинтересованные стороны, которые не упомянуты, но важны, по вашему мнению. Важность для BC: ВЫСОКАЯ, СРЕДНЯЯ, НИЗКАЯ, Н/П

Заинтересованная сторона	**Ожидания**	**Важность для BC**
Государственная власть	_____ _____ _____	_____ _____ _____
ICANN	_____ _____ _____	_____ _____ _____
Правление	_____ _____ _____	_____ _____ _____
Широкая общественность	_____ _____ _____	_____ _____ _____
Правоохранитель-ные органы	_____ _____ _____	_____ _____ _____
Регистраторы	_____ _____ _____	_____ _____ _____
Владельцы доменов	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____

Перечень угроз

Проверьте, какие угрозы применимы и какова их вероятность на основе статистических данных.

Категория угрозы	Угроза	Применимо (Да/Нет)	Вероятность
Стихийные бедствия	Пожар Наводнение Ураган/торнадо/тайфун Сложные метеоусловия Землетрясение Оползень/лавина Вулканическая активность Цунами Поражение молнией Проседание грунта Загрязнение Нашествие насекомых Грызуны _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
Кадры и медицина	Потеря ключевого персонала Эпидемия Нехватка навыков/персонала Семейные вопросы Воровство Злоумышленное причинение вреда (саботаж) Вымогательство _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Цифровое пространство	DDOS Хакеры Потеря данных Программы-вымогатели Деятельность, связанная с информационными войнами _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____
Внешние факторы	Экономический спад Гражданское неповиновение Террористическая деятельность Война/вторжение Политическое вмешательство/политические изменения Противоправное проникновение Изменения/актуальность технологий _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

Финансовый	Проблемы с движением наличных средств/ликвидностью Нехватка капитала Финансовые преступления Безнадежный долг Процентный риск Валютный риск Казначейский риск _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Технологии и инфра-структура	Отказ сети — глобальный Электричество — прекращение электроснабжения Неисправности в питающей сети переменного тока Неисправности в центрах обработки данных Неисправности компонентов[5] _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
Сбой в системе поставок	Недопустимый уровень обслуживания Низкое качество Неполучение услуг Невыполнение обязательств в рамках аутсорсинга/контракта на поставку Отсутствие товаров на складе Утрата критически важных активов Зависимость от поставщика _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

Вероятность:

1. Весьма вероятное: событие повторяется ежегодно или чаще
2. Вероятное: событие происходит в среднем каждые три года
3. Редкое: событие происходит раз в десять лет
4. Маловероятное: событие происходит раз в 50 лет или реже
5. OoS: вне сферы охвата — события не учитываются в рамках обеспечения бесперебойной деятельности

[5] Неисправности компонентов — это общий термин, обозначающий неисправные компьютерные системы, блоки питания, компьютерную память, диски и т. д. Можно включить это в план обеспечения бесперебойной деятельности или предположить, что такие риски по умолчанию смягчены при проектировании и разработке архитектуры инфраструктуры (то есть благодаря резервным источникам питания, дисковым системам RAID, использованию в серверах памяти ECC и т. д.).

Таблица рисков

Вид	НУЛЕВОЙ или Н/П	Низкий	Средний	Высокий	Критический
Финансовый	риск не существует или не применим				
Операционный					
Репутационный					
Юридический					
Управленческий[6]					
Человеческий					

[6] Управленческие риски, возможно, являются самыми сложными и в то же время самыми конкретными видами рисков. Для некоторых регистратур этот риск может полностью отсутствовать. Это требует от руководства четкого определения и описания того, как регистратура зависит от внешних воздействий.

Оценка последствий для деятельности

Выберите в перечне одну из угроз, которая оказывает очевидное воздействие на бесперебойность деятельности, и на основе таблицы рисков оцените ее влияние на различные риски. Вероятность берется из перечня угроз.

Вероятность:

1. Весьма вероятное: событие повторяется ежегодно или чаще
2. Вероятное: событие происходит в среднем каждые три года
3. Редкое: событие происходит раз в десять лет
4. Маловероятное: событие происходит раз в 50 лет или реже
5. OoS: вне сферы охвата — события не учитываются в рамках обеспечения бесперебойной деятельности

RTO (целевое время восстановления или скорость восстановления деятельности после прерывания) и RPO (допустимые потери данных) определяются условиями деятельности (это могут быть договорные, юридические, управленческие требования); не следует принимать во внимание, что является технически возможным или невозможным.

