Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 10, Is. 4, pp. 152-157, 2016

DOI: 10.13187/vesp.2016.10.152
www.ejournal21.com

Modern security

UDC 004.056.53

The Business Continuity Management

Tatyana S. Ivanova [a, *], Natalya S. Ralnikova [a], Xenia A. Kudryavtseva [a]

[a] ITMO University, Russian Federation

Abstract

This article discusses the issue of business continuity management in general, and also from the point of view of information security. The ensuring of business continuity is an important component of a successful and productive activities in almost any modern organization. The work in this direction should be carried out in accordance with a set of national and foreign guidelines and practices.

As materials for the study there were used the international and Russian standards in the field of information security management and business continuity management in particular, as well as the latest works of specialists in this field. The main methods of the study were the methods of scientific cognition, methods of analysis and synthesis, logical methods.

Keywords: business continuity, business continuity management, information security management.

1. Введение

В современном мире в век информационных технологий, в условиях рыночной экономики и развивающейся конкуренции, эффективность работы систем обработки данных во многих видах бизнеса, таких как банковский, страховой, торговый бизнес тесно связана с обеспечением непрерывности поддерживаемых ими бизнес-процессов. Таким образом, необходимость доступности систем обеспечения непрерывного функционирования всех видов деятельности является одной из ключевых задач, стоящих перед руководством любой организации.

Каждая из них так или иначе сталкивалась с проблемами нарушения или прерывания деятельности – вследствие сбоев энергетики, поставок или функционирования информационных и телекоммуникационных систем, нарушений информационной безопасности (ИБ), недоступности офиса, ухода ключевого персонала, преднамеренных действий или ошибок персонала, а также пожаров, наводнений, техногенных катастроф и т.д. В следствии возникновения такого рода инцидентов, которые нарушают непрерывность

* Corresponding author
E-mail addresses: ivanova.tat.ser@gmail.com (T.S. Ivanova), natalya.ralnikova@gmail.com (N.S. Ralnikova), kudriavtseva.ksyu@yandex.ru (X.A. Kudryavtseva)

бизнеса, для организации могут наступить такие негативные последствия как снижение прибыли, дополнительные расходы, удар по репутации и даже полная ликвидация организации. А в высокотехнологичных отраслях, таких как, например, телекоммуникации, обеспечение непрерывности деятельности является не просто потребностью бизнеса, но и требованием на уровне законодательства. Временное не предоставление услуг вне зависимости от причин и факторов, вызвавших этот перерыв, в худшем случае может привести к отзыву лицензии и, как следствие, полному прекращению деятельности организации.

2. Материалы и методы

В качестве материалов для исследования использованы международные и российские стандарты в области управления информационной безопасностью и управления непрерывностью бизнеса в частности, а также последние работы специалистов в данной области.

Основными методами для исследования послужили методы научного познания, методы анализа и синтеза, логические приемы.

3. Обсуждение

Для начала необходимо определить, что понимается под непрерывностью бизнеса и под управлением непрерывности бизнеса.

Под непрерывностью бизнеса будем понимать способность организации планировать свою работу в случае возникновения инцидентов и нарушения ее деятельности, направленной на обеспечение непрерывности бизнес-процессов на должном уровне (Милославская и др., 2014).

Тогда управление непрерывностью бизнеса определим, как полный процесс управления, предполагающий определение потенциальных угроз и их воздействие на деятельность организации, и создающий основу для повышения устойчивости организации к инцидентам, и направленный на реализацию эффективных ответных мер против них, что обеспечивает защиту интересов организации, ее репутации и деятельности (Милославская и др., 2014).

Процесс управления непрерывностью деятельности направлен на решение вопросов, с которыми сталкивается любая организация, а именно:

- какова критичность того или иного риска прерывания бизнеса;
- каким образом избежать данного риска или свести к минимуму его негативные последствия;
- какие действия необходимо осуществить для профилактики;
- как найти эту грань между приемлемыми инвестициями в защитные меры и возможными потерями от реализации рисков.

Таким образом, процесс управления непрерывностью бизнеса можно представить состоящим из двух направлений:

1) обеспечение устойчивости бизнес-процессов к инцидентам;
2) восстановление бизнеса после инцидентов, что включает восстановление бизнес-процессов, операций и ресурсов, и организации в целом.

Задача управления непрерывностью бизнеса для первого направления состоит в минимизации вероятности наступления рискового события и проявляется в разработке и внедрении антикризисных мероприятий; во втором же направлении – в уменьшении и корректировке негативных последствий уже произошедшего инцидента.

