Управление инцидентами информационной безопасности:

о чем говорят стандарты

Анна РЫЖЕНКОВА,
ведущий консультант-аналитик, ОАО «ЭЛВИС-ПЛЮС»

Управление инцидентами информационной безопасности (далее – инциденты) – тема далеко не новая, но по-прежнему не теряющая своей актуальности. Возникновение инцидентов – это те случаи, когда непременно вспоминают о существовании информационной безопасности (ИБ). А вот какими словами сопровождается данный процесс, зависит от используемого подхода к управлению инцидентами (реактивный или проактивный). Реактивный – всем хорошо известный метод «пока гром не грянет», с проактивным все гораздо сложнее. Применить его на практике удается далеко не всегда. Зачем делать что-то сейчас, если потом это может вообще не потребоваться? Тем не менее от возникновения инцидентов не застрахован никто. Риски, как бы мы их ни минимизировали, остаются всегда (не зря же введено такое понятие, как «остаточный риск», да и все случаи предусмотреть на 100% просто нереально). Изменение внешней и внутренней среды компании, развитие технологий – все это может привести к различным инцидентам. Как противостоять им и стоит ли изобретать что-то свое – личное дело каждого, но обратить внимание на накопленный опыт и имеющиеся разработки стоит в любом случае.

Выбор стандартов и руководств на тему управления инцидентами сейчас достаточно богатый. Вопросы управления инцидентами рассматриваются как в общих стандартах по управлению ИТ или ИБ (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 20000, COBIT5, ITIL), так и в специализированных стандартах и руководствах (ISO/IEC 27035, NIST 800-61) или отраслевых стандартах (PCI DSS, СТО БР ИББС) – и это только наиболее известные из них. Российские ГОСТы в данном случае не упоминаются умышленно: по сути, они представляют собой лишь перевод соответствующего международного стандарта, причем за то время, пока к выходу готовится ГОСТ, часто появляется уже обновленная версия международного стандарта, что вносит дополнительную путаницу.

Стандарты обычно носят рекомендательный характер, их требования становятся обязательными, если компания официально заявляет о приверженности идеям того или иного стандарта. Причем степень приверженности и корректности выполнения всех предписаний в этом случае обычно проверяется независимым контролирующим органом.

Помимо стандартов требования к наличию процесса управления инцидентами можно встретить в различных законах и положениях. Здесь о рекомендательном характере уже речь не идет, эти требования необходимо выполнять (конечно, если они применимы к той сфере деятельности, в которой работает компания). Так, например, в Федеральном законе от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ст. 16 п. 4) идет речь об обязанности обеспечить «своевременное обнаружение фактов несанкционированного доступа к информации», что является не чем иным, как частным случаем процесса управления инцидентами. Аналогичное требование

Таблица. Актуальные версии стандартов, затрагивающих вопросы управления инцидентами ИБ

	Стандарты		Руководства и рекомендации
	Международные	Российские	
Специализированные по инцидентам ИБ	*ISO/IEC TR 18044:2004*[1]	ГОСТ Р ИСО/МЭК ТО 18044-2007	NIST 800-61 Revision 2 (2012 г.)
	ISO/IEC 27035:2011	–	
Универсальные по тематике ИБ	*ISO/IEC 27001:2005*	ГОСТ Р ИСО/МЭК 27001-2006	*В рамках данной статьи не рассматривались*
	ISO/IEC 27001:2013	–	
	ISO/IEC 27002:2005	ГОСТ Р ИСО/МЭК 27002-2012	
	ISO/IEC 27002:2013	–	
Общие по тематике ИТ	ISO/IEC 20000-1:2011	ГОСТ Р ИСО/МЭК 20000-1-2013	COBIT 5 ITIL
Отраслевые	–	СТО БР ИББС-1.0-2014	РС БР ИББС-2.5-2014 PCI DSS v 3.0 (2013 г.)

[1] Курсивом выделены международные стандарты, которые уже не действуют, но тем не менее на данный момент действуют идентичные им ГОСТы.

можно встретить и в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных» (ст. 19 п. 2): «обнаружение фактов несанкционированного доступа к персональным данным и принятие мер».

Если рассматривать отраслевые требования, то, например, в Положении от 09.06.2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (п. 2.13) определен состав требований к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них.

Таким образом, в настоящее время есть как систематизированное описание имеющегося опыта в виде различных стандартов, так и дополнительные стимулы для организации процесса управления инцидентами.

