УДК 681.324-75

**Гордиенко С. Б.,** к.т.н.; **Положивцева С. С.,** магистрант
(Государственный университет телекоммуникаций. +380 (44) 249 25 22); gor-sb@ukr.net)

# РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

**Гордієнко С. Б., Положивцева С. С. Реагування на інциденти інформаційної безпеки в інфокомунікаційних системах.** В даній статті розглядаються актуальні питання управління інцидентами інформаційної безпеки, що дає організаціям інструменти управління та процедури, які дозволяють контролювати широкий діапазон інцидентів та вразливостей. Визначені пріоритетні принципи, яких необхідно дотримуватись при організації процесу реагування на інциденти. Визначені актуальні питання впровадження процедури управління безперервністю бізнесу на основі управління інформаційними інцидентами. Здійснено аргументацію питань сертифікації Системи управління безперервністю бізнесу, яка є частиною загальної системи управління організацією та забезпечує супровід і удосконалення процесів забезпечення безперервності бізнесу (діяльності) організації.

***Ключові слова:*** інформаційні технології, інформаційна безпека, управління інцидентами, безперервність бізнесу, сертифікація

**Гордиенко С. Б., Положивцева С. С. Реагирование на инциденты информационной безопасности в инфокоммуникационных системах.** В данной статье рассматриваются актуальные вопросы управления инцидентами информационной безопасности, которые дают организациям инструменты управления и процедуры, позволяющие контролировать широкий диапазон инцидентов и уязвимостей. Определены приоритетные принципы, которых необходимо придерживаться при организации процесса реагирования на инциденты. Определены актуальные вопросы внедрения процедуры управления непрерывностью бизнеса на основе управления информационными инцидентами. Осуществлена аргументация вопросов сертификации Системы управления непрерывностью бизнеса, которая является частью общей системы управления организацией и обеспечивает сопровождение и усовершенствование процессов обеспечения непрерывности бизнеса (деятельности) организации.

***Ключевые слова:*** информационные технологии, информационная безопасность, управление инцидентами, непрерывность бизнеса, сертификация

**Hordiyenko S. B., Polozhyvtceva S. S. Response to information security incidents within the infocomm systems.** This article deals with the matters of current interest related to information security incidents management, so providing the management tools and procedures for the entities that allow to exercise control over a wide range of security incidents and vulnerabilities. The priority principles to be followed when organizing the process of incident response were established. The current issues of implementing the business continuity management procedures based on the information management incidents were defined. It was carried out an argumentation of the matters related to certification of the business continuity management system which is an integral part of the overall entity management system providing the support and improvement of the business continuity processes (activities) of the entity.

***Keywords:*** information technologies, information security, incident management, business continuity, certification

**Вступление**

По мере расширения сферы использования информационных систем и их усложнения обостряется проблема обеспечения информационной безопасности (ИБ). Игнорирование проблем ИБ, практика "латания дыр" сегодня могут обойтись компании очень дорого. Вместе с тем, в большинстве компаний организационная составляющая системы ИБ проработана слабо.

Ещё одна острая проблема в сфере защиты данных связана с обеспечением непрерывности функционирования информационных систем.

Например, данные, как таковые, зачастую не классифицированы, то есть компания не имеет чёткого представления о том, какие у неё есть типы данных с позиций их конфиденциальности, критичности для бизнеса. А это влечёт за собой целый ряд проблем, начиная от сложностей в обосновании адекватности мероприятий по защите информации и заканчивая невозможностью при возникновении инцидента использовать правовые методы их расследования.

Для многих современных компаний, прежде всего, финансовых организаций, производственных холдингов, крупных дистрибьюторов бесперебойная работа информационных систем, поддерживающих основной бизнес, и доступность данных становятся критичным вопросом. Сбои в работе систем ведут к прерыванию бизнес-процессов и, соответственно, к недовольству клиентов, штрафам и другим потерям.

Решить эти вопросы можно путём построения эффективной системы управления информационной безопасностью. Нарушения в области информационной безопасности могут ставить под угрозу функционирование бизнес-систем и нарушать работу бизнеса.

Внедрение информационных технологий (ИТ) привело к тому, что существенно изменились подходы к организации современных экономических процессов. Несомненные преимущества, которые несут в себе ИТ, позволили не только вести бизнес более эффективно, но и автоматизировать функциональные процессы [1].

Однако активное применение информационных технологий обусловило риски, с которыми многие до этого не сталкивались и даже не знали об их существовании. С приходом высоких технологий в мир бизнеса одной из важнейших угроз является вмешательство киберпреступников в работу учреждений различной сферы деятельности.