Категория угрозы	**Угроза**	**Применимо (Да/Нет)**	**Вероятность**
		Да	
Риски	**Уровень**	**Мотивировка/описание/пояснение**	
Финансовый			
Операционный			
Репутационный			
Юридический			

Управленческий		
Человеческий		
RTO		
RPO		
Снижение рисков	«Н/П» или описание планов по снижению риска	
Принять риск		
Избежать риска		
Снизить риск		
Ограничить риск		
Передать риск		

План обеспечения бесперебойной деятельности

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ (ШАБЛОН)			
Ссылка:	[ССЫЛКА]	Вид угрозы	Затрагиваемые активы
Сценарий:	*Описание условий, которые служат толчком к приведению плана в действие. Это может быть событие, время, конкретное условие и т. д.*		
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:	*Когда план приводится в действие? Это может быть сделано сразу при обнаружении инцидента или через несколько часов.*		
RTO:	*Целевое время восстановления*		
RPO:	*Целевая точка восстановления*		
Кризисная группа:	*Кто входит в состав кризисной группы? Кто будет фактически заниматься преодолением последствий инцидента? Во избежание неоднозначного толкования указывайте имена сотрудников, партнеров, поставщиков.*		
Приоритеты:	*Каковы первоочередные задачи? Это следует толковать как последовательный список.*		
Оценка:	*Начальная стадия преодоления последствий инцидента — это оценка его масштабов. Опишите факторы, которые следует принять во внимание.*		
Сдерживание:	*Опишите порядок действий, направленных на предотвращение ухудшения ситуации.*		
Восстановление:	*Опишите порядок действий, направленных на восстановление минимальной эксплуатационной готовности, с учетом установленных выше приоритетов.*		

Завершение работы:	*После восстановления деятельности кризисная группа завершает работу и оставляет указания относительно дальнейших мер по возврату к состоянию, предшествовавшему инциденту.*
Коммуникация:	*Определите внутренний и внешний информационный обмен, включая сообщение, список адресатов и средства его доставки. Всегда начинайте с внутриорганизационных контактов.*
Жизненно важные материалы:	*Список ресурсов, которые необходимы для преодоления последствий инцидента. Это часть подготовительного этапа. План не содержит фактической информации и ограничен ссылками (подготовка материалов, поддержание их актуальности, точности и, по мере возможности, портативности — обязанность руководителей различных отделов и/или партнеров).*
Отчеты:	*Какие отчеты должны быть составлены во время и после кризиса. Эти отчеты полезны для сбора доказательств, извлечения уроков и отслеживания инцидента.*

План обеспечения бесперебойной деятельности

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ (ШАБЛОН)			
Ссылка:	[ССЫЛКА]	Вид угрозы	Затрагиваемые активы
Сценарий:			
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:			
RTO:			
RPO:			
Кризисная группа:			
Приоритеты:			
Оценка:			
Сдерживание:			
Восстановление:			
Завершение работы:			

Коммуникация:	
Жизненно важные материалы:	
Отчеты:	

Описание деловой игры (TTX)

Деловая игра проводится по полностью подготовленному сценарию и предусматривает 5 раундов 10 минут. В начале каждого раунда группа получает исходную информацию и должна отреагировать на нее, используя соответствующий план обеспечения бесперебойной деятельности.

Чтобы способствовать выполнению этой задачи, членам каждой группы раздаются карточки. На карточках указаны действия, которые нужно выполнить в ответ на полученную в начале раунда информацию.

Участник может выбрать до 3 действий (карточек) за один раунд, которые откладываются в сторону для последующего обсуждения. Карточки сгруппированы по 4 категориям: ТЕХНИЧЕСКАЯ, ЮРИДИЧЕСКАЯ, УПРАВЛЕНИЕ, КОММУНИКАЦИЯ. По существу, они соответствуют техническому отделу, юридическому отделу, руководству и отделу по связям.

При проведении раунда может быть представлена дополнительная информация, которую группа должна обработать и, возможно, скорректировать свои действия.