В некоторых случаях государство устанавливает для организаций обязательные требования, связанные с обеспечением непрерывности бизнеса. И даже если применение требований законодательно не закреплено, использование международных и отечественных стандартов обуславливается облегчением построения процесса и повышением эффективности управления непрерывностью бизнеса. В настоящее время существует большое количество нормативных документов, которые регламентируют вопросы менеджмента непрерывности бизнеса.

Согласно ГОСТ Р ИСО/МЭК 27002-2012 (ГОСТ Р ИСО/МЭК 27002-2012) в организации должен быть разработан и поддерживаться в актуальном состоянии управляемый процесс

по обеспечению непрерывности бизнеса, который рассматривает требования защиты информации, необходимые для обеспечения непрерывности бизнеса организации.

При осуществлении работ по управлению непрерывностью бизнеса важным является идентификация активов, от которых зависит нормальное функционирование организации, а также определение условий, необходимых для продолжения деятельности и непрерывности выполнения организацией своих обязательств. Это позволяет организации получить представление о том, как и когда может произойти нарушение ее деятельности. Что, в свою очередь, дает возможность ещё до реализации самого инцидента определить необходимые в конкретной ситуации дополнительные возможности и ответные меры для защиты активов. В связи с этим в рамках общего процесса обеспечения непрерывности бизнеса организации важным является решение вопросов, связанных с обеспечением информационной безопасности, ключевыми среди которых являются следующие (ГОСТ Р 53131-2008):

- проведение анализа рисков ИБ, связанных с чрезвычайными ситуациями (ЧС);
- установление критериев оценки возможности перерастания инцидента ИБ в ЧС и планирование действий в данном случае;
- определение возможных сценариев реализации ЧС, связанных с ИБ, для которых будут разработаны соответствующие планы;
- выбор стратегии обеспечения ИБ в процессе ЧС;
- разработка, периодическое тестирование и обновление плана обеспечения непрерывности функционирования процессов обеспечения ИБ и соответствующих защитных мер и средств (или включение соответствующих разделов в уже имеющиеся планы в организации);
- разработка, периодическое тестирование и обновление плана восстановления работы защитных мер после ЧС (или включение соответствующих разделов в уже имеющиеся планы в организации).

Иными словами, те задачи обеспечения непрерывности бизнеса, что связанны с защитой информации, основываются на выявлении последовательности событий нарушения того или иного аспекта информационной безопасности, которые могут вызвать прерывания в деловых процессах организаций. В качестве примера можно привести следующие: сбои в работе оборудования, человеческий фактор, ошибки операторов, преднамеренные действия с целью нанесения вреда, кражи, возгорания, стихийные бедствия, техногенные катастрофы и акты терроризма.

После оценки рисков следует определить вероятность их реализации и влияние таких событий на работу организации с точки зрения временных рамок, масштаба наносимого ущерба и времени, которое потребуется для восстановления.

Для обеспечения полноты и точности оценка вышеописанных рисков проводится с максимально полным вовлечением владельцев используемых деловых ресурсов и процессов. При оценке рассматриваются все деловые процессы. Не должно быть ограничений средствами обработки информации, но должны включаться результаты, специфичные для защиты информации. Для того чтобы получить наиболее полную картину требований для обеспечения непрерывности, важно связать воедино различные аспекты рисков.

В результате оценки риски должны быть выявлены и количественно определены. А также каждому из них должны быть назначены приоритеты в соответствии с критериями и задачами, значимыми для организации, а именно: критические ресурсы, влияния нарушений, допустимые периоды простоя и приоритеты восстановления.

По итогам оценки рисков разрабатывается стратегия обеспечения непрерывности бизнеса, отправляется на подтверждение к руководству, после чего создается и реализуется план претворения в жизнь данной стратегии.

4. Результаты

Для успешного управления работой организации должна быть разработана система управления непрерывностью бизнеса.

Система управления непрерывностью бизнеса (СУНБ) - часть интегрированной системы управления организации, охватывающая создание, внедрение, функционирование,

мониторинг, анализ, поддержку и улучшение управления непрерывностью в организации (ГОСТ Р 53647.1-2009; ГОСТ Р 53647.2-2009).