Существует значительный перечень различных инцидентов информационной безопасности. Среди наиболее распространенных можно выделить следующие: DDoS-атаки (распространенные атаки типа "отказ обслуживания"), мошенничество в системах дистанционного обслуживания, взлом серверов и кража конфиденциальной информации, утечка важных корпоративных данных, атака на репутацию путем размещения клеветнической информации в Интернете. Каждый из этих инцидентов наложил негативный отпечаток на деятельность пострадавших компаний.

**Постановка задачи**

В связи с активизацией деятельности компьютерных преступников и прогнозируемым ростом количества внутренних и внешних инцидентов как в мире, так и в Украине перед службами информационной безопасности в организациях остро встаёт вопрос создания и последовательного применения правил реагирования на случаи нарушения ИБ.

От подготовленности, своевременности и эффективности реагирования на инциденты ИБ может зависеть, выльется ли инцидент в незначительное происшествие или станет катастрофой для бизнеса. Применение системы управления инцидентами ИБ даст организациям инструменты управления и процедуры, позволяющие контролировать широкий диапазон инцидентов и уязвимостей [2].

Негативные последствия широкого круга угроз ИБ (начиная от атак хакеров и заканчивая действиями инсайдеров, использующих свои знания и права доступа к данным компании для своей выгоды) можно уменьшить, используя подход к управлению инцидентами ИБ, описанный в новом международном стандарте ISO/IEC 27035:2011.

**Управление инцидентами в системе обеспечения ИБ**

Управление инцидентами – одна из важнейших процедур управления информационной безопасностью.

Основная задача процесса управления инцидентами ИБ – повышение уровня защищенности информационной системы компании, а также её информационных ресурсов.

Именно этот процесс позволяет понять недостатки процессов и контроля, получить исходные данные для разработки планов восстановления непрерывности бизнеса и определить ключевые роли персонала в случае возникновения нештатных ситуаций.

Таким образом, любой организации, серьезно относящейся к вопросам обеспечения информационной безопасности, необходимо реализовать комплексный подход к решению следующих задач:

– обнаружение, информирование и учет инцидентов информационной безопасности;

– реагирование на инциденты ИБ, включая применение необходимых средств для предотвращения, уменьшения и восстановления нанесенного ущерба;

– анализ произошедших инцидентов с целью планирования превентивных мер защиты и улучшения процесса обеспечения информационной безопасности в целом.

Прежде всего, важно правильно и своевременно устранить последствия инцидента, а также иметь возможность проконтролировать, какие действия были выполнены для этого.

Необходимо также расследовать инцидент, что включает определение причин его возникновения, виновных лиц и конкретных дисциплинарных взысканий.

Далее, как правило, следует выполнить оценку необходимости действий по устранению причин инцидента, если нужно – реализовать их, а также выполнить действия по предупреждению повторного возникновения инцидента.

Кроме этого, важно сохранять все данные об инцидентах ИБ, так как статистика инцидентов ИБ помогает осознавать их количество и характер, а также изменение во времени.

С помощью информации о статистике инцидентов можно определить наиболее актуальные угрозы для компании и, соответственно, максимально точно планировать мероприятия по повышению уровня защищенности информационной системы компании.

При организации процесса реагирования на инциденты в любой нештатной ситуации, в порядке приоритета, следует придерживаться следующих принципов:

1. Безопасность сотрудников и посетителей;
2. Сдерживание инцидента и минимизация ущерба;
3. Безопасность активов организации;
4. Безопасность информационных ресурсов;
5. Восстановление в соответствии с требованиями бизнеса;
6. Расследование инцидента;
7. Принятие мер по недопущению повторения инцидента.

Эти семь очевидных шагов – семь важных правил, которые нужно соблюдать, чтобы эффективно построить процессы управления инцидентами ИБ.

**Реагирование на инциденты**

Своевременное и эффективное реагирование на инциденты в системе безопасности является чрезвычайно важным для минимизации потенциального влияния таких инцидентов на репутацию организации.

Как правило, о возникновении инцидентов в системе информационной безопасности компании стараются не заявлять открыто, чтобы не дискредитировать себя и не давать дополнительное "оружие" конкурентам или криминальным структурам, которые в последнее время проявляют повышенный интерес к возможностям информационных технологий. В результате, хотя количество инцидентов ИБ постоянно растет, сведения о них, как правило, держатся в секрете, а мы узнаем лишь о тех немногочисленных инцидентах, информация о которых "просочилась" в прессу.

