УДК 004.056 + 338.2

Оладько Владлена Сергеевна
к.т.н., доцент
Волгоградский государственный университет
г. Волгоград, Российская Федерация
Микова Софья Юрьевна
студент 4 курса
Волгоградский государственный университет
г. Волгоград, Российская Федерация

Oladko V. S.
Ph.D., Associate Professor, Volgograd State University
Volgograd, Russian Federation
Mikova S. Y.
4th year student, Volgograd State University
Volgograd, Russian Federation

СТРАТЕГИИ И ПОКАЗАТЕЛИ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА

STRATEGIES AND INDICATORS OF BUSINESS CONTINUITY

Аннотация. *Исследована проблема обеспечения непрерывности бизнеса на предприятии. Выделены две основные стратегии обеспечения непрерывности бизнеса и решения реализующие их. Описаны показатели оценки непрерывности бизнеса. Проведен анализ влияния выбранных стратегий и решений по обеспечению непрерывности бизнеса на значения показателей непрерывности.*

Ключевые слова: *информационная безопасность, непрерывность деятельности, резервирование, информационная система, восстановление, бизнес-процесс.*

Summary. *The problems of ensuring business continuity in the enterprise are investigated. Two main strategies and solutions to ensure business continuity identified. Indicators of business continuity assessment identified. Influence of selected strategies and solutions to value business continuity indicators analyzed.*

Keywords: *information security, business continuity, backup, information system, recovery, business process.*

В настоящее время практически каждое предприятие для реализации своих бизнес-процессов использует информационную инфраструктуру и корпоративные информационные системы (ИС). Данные системы позволяют автоматизировать бизнес-процессы и осуществлять обработку, хранение и передачу больших объемов данных необходимых для деятельности предприятия. Следовательно, от надежности и безопасности функционирования информационной инфраструктуры будет напрямую зависеть непрерывность бизнес-процессов, доступность и целостность данных, а значит и деятельность всего предприятия в целом.

Анализ нормативно-методической документации показывает, что стратегию обеспечения непрерывности деятельности предприятия можно разделить на две составляющие:

1) планирование непрерывности бизнеса (ПНД) — обеспечение выполнения бизнес-процессов и поддержки их непрерывного и согласованного взаимодействия, для реализации целей деятельности предприятия в допустимом объеме при любых деструктивных воздействия угроз;

2) планирование аварийного восстановления (ПАВ) — подготовка предприятия к скорейшему восстановлению ее деятельности в условиях деструктивного воздействия угроз.

А так как непрерывность деятельности предприятия напрямую зависит от непрерывности

функционирования ИС, то в первую очередь при реализации стратегии и цикла управления непрерывностью необходимо обеспечить решение следующих задач:

1) надежности и устойчивости функционирования ИС в условиях атак злоумышленника и других деструктивных воздействий случайного и умышленного характера, за счет введения планов обеспечения непрерывности деятельности, резервирования, избыточности и превентивных мер противодействия возможным угрозам;

2) быстрого восстановления работоспособности ИС и/или ее подсистем в случае отказа, с минимально допустимым объемом потерь данных и временем простоя сервисов ИС.

Анализ [1–5] показывает, что для решения первой задачи используются организационные, технические и программно-аппаратные решения:

1) план обеспечения непрерывности деятельности в условиях воздействия угроз и дестабилизирующих факторов различной природы;

2) план и методика поведения персонала, в случае возникновения инцидента нарушающего непрерывность деятельности;

3) резервирование и дублирование критичных данных и подсистем ИС;

4) аппаратная и программная избыточность;

5) создание локальной или удаленной альтернативной площадки:

- площадка в горячем резерве — в этом случае альтернативная площадка максимально советует реальной, что позволяет обеспечить режим готовности 24/7;
- площадка в теплом резерве — развернут прототип реальной ИС, например в наличие все коммуникационные и программно-аппаратные средства ИС, но информация в базах данных не актуализирована, отдельные конфигурационные настройки и обновления ПО не сделаны (среднее время приведения в состояние полной готовности — день);
- площадка в холодном резерве — как правило, лишь помещение, среднее время приведения в состояние готовности от недели до месяца.

6) площадки динамического распределения нагрузки на сеть и сервера ИС;

7) применение систем обнаружения и предотвращения вторжений;

8) применение средств защиты информации;

9) обслуживание и контроль над работоспособностью и надежностью технических средств обработки и передачи данных в ИС;

10) мониторинг состояния ИС;

11) создание кластеров;

12) виртуализация серверов;

13) облачные решения;

14) аренда сторонних резервных центров хранения и обработки данных;

15) аутсорсинг и соглашения;

16) ситуационные центры чрезвычайных ситуаций и обеспечения непрерывности бизнеса (BI-системы).