Как любая другая система управления, СУНБ включает в себя следующие основные компоненты:

- структуру;
- политику;
- программу управления непрерывностью бизнеса;
- человеческие ресурсы;
- иные ресурсы организации, вовлеченные в процесс;
- процессы управления, касающиеся политик, планирования, внедрения и функционирования, оценки выполнения работ, анализа управления и улучшения;
- документацию, обеспечивающую свидетельства аудита действий в области обеспечения непрерывности бизнеса;
- общие и специальные процедуры и процессы, связанные с обеспечением непрерывности бизнеса, такие как анализ воздействия на бизнес и разработка плана обеспечения непрерывности бизнеса.

К СУНБ относятся и технические решения для непрерывности бизнеса, а именно:

1) резервные центры обработки данных;
2) системы обеспечения высокой доступности и виртуализации;
3) системы резервного копирования и репликации;
4) системы резервного электропитания;
5) системы охранно-пожарной сигнализации и автоматического пожаротушения;
6) прочие системы защиты деятельности от различного вида угроз.

Реальными примерами технической базы непрерывности бизнеса можно назвать информационно-телекоммуникационные системы высокой доступности, меры и механизмы обеспечения надежности, живучести, отказо- и катастрофоустойчивости информационных систем и т. д.

Обязательными для выполнения задачами в условиях существования СУНБ является не только обеспечение непрерывности бизнеса, но и разработка и поддержание системы управления инцидентами, а также планов по восстановлению ущерба после их реализации. При этом здесь важно то, что в каждой из задач обязательным является наличие аспекта защиты информации. Это необходимо для поддержания или восстановления операций и обеспечения доступности информации на необходимом уровне, выполнение которых следует за прерыванием критических бизнес-процессов.

При планировании непрерывности бизнеса необходимо выполнять следующие действия (ГОСТ Р ИСО/МЭК 27002-2012):

1) составить список всех операций, связанных с обеспечением непрерывности бизнеса;
2) определить приемлемую величину возможных потерь;
3) определить список процедур по восстановлению бизнеса;
4) составить соответствующую документацию;
5) довести до сведения персонала принятую документацию, провести обучение;
6) периодически проводить испытание имеющегося плана и по результатам вносить в него корректировки.

В связи с тем, что планы обеспечения непрерывности бизнеса должны учитывать организационные слабые места, они могут содержать критически важную информацию, которую необходимо должным образом защищать. Поэтому важно планы продублировать, копии должны храниться в отдаленном местоположении, на достаточном расстоянии для того, чтобы избежать любого ущерба в случае возникновения какого-либо бедствия на основном месте (ГОСТ Р ИСО 22313-2015).

Руководство должно обеспечить, обновление копий планов обеспечения непрерывности бизнеса были и их защиту на том же самом уровне, который применяется для документации на основном месте. Другие материалы, необходимые для реализации планов обеспечения непрерывности, также следует хранить в отдаленном местоположении.

5. Заключение

Обеспечение непрерывности бизнеса – важная составляющая успешной и продуктивной деятельности практически любой современной организации. Работа в этом направлении должна осуществляться в соответствии с набором отечественных и зарубежных инструкций и практик.

Важным является наличие и состав документации в области непрерывности бизнеса, в частности, должны быть разработаны и должным образом согласованы и утверждены политика управления непрерывностью бизнеса и планы управления инцидентами, обеспечения непрерывности и восстановления бизнеса. Эти планы должны регулярно испытываться и обновляться для обеспечения их актуальности и результативности.

Примечания

ГОСТ Р 53131-2008 – ГОСТ Р 53131-2008 Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен 18.12.2008.

ГОСТ Р 53647.1-2009 – ГОСТ Р 53647.1-2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство. Введен 15.12.2009.

ГОСТ Р 53647.2-2009 – ГОСТ Р 53647.2-2009 Менеджмент непрерывности бизнеса Часть 2. Требования. Введен 15.12.2009.

ГОСТ Р ИСО 22313-2015 – ГОСТ Р ИСО 22313-2015 Менеджмент непрерывности бизнеса. Руководство по внедрению. Введен 18.11.2015.

ГОСТ Р ИСО/МЭК 27002-2012 – ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Введен 24.09.2012.

Дорофеев, Марков, 2015 – *Дорофеев А.В., Марков А.С.* Планирование обеспечения непрерывности бизнеса и восстановления. // Вопросы кибербезопасности. 2015. №3. С. 68-73.

Международный стандарт ISO/IEC 27002-2005 – Международный стандарт ISO/IEC 27002-2005 Информационные технологии. Свод правил по управлению защитой информации. Введен 1.09.2008.