После 5 раундов карточки собираются и обсуждаются в контексте ряда тем для получения обратной связи от участников.

Описание регистратуры

Вы работаете в «**регистратуре OK**». Это оператор регистратуры ccTLD .ok. OK или Old Kontry — небольшая европейская страна с населением около 50 000 человек. Из-за своей либеральной политики домен верхнего уровня .ok довольно популярен, и по состоянию на 1 ноября 2019 года в нем зарегистрировано 372 304 доменных имени. Доменные имена .ok продаются через международную сеть, в которой около 250 регистраторов.

Old Kontry — унитарная парламентская конституционная монархия.

Old Kontry не входит в ЕС.

Регистратура находится в столице и входит в состав «**Университета OK**», но является самостоятельным подразделением (в управленческом, финансовом и техническом отношениях); однако университет — контролирующий орган.

Для своих серверных служб она использует услуги компании MegaRyCorp. Inc., немецкого поставщика услуг регистратуры, который специализируется на предоставлении серверных служб регистратурам. За оказание услуг DNS 1 отвечает американский провайдер Anycast, но у регистратуры есть 3 старых DNS-сервера Unicast, работающие в университетской сети.

Для обеспечения своего интернет-присутствия (корпоративный сайт, социальные медиа и т.д.) регистратура в значительной степени полагается на местное креативное агентство по работе с данными и технологиями, которое входит в состав международной группы.

Помимо скрытого основного DNS-сервера и авторитативных DNS-серверов, регистратура управляет сервером EPP, сервером WHOIS и внешней сетью регистраторов, имеющей те же функциональные возможности, что и EPP, и не только.

Из-за популярности и значимости этого домена для местной экономики **правительство OK** приняло за последние несколько лет ряд законов, соответствующих европейским GDPR по защите персональных данных и директиве NIS по защите критической инфраструктуры и операторов основных услуг. Оно также назначило Министерство связи контролирующим и директивным органом.

«**Регистратура OK**» — небольшая организация, в которой 7 штатных сотрудников. Она может пользоваться IT-поддержкой университета в отношении ноутбуков, настольных компьютеров, электронной почты и т. д.

Среди сотрудников 3 инженера (1 разработчик, 1 системный администратор и 1 сетевой инженер), которые занимаются веб-порталом регистратора, осуществляют текущий контроль, обслуживают старые DNS-серверы, брандмауэры, (W)LAN, поддерживают регистраторов и составляют технические отчеты.

Есть генеральный директор, менеджер по продажам и маркетингу, финансовый директор и менеджер юридического отдела; техническая группа подчиняется непосредственно генеральному директору. Управление непрерывностью бизнеса входит в круг обязанностей менеджера юридического отдела.

План BCP для сценария ЦИФРОВОЕ ПРОСТРАНСТВО: ДЕЙСТВИЯ ХАКЕРОВ

ПЛАН ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ ДЕЯТЕЛЬНОСТИ			
Ссылка:	BCP-101.01	ЦИФРОВОЕ ПРОСТРАНСТВО: ДЕЙСТВИЯ ХАКЕРОВ	Глобальный
Сценарий:	Есть доказательства того, что инфраструктура регистратуры была взломана и скомпрометирована. Сторонний злоумышленник установил программное обеспечение, создал учетные записи, средства удаленного доступа и т. д., чтобы проникнуть в систему регистратуры. Могла произойти утечка данных (требующих особенного внимания).		
ПРИВЕДЕНИЕ В ДЕЙСТВИЕ:	СРАЗУ ПОСЛЕ ОБНАРУЖЕНИЯ		
RTO:	24 часа		
RPO:	Потеря данных за 24 часа		
Кризисная группа:	Менеджер юридического отдела – +CC 123 55 88 – ivan.horvat@registry.tld Менеджер технического отдела – +CC 123 44 55 – juan.perez@registry.tld Менеджер по BC – +CC 123 33 66 – jane.doe@registry.tld Генеральный директор – +CC 123 56 44 – yamado.toro@registry.tld		
Приоритеты:	Защита доступности и целостности DNS-серверов и зоны .ok. Изоляция инфраструктуры DNS-серверов в случае необходимости. Изоляция взломанных систем. Сбор доказательств.		
Оценка:	Оценить, какие системы скомпрометированы, и составить их список. Какие службы подверглись воздействию? Оказано ли воздействие на DNS, регистрационную платформу, внутренние системы, сайт? Перепроверить инфраструктуру DNS-серверов и службы. Не смог ли хакер закрепить свое присутствие в системе? Присутствует ли хакер в момент обнаружения? Необходима ли внешняя помощь компаний, специализирующихся на инцидентах в цифровом пространстве (существуют ли такие государственные субъекты)?		

