ПЛАНИРОВАНИЕ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА И ВОССТАНОВЛЕНИЯ

***Дорофеев Александр Владимирович**, CISSP, CISM, CISA, г. Москва*
***Марков Алексей Сергеевич**, доктор технических наук, старший научный сотрудник, CISSP, SBCI, г. Москва*

Публикация продолжает серию статей по подготовке к сдаче экзамена на статус сертифицированного специалиста по информационной безопасности (Certified Information Systems Security Professional) [1–8]. Рассмотрены вопросы управления непрерывностью деятельности организации и восстановления ее деятельности после инцидентов безопасности. Дан сравнительный анализ операций планирования непрерывности бизнеса и планирования восстановления бизнеса. Рассмотрены основные процедуры непрерывности бизнеса в контексте процессной модели менеджмента. Перечислены подходы, методы и стандарты бесперебойной работы информационных систем. Рассмотрены основные стратегии и техники резервирования и аварийного восстановления ресурсов. Приведены показатели готовности и надежности информационных систем в контексте менеджмента непрерывности бизнеса. Приведена классификация способов тестирования планов обеспечения непрерывности бизнеса и аварийного восстановления после бедствий. Даны рекомендации по успешной сдаче экзамена CISSP.

***Ключевые слова**: информационная безопасность, управление непрерывностью бизнеса, планирование непрерывности бизнеса, планирование восстановления бизнеса, кризисный менеджмент, прерывание бизнеса, сертификация специалистов, CISSP.*

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

***Aleksandr Dorofeev**, CISSP, CISM, CISA, Moscow*
***Alexey Markov**, Doctor of Sciences, Associate Professor, CISSP, SBCI, Moscow*

This publication continues our series of articles for information security specialists, preparing to take an exam for Certified Information Systems Security Professional certification. The questions of a business continuity management and recovering after security incidents are considered. A comparative analysis of the operations of business continuity planning and disaster recovery planning are given. The basic procedures of business continuity planning in the context of a management model are defined. The approaches, methods and standards for the uninterrupted operation of information systems are briefly presented. The basic strategies and technologies for backup and recovery are considered. The availability and reliability indicators of information systems in the context of business continuity management are analyzed. A classification of testing methods of continuity plans and recovery are reviewed. The recommendations for a successful exam CISSP are given.

***Keywords**: information security, BCM, BCP, DRP, crisis management, disruption, experts certification, CISSP, certified information systems security professional, ISC2.*

Введение

Одним из самых важных положений курса CISSP (Certified Information Systems Security Professional) является тема планирования непрерывности бизнеса и планирования восстановления после инцидентов безопасности. В новой версии экзамена CISSP данная тема представляет отдельный раздел домена по управлению рисками информационной безопасности (Security and Risk Management) [9]. В данной статье мы постараемся разобраться в основных понятиях, которые необходимо знать для того, чтобы успешно сдать экзамен.

Управление непрерывностью бизнеса

В любой социальной сфере (к которой относится и область информационной безопасности) инциденты безопасности, прерывания работы (disruptive events) и аварии (disasters) неизбежны. Однако их воздействие на деятельность компании должно быть минимизировано: данные должны быть сохранены, технические средства находится в рабочем состоянии, репутация спасена, люди – вне опасности. Решения указанных задач возможно осуществить в рамках управления непрерывностью бизнеса (Business Continuity Management,

Рис. 1. *Примеры BCP и DRP*

BCM). Исторически выделяют две составные части менеджмента непрерывности бизнеса:

- планирование непрерывности бизнеса (Business Continuity Planning, BCP);
- планирование аварийного восстановления (Disaster Recovery Planning, DRP).

В первом случае основной целью планирования является обеспечение выполнения бизнес-задач хотя бы в минимально допустимом объеме. Во втором случае основное внимание обращено на подготовку организации к скорейшему полному восстановлению ее деятельности в случае аварии, ЧП, бедствия, кризисной ситуации и т.п. Общую идею указанных целевых отличий можно проиллюстрировать с помощью рисунка 1.

Однако различие между BCP и DRP состоит не только в этапе и «масштабе бедствия», но и в уровне планирования, например: BCP является прерогативой топ-менеджмента и соотносится больше с операционной безопасностью, а DRP тесно касается решения технических задач по резервированию и восстановлению данных и систем (табл. 1).