Для решения второй задачи используются следующие механизмы и средства:

1) разработка плана восстановления деятельности с учетом имеющихся средств и мощностей;

2) тестирование разработанных планов, методик и процедур:

- опрос с помощью анкетирования персонала и пользователей ИС;
- проход по плану, заключается в пошаговом чтении планов группой, ответственной за восстановление функционирования ИС и деятельности, выработке решения об эффективности положений и необходимости их коррекции и доработки;
- моделирование «виртуальных» прерываний и отказов ИС с целью отработки методов предупреждения и восстановления.

3) непосредственное восстановление работоспособности поврежденных и отказавших служб, процессов и подсистем ИС.

Указанные выше решения имеют свою стоимость, совместимость, сложность реализации, время развёртывания и эффективность. Могут применяться как по отдельности, так и в виде комплекса мер, реализуемых до, во время и/или после инцидента, вызвавшего нарушения непрерывности функционирования ИС и деятельности предприятия.

Таким образом, в случае возникновения инцидента в соответствии с [1–3] ключевое значение будут иметь следующие показатели непрерывности, связь между которыми представлена на рис. 1:

- максимально допустимое время простоя (Maximum Allowable Outage, MAO) — период времени, по истечении которого существует риск окончательного прекращения деятельности предприятия, в случае, если предоставление сервисов, данных, бизнес-процессов и/или услуг не будут возобновлены.
- текущее время простоя (TOF) — период времени, в течение которого деятельность была прервана в результате отказа ИС или ее компонентов, недоступности сервисов и данных, в приемлемом для предприятия случае должна быть меньше максимально допустимого времени простоя *TOFMAO*;
- целевое время восстановления (Recovery Time Objective, RTO) — время, в течение которого, долж-

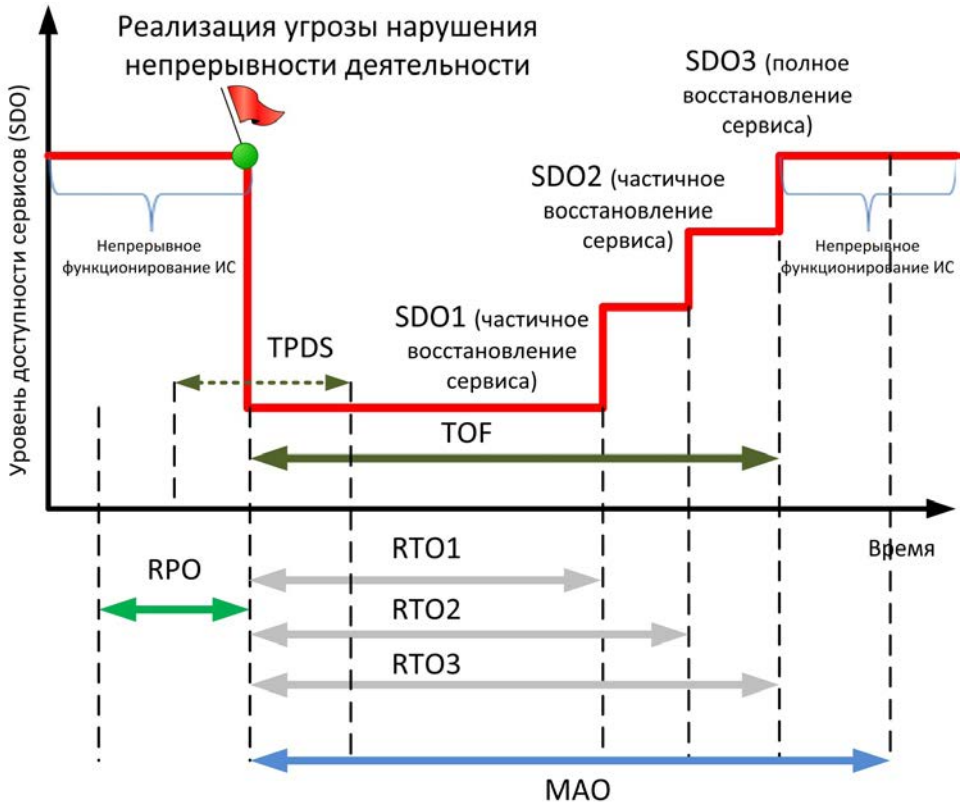

Рис. 1. Определение показателей непрерывности деятельности

но происходить восстановление бизнес-процесса, данных или ресурса при наступлении угрозы, вызвавшей нарушение непрерывности функционирования ИС;

– целевая точка восстановления (Recovery Point Objective, RPO) — определяет объем допустимых потерь данных в случае прерывания операций (например, если RPO составляет 20 минут, то допускается потеря данных за последние 20 минут);
– целевая доступность сервиса (Service Delivery Objective, SDO) — показывает уровень доступности сервиса в определенный момент времени;
– время планирования и развёртывание решений обеспечения и восстановления непрерывности деятельности (TPDS), в идеальном случае решения и планы должны быть разработаны и внедрены до наступления инцидента нарушения непрерывности, *TPDS*.