	Произошла ли утечка данных и если да, то каких именно? Каковы последствия утечки данных?
Сдерживание:	Удостовериться, что инфраструктура DNS-серверов защищена, и изолировать DNS-серверы от затронутой области. Отключить затронутые системы. Не пытаться восстановить или исправить скомпрометированные системы или бороться со злоумышленником. Сосредоточить усилия на изоляции скомпрометированных систем. Постараться собрать доказательства; не нарушать целостности полученных доказательств
Восстановление:	Затронутые системы необходимо восстановить и развернуть повторно. Если скомпрометировано оборудование конечного пользователя, развертываются новые системы.
Завершение работы:	После изоляции и отключения скомпрометированных систем и возобновления работы служб путем восстановления и повторного развертывания систем кризисная группа создает команду для выполнения следующих действий: 1. Обращение в правоохранительные органы и подача иска. 2. Проверка того, что скомпрометированные системы хранятся в безопасном месте, а журналы событий оставлены в качестве доказательств. Анализ целостности основной базы данных (есть ли следы изменений?).
Коммуникация:	**Внутренняя коммуникация:** Первичное информирование всех о компрометации систем и изоляции скомпрометированных систем. Подчеркнуть, что дальнейшие контакты с внешним миром будут осуществляться непосредственно через менеджера по продажам и маркетингу или менеджера юридического отдела. **Внешняя коммуникация:** Проинформировать заинтересованные стороны (правление университета, органы власти). Проинформировать регистраторов в случае отключения систем (то есть сайта, WHOIS, EPP) и сообщать им о предпринятых дальнейших шагах. Проинформировать правоохранительные органы. Регулярно публиковать информацию о продвижении работ в социальных медиа и на общедоступном сайте.

Жизненно важные материалы:	Документация по инфраструктуре и настройке. Хранилище паролей для доступа к различным системам. Развертывание и установка инфраструктуры, необходимой для развертывания новой инфраструктуры. Списки контактов для рассылки сообщений (регистраторы, сотрудники, заинтересованные стороны)
Отчеты:	Составить отчет об инциденте: что было обнаружено, какие меры приняты, какие доказательства собраны. Заняться этим во время преодоления кризисной ситуации, а не задним числом.

Сценарий деловой игры

РАУНД 1: исходная информация Пятница, 17:00

- С генеральным директором оператора регистратуры связывается специалист по безопасности и сообщает о том, что он обнаружил в веб-приложении Pastebin часть базы данных, которая, по-видимому, указывает на внешнюю сеть регистратуры, используемую регистраторами.
- Этот исследователь проверил хэшированные на Pastebin пароли и сумел довольно легко «взломать» некоторые из них. Как и ожидалось, довольно часто встречается пароль «password123». Он подтверждает, что несколько раз вошел во внешнюю сеть регистраторов (и передает директору данные об этих операциях входа в сеть).
- Данные все еще находятся в веб-приложении Pastebin, и исследователь также нашел доказательства того, что кто-то продает учетные данные в глубоком интернете.
- По его мнению, собранные доказательства дают основания считать, что какой-то злоумышленник взломал систему регистратуры и начал наживаться на этом.

Такова исходная информация, полученная регистратурой. Как отреагирует генеральный директор, что он сделает? С этого момента к директору должна поступать некоторая дополнительная информация в зависимости от его плана действий. Не забывайте следить за временем. У участников есть только 15 минут на каждый раунд.

ВЫБЕРИТЕ 3 КАРТОЧКИ

РАУНД 2: исходная информация Пятница, 20:00

- С момента обнаружения взлома прошло 3 часа.
- Кто-то опубликовал в Твиттере ссылку на другое веб-приложение Pastebin с хэштегом #freeDomains4All #longLive.OK; это копия оригинального сообщения Pastebin.
- Этот твит становится популярным и делаются его ретвиты; хэштег исправлен на #itWorks.