Модель менеджмента непрерывности бизнеса

Несмотря на различие, BCP и DRP являются неотъемлемыми частями менеджмента непрерывности бизнеса и процедурно пересекаются. В этом плане удобно их рассмотреть с помощью модели менеджмента PDCA (Plan-Do-Check-Act) [2, 3], например:

1. На этапе планирования (Plan) могут решаться следующие задачи:
- подготовка планирования;
- оценка влияния прерываний на бизнес;
- определение стратегий обеспечения непрерывности бизнеса;
- разработка документации;
- определение необходимости внедрения контролей (мер и средств защиты) для минимизации выявленных рисков;

2. На этапе исполнения (Do):
- внедрение разработанных документов и необходимых технических решений;
- обучение персонала;

3. На этапе проверки (Check):
- тестирование разработанных планов;

4. На этапе действия/исправления (Act):
- исправление выявленных в ходе тестирования проблем;
- совершенствование системы.

Рассмотрим некоторые важные, на наш взгляд, процедуры.

Подготовка планирования непрерывной работы

Подготовка планирования начинается с одобрения работ руководством и включает в общем случае решение ряда задач:

- уточнение целей и задач непрерывности бизнеса;

Таблица 1.
Отличия BCP и DRP

Характеристика	BCP	DRP
Сфера ответственности	CEO	CIO
Предмет деятельности	Предупреждение проблем	Решение проблем
Целевая задача	Функционирование основных бизнес-процессов	Сокращение времени восстановления
Событие	Прерывание бизнес-процесса	Авария
Объект	Бизнес-процесс	Информационный ресурс, технические системы, инфраструктура

- определение области (границ и уровня детализации);

- определение задействованных лиц и формирование групп планирования;

- предварительную оценку ресурсов;

- определение этапов, временных рамок, отчетных материалов.

Что касается границ планирования, то здесь речь больше идет о физических границах, например, какой офис международной компании попадает в границы системы. Что касается подразделений и бизнес-процессов, то здесь целесообразен их полный предварительный анализ с целью выделения критичных с точки зрения непрерывности бизнеса.

При формировании группы планирования, кроме компетенции специалистов, важно обеспечить баланс интересов различных сторон. Обычно в группу включают представителей руководства, ИТ-отделов, службы информационной безопасности (ИБ), службы охраны, юридической службы, руководства и других заинтересованных подразделений. Допускается создание различных групп по целевым задачам, например: команда восстановления помещений (Facility Recovery Team), команда восстановления сетевой инфраструктуры (Network Recovery Team), команда восстановления бизнес-приложений (Application Recovery Team), которые могут быть замкнуты на команду управления (Crisis Management Team). Различные дополнительные функции в случае кризисной ситуации могут быть определены и для отдела кадров, PR-отдела и т.п.

В рамках определения задействованных лиц важно запротоколировать четкие роли, обязанности, конкретных ответственных (кого следует наказать в случае чего).

При оценке ресурсов следует предварительно предусмотреть потребности всего цикла непрерывности бизнеса, как-то: разработки, тестирования, обучения, сопровождения, собственно прерывания бизнеса.

Оценка влияния прерываний на бизнес

Оценка влияния прерываний на бизнес (Business Impact Analysis, BIA) является ключевой темой непрерывности бизнеса и состоит в функциональном анализе того, как прерывания повлияют на деятельность организации.

К задачам BIA относят:

- определение ценности каждого бизнес-процесса;

- идентификацию и ранжирование прерываний каждого бизнес-процесса;

- приоритизацию бизнес-процессов;

- оценку ресурсов на обеспечение непрерывности бизнес-процессов.

Итоговым результатом BIA является выбор стратегий управления непрерывностью бизнеса.

Можно прокомментировать, что при анализе прерываний конкретных бизнес-процессов обычно используются различные сценарии развития кризисной ситуации, в том числе фиксируют скорость распространения и длительность прерывания.