Оборотная сторона такой информационной непрозрачности – трудности при поиске специалистов, которые могли бы провести работы по расследованию инцидентов или выстраиванию в компании процесса реагирования на инциденты.

Первопричиной наступления события инцидента ИБ является потенциальная способность злоумышленника получить необоснованные привилегии для доступа к активу организации. Оценить риск подобной возможности и принять правильное решение о защите, составляет основную задачу команды реагирования [3].

Каждый риск должен быть приоритезирован и обработан в соответствии с политикой оценки рисков принятой в организации. Оценка рисков рассматривается как перманентный процесс, целью которого является достижение приемлемого уровня защиты, иными словами, должны быть внедрены достаточные меры защиты актива от необоснованного или неправомочного использования. Оценка рисков способствует классификации активов.

Критичные, с точки зрения рисков активы, в подавляющем большинстве случаев, также являются критичными для бизнеса организации.

**Реализация проекта управления непрерывностью бизнеса**

Процедура реагирования на инциденты информационной безопасности является одним из основных источников данных для анализа состояния внедрения процедур управления непрерывностью бизнеса на основе управления информационными инцидентами [3].

Управление непрерывностью бизнеса (Business Continuity Management – BCM) – это бизнес-процесс, отвечающий за управление рисками, которые могут серьезно повлиять на бизнес. BCM защищает интересы ключевых заинтересованных сторон, репутацию, бренд и деятельность по созданию ценности. Процесс BCM включает в себя снижение рисков до приемлемого уровня и планирование способов восстановления бизнес-процессов в случае нарушения бизнеса. BCM устанавливает цели, охват и требования по отношению к Управлению непрерывности ИТ-услуг.

Главным вопросом реализация проекта управления непрерывностью бизнеса есть План обеспечения непрерывности бизнеса (Business Continuity Plan – BCP), который состоит из Планов обеспечения непрерывности услуг и Планов восстановления услуг и определяет шаги, необходимые для восстановления бизнес-процессов в случае нарушения их функционирования.

План также должен содержать информацию о событиях, которые являются основанием для его инициирования; людях, которые должны быть задействованы в реализации плана; средствах коммуникаций и т.п. [1].

Управление непрерывностью услуг фокусируется на значимых негативных событиях, которые ITIL называет "катастрофами" для бизнеса. Менее значимые события рассматриваются в рамках процесса Управления инцидентами. То, является ли какое-то конкретное событие катастрофой, зависит от организации, в котором оно произошло. Размер и значимость негативного влияния события на бизнес, например, финансовые потери или потеря репутации, измеряется в рамках Анализа влияния на бизнес. Анализ влияния на бизнес определяет минимальные требования к критичности.

В рамках Управления непрерывностью услуг должны выполняться следующее основные действия:

1. Анализ влияния на бизнес для количественной оценки влияния потери услуги на бизнес;
2. Анализ рисков – идентификация и оценка рисков с целью определения потенциальных угроз непрерывности и оценки вероятности их осуществления;
3. Формирование Планов обеспечения непрерывности, интегрированных в планы BCM.
4. Тестирование планов обеспечения непрерывности;
5. Непрерывное осуществление планов и управление ими.

В мировой практике существуют компании которые проводят полный цикл работ по созданию систем управления непрерывностью бизнеса в соответствии с требованиями стандартов и действующего законодательства, включая их последующую сертификацию и регистрацию в авторитетных международных органах по сертификации систем менеджмента.

Система управления непрерывностью бизнеса (СУНБ) представляет собой часть общей системы управления организацией, обеспечивающая создание, внедрение, эксплуатацию, мониторинг, анализ, сопровождение и совершенствование процессов обеспечения непрерывности бизнеса (деятельности) организации. СУНБ включает в себя организационную структуру, политики, процессы планирования и управления, обязанности, процедуры и ресурсы.

Важнейшей составляющей современной СУНБ является система управления непрерывностью информационно-технологических сервисов (НИТС), представляющая собой

совокупность политик, стандартов, процессов и инструментов, с помощью которых компании не только улучшают свои возможности по реагированию на серьезные отказы систем, но и повышают способность к восстановлению после серьезных инцидентов таким образом, чтобы предотвратить отказ критически важных систем и сервисов. Управление НИТС направлено на обработку рисков, способных оказать внезапное серьезное воздействие, подвергая непрерывность бизнеса непосредственной угрозе [4].