ВЫБЕРИТЕ 3 КАРТОЧКИ

РАУНД 3: исходная информация Пятница, 22:00

- Прошло 2 часа.
- С оператором регистратуры связываются журналисты, которые хотят узнать, что происходит, и просят сделать официальное заявление.
- Генеральному директору оператора регистратуры звонят представители государственного телеканала.
- Инженеры по-прежнему изучают вопрос, но еще не нашли причину утечки данных.

ВЫБЕРИТЕ 3 КАРТОЧКИ

БОНУСНЫЙ РАУНД: исходная информация (за 3 минуты до конца раунда)

Чтобы сделать деловую игру интереснее, можно сообщить дополнительную информацию. В реальной жизни ход событий нельзя предсказать, тем более во время кризиса. Во время бонусных раундов поступает дополнительная информация, которую нужно успеть проанализировать и на которую нужно успеть отреагировать до конца раунда.

- У инженеров есть и хорошие, и очень плохие новости.
- Они нашли точку входа хакеров в систему и отследили внесенные изменения.
- Они также заметили, что зарегистрировано больше 50 000 новых доменных имен и изменено неопределенное количество существующих доменных имен, часть которых — широко известные доменные имена.
- Они предлагают вернуть DNS в исходное состояние и обратиться к крупным интернет-провайдерам с просьбой перезагрузить резолверы.

ОБНОВИТЕ 3 КАРТОЧКИ

РАУНД 4: исходная информация Суббота, 06:00

- Прошло 8 часов.
- С оператором регистратуры связывается национальная группа CERT; она получила информацию об источнике атаки.
- Обеспокоенные владельцы доменов и регистраторы засыпают вопросами страницы оператора регистратуры в социальных медиа.
- В основных почтовых ящиках накопилось больше 5 000 электронных писем.
- Представители СМИ опять обращаются к оператору регистратуры за новой информацией и интересуются, почему устранение проблемы занимает так много времени.
- Соответствующее контролирующее министерство (например, министерство связи) связывается с генеральным директором оператора регистратуры, желая получить информацию о состоянии дел и последствиях инцидента.

ВЫБЕРИТЕ 3 КАРТОЧКИ

РАУНД 5: завершение Воскресенье, 09:00

- Прошел 21 час.
- Технические специалисты вернули базу данных в состояние, которое она имела в четверг в 23:47, воспользовавшись последней резервной копией без признаков изменения доменных имен.
- DNS-серверы были перезагружены.
- Уязвимость, которой воспользовались хакеры, была устранена.
- Все учетные данные регистраторов были сброшены.
- Служба поддержки получила список затронутых доменных имен, регистраторов и владельцев доменов.
- У службы поддержки очень много незавершенной работы, поскольку поступило больше 10 000 электронных писем с заявками на обслуживание и бесчисленное количество твитов с претензиями.
- Несколько блогеров и видеоблогеров заинтересовались проблемой и опубликовали свои мнения.

ВЫБЕРИТЕ 3 КАРТОЧКИ

КОНЕЦ ДЕЛОВОЙ ИГРЫ — ПАУЗА

Участникам потребуется перерыв ☺.

ПОДВЕДЕНИЕ ИТОГОВ

Каждая группа демонстрирует свои карточки.

Чтобы деловая игра была эффективной и результативной, важно правильно подвести итоги и обсудить действия группы. Поэтому требуется регистрация действий кризисной группы в письменном виде или с помощью аудиозаписи. При подведении итогов следует сосредоточить внимание на ряде тем:

1. Каковы общие впечатления от деловой игры?
2. Насколько хорошо соблюдался план обеспечения бесперебойной деятельности?
3. Когда группа начала импровизировать?
4. Возникло ли ощущение компетентности и способности справиться с задачей?
5. Чему они научились?
6. Что необходимо улучшить?

Карточки

Распечатайте эти карточки в формате визиток, используя для каждой категории свой цвет.