Милославская и др., 2014 – *Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. 2-е изд., испр. Москва: Горячая линия-Телеком, 2014. 170 с.

Мусатов – Мусатов К. Непрерывность бизнеса. Подходы и решения [Электронный ресурс]. Режим доступа: http://www.jetinfo.ru/stati/nepreryvnost-biznesa-podkhody-i, свободный.

Ярочкин, Бузанова, 2005 – *Ярочкин В.И., Бузанова Я.В.* Основы безопасности бизнеса и предпринимательства: Учеб. пособие. М.: Академический проект: Фонд "Мир", 2005. 241 с.

References

GOST P 53131-2008 – GOST P 53131-2008 Zashchita informatsii. Rekomendatsii po uslugam vosstanovleniya posle chrezvychainykh situatsii funktsii i mekhanizmov bezopasnosti informatsionnykh i telekommunikatsionnykh tekhnologii. Obshchie polozheniya. Vveden 18.12.2008.

GOST P 53647.1-2009 – GOST P 53647.1-2009 Menedzhment nepreryvnosti biznesa. Chast' 1. Prakticheskoe rukovodstvo. Vveden 15.12.2009.

GOST R 53647.2-2009 – GOST R 53647.2-2009 Menedzhment nepreryvnosti biznesa Chast' 2. Trebovaniya. Vveden 15.12.2009.

GOST R ISO 22313-2015 – GOST R ISO 22313-2015 Menedzhment nepreryvnosti biznesa. Rukovodstvo po vnedreniyu. Vveden 18.11.2015.

GOST R ISO/MEK 27002-2012 – GOST R ISO/MEK 27002-2012 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informatsionnoi bezopasnosti. Vveden 24.09.2012.

Dorofeev, Markov, 2015 – *Dorofeev A.V., Markov A.S.* (2015). Planirovanie obespecheniya nepreryvnosti biznesa i vosstanovleniya. Voprosy kiberbezopasnosti. №3. S. 68-73.

Mezhdunarodnyi standart ISO/IEC 27002-2005 – Mezhdunarodnyi standart ISO/IEC 27002-2005 Informatsionnye tekhnologii. Svod pravil po upravleniyu zashchitoi informatsii. – Vveden 1.09.2008.

Miloslavskaya i dr., 2014 – *Miloslavskaya N.G., Senatorov M.Yu., Tolstoi A.I.* (2014). Upravlenie intsidentami informatsionnoi bezopasnosti i nepreryvnost'yu biznesa. Uchebnoe posobie dlya vuzov. 2-e izd., ispr. Moskva: Goryachaya liniya-Telekom, 170 s.

Musatov – Musatov K. Nepreryvnost' biznesa. Podkhody i resheniya [Elektronnyi resurs]. Rezhim dostupa: http://www.jetinfo.ru/stati/nepreryvnost-biznesa-podkhody-i, svobodnyi.

Yarochkin, Buzanova, 2005 – Yarochkin V.I., Buzanova Ya.V. (2005). Osnovy bezopasnosti biznesa i predprinimatel'stva: Ucheb. posobie. M.: Akademicheskii proekt: Fond "Mir". 241 s.

УДК 004.056.53

Управление непрерывностью бизнеса

Татьяна Сергеевна Иванова [a, *], Наталья Сергеевна Ральникова [a],
Ксения Александровна Кудрявцева [a]

[a] Университет ИТМО, Российская Федерация

Аннотация. В данной статье рассматривается вопрос, связанный с управлением непрерывностью бизнеса в общем виде, а также с точки зрения информационной безопасности. Обеспечение непрерывности бизнеса – важная составляющая успешной и продуктивной деятельности практически любой современной организации. Работа в этом направлении должна осуществляться в соответствии с набором отечественных и зарубежных инструкций и практик.

В качестве материалов для исследования использованы международные и российские стандарты в области управления информационной безопасностью и управления непрерывностью бизнеса в частности, а также последние работы специалистов в данной области. Основными методами для исследования послужили методы научного познания, методы анализа и синтеза, логические приемы.

Ключевые слова: непрерывность бизнеса, управление непрерывностью бизнеса, управление информационной безопасностью.

* Корреспондирующий автор
Адреса электронной почты: ivanova.tat.ser@gmail.com (Т.С. Иванова), natalya.ralnikova@gmail.com (Н.С. Ральникова), kudriavtseva.ksyu@yandex.ru (К.А. Кудрявцева)