При определении ценности бизнес-процессов для информационных систем могут быть зафиксированы значения ряда технических показателей:

- MTPD (Maximum Tolerable Period of Disruption, максимально приемлемый период прерывания бизнеса) – период времени, по истечении которого неблагоприятные последствия, возникшие в результате прерывания бизнеса, становятся неприемлемыми;

- RTO (Recovery Time Objective, целевое время восстановления) – период времени после произошедшего прерывания, в течение которого должен быть восстановлен минимальный уровень деятельности организации, а также поддерживающие его системы, прикладные программы и функции;

- RPO (Recovery Point Objective, целевая точка восстановления) – период времени, за которое должны быть восстановлены данные после прошедшего прерывания.

Полагается, что: RTO < MTPD.

В литературе можно встретить другие показатели, например:

- MAO (Maximum Acceptable Outage), MAD (Maximum Allowable Downtime), MTD (Maximum Tolerable Downtime) - допустимое время простоя, применяемое в области непрерывности бизнеса в качестве синонима MTPD.

- MDL (Maximum Data Loss) - в качестве синонима RPO.

Можно показать, что указанные показатели будут влиять на выбор решений по восстановлению бизнес-процессов или данных. Например, если RTO = 8 час, то, скорее всего, ИТ-специалисты успеют полностью переустановить, например, системное ПО и восстановить данные из резервных копий, если RTO составляет 5 минут, то здесь речь уже будет идти о параллельно работающих элементах системы с дублированием данных.

Кроме технических характеристик в рамках BIA имеет место задание ограничений по стоимости, репетиционных критериев, показателей выполнения требований регуляторов.

Надо понимать различие между BIA и оценкой риска (risk assessment) ИБ [2]. Несмотря на общность подходов, BIA лежит в области менеджмента организаций и, опираясь на приоритизацию бизнес-процессов, позволяет в конечном счете выработать

стратегии менеджмента непрерывности бизнеса. Оценку риска ИБ относят к области технической защиты информации, в ее основе лежит определение стоимости активов и, главное, идентификация угроз и уязвимостей их касающихся, что позволяет выработать (на основе оцененных рисков ИБ) меры защиты от угроз конкретным активам. Таким образом, оценка риска ИБ может являться уточняющей процедурой управления безопасностью информационных систем и отталкиваться от результатов BIA.

Определение стратегий обеспечения непрерывности бизнеса

После того как мы разобрались, что угрожает критичным бизнес-процессам организации, необходимо определит как будет обеспечиваться непрерывность бизнеса. В CISSP подчеркивается, что основным приоритетом безопасности работы организации являются люди, т.е. должны быть инструкции, направленные на обеспечение здоровья до, во время и после прерывания бизнеса.

Относительно защиты активов, предусматривается две концепции:

- усиление за счет использования различных защитных мер и средств;
- дублирование.

В качестве дублирования информационной системы используется концепция альтернативных площадок, к которым относят, главным образом, следующие:

- площадка в горячем резерве (Hot Site), когда альтернативная площадка максимально соответствует реальной (т.е. обеспечивается режим готовности 24/7);
- площадка в теплом резерве (Warm Site), когда на альтернативной площадке развернут прототип реальной компьютерной системы, например, в наличии все коммуникации и базовые устройства, однако информационные базы не актуализированы, отдельные настройки и обновления не произведены и т.п.;
- площадка в холодном резерве (Cold Side) – как правило, это лишь помещение;

Надо понимать, что, кроме увеличения затрат при снижении времени аварийного восстановления, наиболее актуализированные площадки требуют обеспечения и соответствующего уровня безопасности.

В качестве особых мер защиты еще выделяют:

- «джентльменское» соглашение о взаимопомощи с другими организациями (reciprocal or mutual aide agreement);
- аутсорсинг - на договорной основе использование подрядчиков (service bureaus).

В качестве стратегий актуализации данных с альтернативными площадками можно назвать следующие:

- копирование резервных данных (electronic vaulting, off-site data protection) - периодическая передача копий баз данных на альтернативные носители, обычно в пакетном режиме;
- удаленное журналирование (remote journaling) - периодическая передача журнала выполненных транзакций с основной площадки на альтернативную;
- удаленное зеркалирование (remote mirroring) - полное дублирование в реальном времени.