Под сертификацией СУНБ организации по требованиям британского стандарта BS 25999-2:2007 понимается комплекс организационно-технических мероприятий, проводимых независимыми аккредитованными аудиторами, в результате которых, подтверждается наличие и надлежащее функционирование рекомендуемых Стандартом механизмов обеспечения непрерывности бизнеса, оценивается полнота и правильность их реализации, а также их адекватность потребностям организации и существующим рискам.

Сертификат соответствия BS 25999-2, выданный уполномоченным и авторитетным органом, является важным показателем надежности организации и высокой степени защищенности ее активов и бизнес-процессов в случае инцидентов и нарушений нормального хода деятельности.

Сертификация СУНБ по требованиям BS 25999-2, позволяет повысить степень привлекательности организации на внутреннем и внешнем рынках, способствует формированию благоприятного имиджа в глазах клиентов, партнеров, акционеров, аудиторов, государственных регулирующих органов, способствует расширению сферы деятельности организации на международном уровне. Наличие данного сертификата является серьезным конкурентным преимуществом при участии в тендерах, а также при принятии решения о выборе делового партнера, подрядчика, поставщика продуктов или услуг.

Процедура сертификации оказывает серьезное мотивирующее и мобилизующее воздействие на персонал компании: повышается уровень осведомленности сотрудников, эффективнее выявляются и устраняются недостатки и несоответствия, что способствует повышению стратегической и тактической способности организации планировать свои действия и реагировать на инциденты и нарушения нормального хода деятельности с целью продолжения бизнес операций на приемлемом уровне. Сертификация СУНБ является добровольной процедурой.

**Выводы**

В соответствии с положениями международного стандарта ISO/IEC 27001:2005, а также многих других стандартов, управление непрерывностью бизнеса и управление инцидентами являются одними из основных областей контроля и необходимой составляющей любой системы менеджмента информационной безопасности и, хотя эти области контроля выходят далеко за рамки вопросов информационной безопасности (ИБ является для них лишь одной из составляющих), выстраивать соответствующие процессы в организациях часто приходится именно специалистам по ИБ, порой значительно расширяя границы своей профессиональной компетенции и должностных полномочий.

В этом случае, информационная безопасность становится основным двигателем процессов обеспечения непрерывности бизнеса, формируя методологическую базу для оценки рисков и анализа воздействия на бизнес чрезвычайных ситуаций, управления инцидентами, разработки стратегии, политики и планов обеспечения непрерывности информационно-коммуникационных технологий и бизнеса в целом, разработки и поддержания в актуальном состоянии контакт-листов, аварийно-восстановительных процедур, реестров информационных и ИТ-активов и т.п.

Создаваемая таким образом система управления непрерывностью бизнеса становится производной от существующей системы управления информационной безопасностью организации, наследуя от последней соответствующие принципы управления и механизмы контроля.

Это, конечно, не означает, что ответственность за непрерывностью бизнеса и управление чрезвычайными ситуациями теперь возлагается на специалистов по информационной безопасности. Для этого требуется иной уровень компетенции и полномочий.

**Литература**

1. Гладиш С. В. Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування / С. В. Гладиш, В. Г. Кононович, М. Ф. Тардаскін // Зв'язок. – 2007. – № 8. – С. 28-31.

2. Гладиш С. В. Інтелектуальна система керування інцидентами інформаційної безпеки телекомунікаційних мереж / С. В. Гладиш // Матеріали міжнародної науково-практичної конференції «Інформаційні технології та інформаційна безпека в науці, техниці та освіті ІНФОТЕХ-2007». – Севастополь: СевНТУ, 2007. – С. 53-57.

3. Гладиш С. В. Реагування та обробка інцидентів інформаційної безпеки в мережі GSM / С. В. Гладиш // Вісник Державного університету інформаційно-комунікаційних технологій. – 2008. – Т. 6, № 1. – С.58-72.

4. Интегрированная система сбора информации об экстремальных состояниях телекоммуникационных сетей и их защиты [Коробко В. В., Скоропаденко А. П., Задоя Г. М., Вовк В. М.] // Зв'язок. – 2004. – № 1. – С. 39-45.

5. Сакович Л. М. Використання системи підтримки прийняття рішення під час експлуатації та ремонту засобів і комплексів зв'язку / Л. М. Сакович, В. І. Політов // Зв'язок. – 2000. – № 5. – С. 37-39.

6. Information technology. Security techniques. Information security incident management I // ISO/IEC TR 18044:2004.

7. Information technology. Security techniques. Information security management systems. Requirements // ISO/IEC 27001:2005.

8. Information technology. Security techniques. Code of practice for information security management // ISO/IEC 17799:2005.