Таким образом, для того что уменьшить время текущего простоя TOF необходимо решать первую и вторую задачи совместно и внедрять превентивные меры, применение которых еще до реализации угрозы нарушения непрерывности позволит не только минимизировать потери данных и сократить целевое время восстановления, но уменьшить общий уровень риска. Подобный эффект достигается за счет того, что планы и средства обеспечения непрерывности деятельности разрабатываются и развёртываются не во время отказа, а в период штатного функционирования ИС до реализации угрозы и возникновения лавинного эффекта. Это позволяет сразу после наступления инцидента скоординировать действия персонала и начать восстановление или полностью избежать простоя и потерь за счет оперативного переключения на резервную площадку (см. рис. 2).

Таким образом, что бы успешно решать задачи обеспечения непрерывности деятельности необходимо реализовать и внедрить на предприятии весь процесс управления непрерывностью деятельности в соответствии с требованиями нормативно-методической документации.

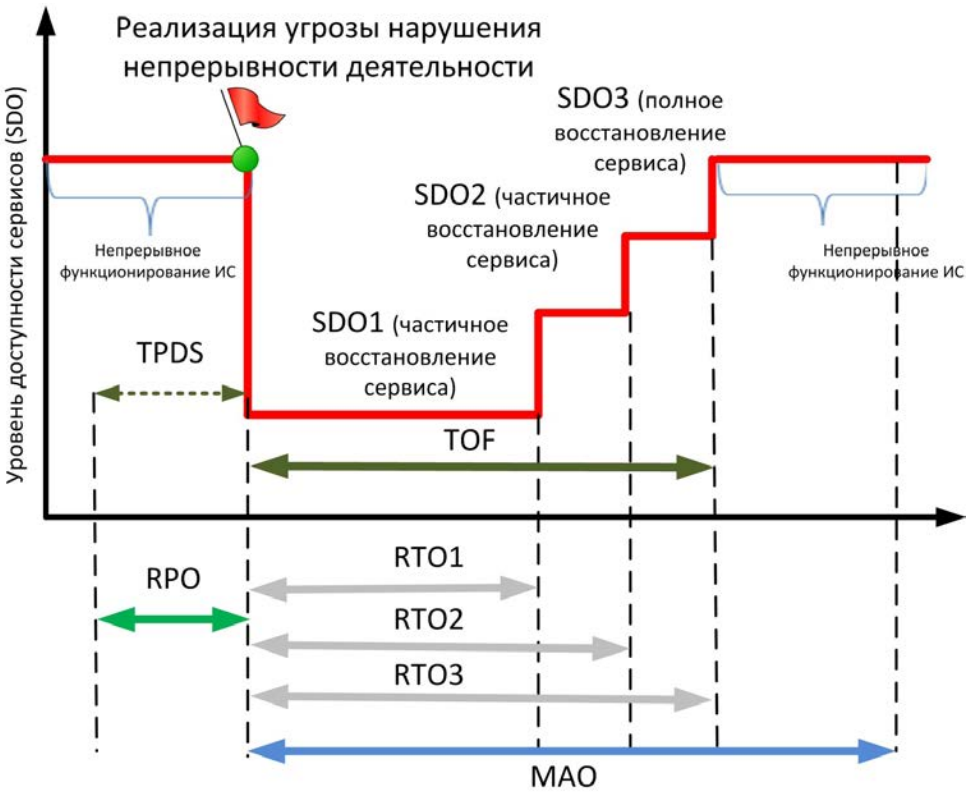

Рис. 2. Снижение времени восстановления функционирования ИС (TOF) за счет применения превентивных планов и мер защиты до наступления инцидента нарушения непрерывности деятельности

Литература

1. Дорофеев А. В., Марков А. С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. № 3(11). С. 68–73.

2. Стандарт АРБ. Система управления непрерывностью деятельности кредитных организаций Банковской системы Российской федерации. Версия 7–4, от 02.04.2012. URL:
http://arb.ru/site/docs/other/Kom32_StandProgUprNepr_2012-04-01.pdf (дата обращения 28.10.2015).

3. Аткина В. С. Разработка метода, алгоритмов и программы для анализа катастрофоустойчивости информационных систем // диссертация ... кандидата технических наук: 05.13.19 / Южный федеральный университет. Волгоград, 2013.

4. Башнин А. Ситуационное управление и непрерывность бизнеса. Часть 3: Ситуационные центры // Управление предприятием. 2015.№ 7(51). С. 2–9.

5. Аткина В. С. Система синтеза проектов рациональных катастрофоустойчивых решений для корпоративных информационных систем // Информационные системы и технологии. 2013. № 4(78). С. 122–130.