	ТЕХНИЧЕСКАЯ	ЮРИДИЧЕСКАЯ/ УПРАВЛЕНИЕ ВС	КОММУНИКАЦИИ	РУКОВОДСТВО
1	Отключить авторитативные DNS-серверы	Обратиться в правоохранительные органы	Опубликовать информацию о состоянии дел в социальных медиа	Объявить о возникновении чрезвычайной ситуации
2	Связаться с оператором услуг регистратуры и сообщить о проблеме	Порекомендовать руководству стратегию коммуникации	Опубликовать сообщение в социальных медиа	Созвать кризисную группу
3	Связаться с оператором Anycast и сообщить о проблеме	Обратиться за помощью в решении проблемы к сторонней компании по реагированию на инциденты	Ответить журналистам	Привести в действие план обеспечения бесперебойной деятельности
4	Отключить регистрационную платформу	Дать рекомендацию максимально ограничить информационный обмен	Подготовить сообщение о возврате в прежнее состояние	Связаться с контролирующим органом/правлением
5	Начать поиск в доступных журналах событий	Рекомендовать руководству обеспечить полную транспарентность	Составить пресс-релиз(ы)	Проинформировать органы государственного контроля
6	Восстановить основную базу данных	Попросить местных провайдеров связи перезагрузить свои резолверы	Составить шаблоны сообщений в период кризиса	Связаться с национальной группой CERT и сообщить об инциденте
7	Переустановить скомпрометирован-ные системы	Передать результаты правоохранительным органам	Отправить журналистам заявления о последствиях	Провести пресс-конференцию

8	Провести техническую оценку и собрать доказательства взлома систем	Попросить регистраторов сменить пароли	Не передавать никаких сообщений по каналам общего доступа без разрешения со стороны менеджера юридического отдела и генерального директора	Представить органам государственного контроля отчет о состоянии дел
9	Начать отвечать на поступившие по электронной почте в службу поддержки заявки на обслуживание и другие запросы	Сообщить о проблеме Европейскому совету по защите данных	Разослать внутренний отчет о состоянии дел	Объявить об окончании кризиса и завершить работу — вернуться к обычной деятельности
10	Составить список измененных доменных имен для идентификации пострадавших	Подать заявление об инциденте в правоохранительные органы	Нанять специалиста по кризисным коммуникациям	Обратиться к национальной группе CERT с просьбой о помощи
11	Составить список добавленных доменных имен	Проинформировать страховую компанию	Отрицать факт взлома	Проинформироват ь ICANN
12	Заблокировать доступ к регистрационной системе	Проинформировать пострадавших владельцев доменов	Отправить TLD-OPS электронное письмо с просьбой о помощи	Воспользоваться круглосуточной линией экстренной связи IANA
13	Сменить все пароли	Проинформировать остальные регистратуры через лист рассылки TLD-OPS		Обвинить TLD-OPS :-)
14	Загрузить список паролей из веб-приложения Pastebin	Обратиться к остальным регистратурам через лист рассылки TLD-OPS с просьбой о помощи		
15	Установить SIEM			

Подготовленный к печати комплект карточек доступен для загрузки на сайте TLD-OPS в формате Adobe InDesign.

ПОЛЕЗНЫЕ СОВЕТЫ ПО ПРОВЕДЕНИЮ СЕМИНАРА

Этот раздел содержит полезные советы по проведению деловой игры DR/BCP. Если у вас есть идеи о том, как улучшить TTX, отправьте их TLD-OPS по электронной почте.

- Невозможно справиться с задачей составления списка заинтересованных сторон, угроз и рисков в одиночку. Постоянно подчеркивайте это.
- Некоторые угрозы являются «пугающими», но это служит еще более убедительным основанием для того, чтобы задокументировать их и составить план противодействия.
- В рамках отдельной деловой игры определите, какие функциональные подразделения/группы/люди в каждом TLD реально выступают в качестве менеджеров по BCP; определите их фактические заинтересованные стороны.
- Некоторые могут бороться с финансовыми последствиями — в этом помогает участие деловых людей; обеспечение бесперебойной деятельности — коллективная задача.
- Выясните в своей организации, кто выполняет роль менеджера по BCP: юрист, PMO, финансовый директор, CIO, CSO, генеральный директор, COO?
- Можно начать деловую игру, раздав каждой группе следующие 3 карты.