Известно несколько схем резервного копирования, например:

- полное копирование (full backup), когда копируются все файлы или блоки;
- инкрементальное или добавочное копирование (incremental backup), когда копируются только измененные файлы или блоки после последнего (инкрементального или полного) копирования;
- дифференциальное копирование (differential backup), когда копируются все измененные файлы или блоки с момента последнего полного копирования.

Разработка организационно-распорядительной документации

Основу создания любой системы менеджмента является документирование. На рис. 2 представлен возможный вариант структуры организационно-распорядительных документов в области непрерывности бизнеса. Перечислим их.

Таблица 2.

Отличия альтернативных площадок

Тип площадки	Уровень RTO	Актуализированность активов		
		БД	ПО, ТС	Помещение
Hot site	Реальное время, час	+	+	+
Warm site	День	-	+	+
Cold site	Неделя, месяц	-	-	+

Как видно из рисунка 2, самым высокоуровневым документом является Политика обеспечения непрерывности бизнеса (Business continuity policy statement), которая содержит основные цели, задачи и принципы в области обеспечения непрерывности бизнеса. Иногда в качестве приложения к Политике безопасности создают документ Стратегия обеспечения непрерывности бизнеса (Business continuity strategy). Следует заметить, что вся деятельность по управлению непрерывности бизнеса начинается с одобрения руководством путем утверждения указанной политики.

План обеспечения непрерывности бизнеса (Business continuity plan) - общий план, описывающий систему менеджмента обеспечения непрерывности бизнеса. Зачастую является неким подобием руководства по качеству только для рассматриваемых нами целей.

План обеспечения непрерывности бизнеса подразделения (Business unit continuity plan) - план действий сотрудников определенного подразделения в кризисной ситуации.

Процедуры по обеспечению непрерывности бизнеса подразделения (Business unit continuity procedures) - описание конкретных процедур подразделения, которые в случае необходимости можно вынести их из плана подразделения (например, PR-подразделению в кризисной ситуации необходимы отдельные процедуры для организации внутренних и внешних коммуникаций).

План восстановления ИТ-системы после сбоев (IT disaster recovery plan) – план восстановления информационных систем и ИТ-инфраструктуры предприятия. Ключевыми составляющими плана являются описание зависимостей систем и последовательности их восстановления.

Процедуры команд восстановления (Emergency team procedures) – процедуры команд восстановления.

Тестирование планов

После внедрения разработанных документов и соответствующего обучения персонала наступает самый занимательный момент – тестирование разработанных планов и процедур. Как правило, на этом этапе выявляются серьезные недостатки планирования, что в свою очередь ведет к их доработке на фазе Act цикла PDCA.

Есть специфические подходы к тестированию, в которых соискателю статуса CISSP необходимо хорошо ориентироваться:

- опрос (checklist test) - проводится методом анкетирования подразделений;

- проход по плану (structured walk-through) - пошаговое «активное» чтение планов всей группой восстановления, выполнение «понарошку» с целью выработки решения об эффективности его положений;

- моделирование (simulation test) - моделирование «виртуального» прерывания каких-либо процессов или сбоя каких-либо компонент системы с целью отработки методов предупреждения и восстановления;

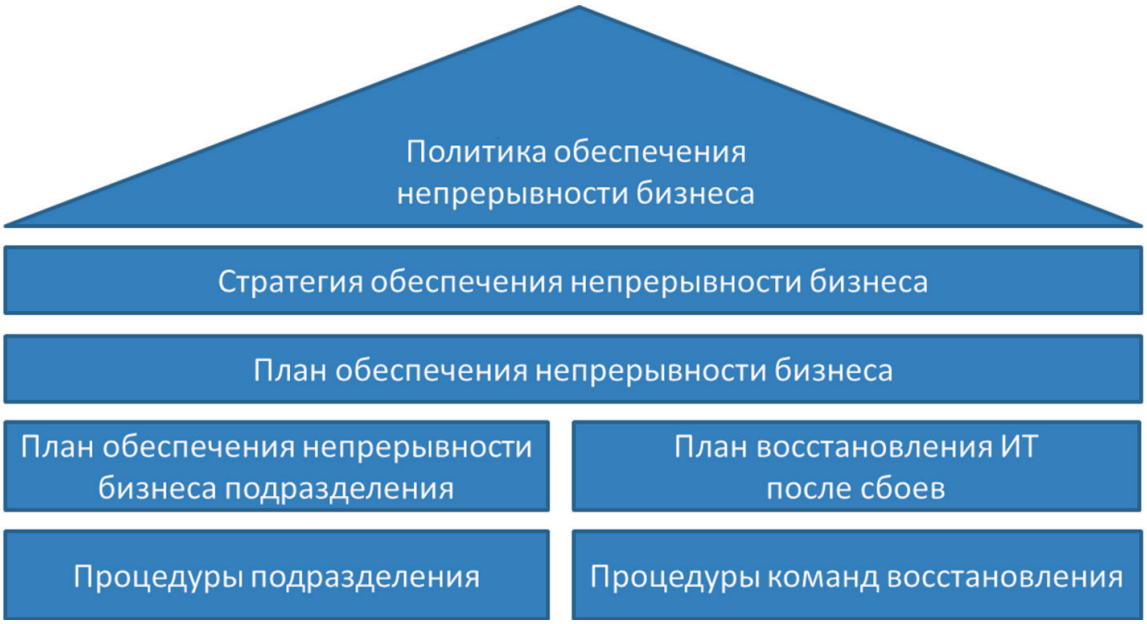

***Рис. 2**. Пример организационно-распорядительных документов ВСМ*

- параллельное тестирование (parallel test) - выполняется на альтернативной площадке и включает в себя выполнение всего плана тестирования с целью проверки эффективности функционирования альтернативной площадки;

- тестирование на реальном объекте (interruption test) - остановка работы системы и выполнение комплекса работ по ее восстановлению.

Заключение

Соискатель статуса CISSP должен хорошо ориентироваться в рассмотренных аспектах внедрения процессов обеспечения непрерывности бизнеса и восстановления, в том числе владеть довольно специфической терминологией. Для более глубокого погружения в данную тему авторы рекомендуют ознакомиться со стандартами и методическими документами в данной области.

Следует указать, что в области непрерывности бизнеса наиболее известны следующие международные стандарты:

- ISO 22301:2012 Societal security - Business continuity management systems – Requirements;

- ISO/IEC 27031:2011 IT - Security techniques - Guidelines for information and communication technology readiness for business continuity.

В США популярным остается NIST Special Publication 800-34 Contingency Planning Guide for Federal Information Systems (Rev.1, 2010).

Что касается России, то у нас приняты международные стандарты ГОСТ Р ИСО/МЭК 27031-2012 (ИТ. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса) и ГОСТ Р ИСО 22301-2014 (Системы менеджмента непрерывности бизнеса. Общие требования), а также серия национальных стандартов ГОСТ Р 53647 (Менеджмент непрерывности бизнеса), релевантной утратившему силу BS 25999.

Относительно методических документов можно рекомендовать материалы, доступные на сайтах ведущих институтов по данной тематике, к коим следует отнести Business Continuity Institute (BCI) и Disaster Recovery Institute International (DRII). Здесь, например, можно рекомендовать Good Practice Guidelines от BCI [4].

Кроме рассмотренных методических вопросов данной темы, соискателю статуса CISSP желательно иметь практику работы со средствами резервного копирования и восстановления, с отказоустойчивыми системами хранения (в первую очередь, RAID-массивами) и с кластерными отказоустойчивыми решениями.

За рамками статьи остались атаки на отказ в обслуживании, однако, подробно рассматриваемые в разделе по сетевой безопасности, а также полуколичественные методики оценки риска, ранее изученные нами в рамках темы менеджмента ИБ [2].

Литература:

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67-73.
3. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С.66-73.
4. Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С.69-73.
5. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4(7). С. 69-74.
6. Барабанов А.В. Подготовка к сдаче CISSP: модели информационной безопасности // Вопросы кибербезопасности. 2014. № 5(8). С. 59-67.
7. Марков А.С., Цирлов В.Л. Основы криптографии: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 1 (9). С. 65-73.
8. Марков А.С., Цирлов В.Л. Безопасность доступа: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 2 (10). С. 60-68.
9. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 7th Edition. - Sybex, 2015. 1104 p.
10. Good Practice Guidelines 2013 Global Edition. A Guide to Global Good Practice in Business Continuity / by ed. L.Bird. BCI. 2013. 116 p.