Но прежде чем строить процесс управления, надо понять, что именно подразумевается под инцидентом.

Что понимается под инцидентами

В международном стандарте ISO/IEC 27000:2014[1] инцидент представляет собой «событие или серию нежелательных или непредвиденных событий ИБ, которые могут с большой долей вероятности привести к компрометации бизнес-операций или созданию угрозы ИБ». Такое же определение можно встретить в родственных стандартах, например ISO/IEC 27035:2011.

В банковском стандарте СТО БР ИББС-1.0-2014 определение инцидента[2] тоже в общих чертах похоже на определение из ISO/IEC 27000:2014, но при этом подробно расписаны результаты реализации инцидента ИБ.

В руководстве NIST 800-61[3] инцидент компьютерной безопасности определен как нарушение или непосредственная угроза нарушения политик компьютерной безопасности, политик допустимого использования или стандартных методов безопасности.

Также для сравнения можно привести определение инцидента из стандарта по управлению ИТ-сервисами ISO/IEC 20000-1:2011[4]: «…любое событие, которое не является частью стандартной операции услуги и которое вызывает или может вызвать прерывание или снижение качества предоставления услуги».

Таким образом, можно выделить основные признаки инцидента:
- вероятностный характер события;
- нарушение чего-либо;
- неблагоприятные последствия.

Рекомендации стандартов серии ISO 27000 и руководства NIST 800-61

Чем следует руководствоваться при построении процесса управления инцидентами? Из перечисленных стандартов наиболее общий характер имеют стандарты серии ISO 27000. Они очень популярны на международном уровне и достаточно динамично обновляются. Так, в прошлом году вышли

[1] *ISO/IEC 27000:2014 (n. 2.36): Information security incident – single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.*

[2] *Инцидент ИБ (СТО БР ИББС-1.0-2014, п. 3.48): событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:*
- *нарушение или возможное нарушение работы средств защиты информации в составе СОИБ организации БС РФ;*
- *нарушение или возможное нарушение требований законодательства РФ, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение или возможное нарушение в выполнении процессов СОИБ организации БС РФ;*
- *нарушение или возможное нарушение в выполнении банковских технологических процессов организации БС РФ;*
- *нанесение или возможное нанесение ущерба организации БС РФ и (или) ее клиентам.*

[3] *NIST Computer Security Incident Handling Guide Special Publication 800-61 Revision 2, август 2012 г.: A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.*

[4] *ISO/IEC 20000-1:2011 (n. 3.10): Incident – unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer.*

новые версии ISO/IEC 27001:2013 и ISO/IEC 27002:2013.

В новой версии ISO/IEC 27001, как и в старой, вопросам управления инцидентами отводится целый раздел Приложения А (А.16). При этом в старой версии стандарта управление инцидентами упоминалось и в основной части, содержащей обязательные требования, – в разделах о внедрении системы управления информационной безопасностью (СУИБ) и управления записями (пп. 4.2.2 (h) и 4.3.3). Критично ли вытеснение вопросов управления инцидентами за пределы основной части стандарта? Скорее всего, нет. Значимость данного процесса при этом нисколько не изменилась. В любом случае, вряд ли найдется компания, которая сможет обоснованно доказать, что у нее нет потребности в управлении инцидентами и данный раздел Приложения А к ней не применим.

ISO/IEC 27001 содержит только краткие требования, выполнение которых необходимо для сертификации СУИБ. Более развернутые рекомендации приведены в ISO/IEC 27002. Хотя даже в развернутом виде эти рекомендации умещаются на пяти неполных страницах печатного текста (по крайней мере, в официальной англоязычной версии стандарта). Тем не менее основные моменты для организации процесса управления инцидентами в этом стандарте отражены, а отсутствие подробных инструкций оставляет место для маневра и применения творческого подхода. Поскольку данный стандарт носит общий характер, под его требования можно подстроить любую другую методологию управления инцидентами.

Итак, основные требования к процессу управления инцидентами в стандартах ISO/IEC 27001 и ISO/IEC 27002 заключаются в следующем:

- распределение ответственности и разработка процедур. Это ключевой момент в любом процессе. Если персонал не будет знать, кому и каким образом реагировать на инцидент, то об управлении данным процессом не может быть и речи. Процедуры должны покрывать весь «жизненный цикл» инцидентов: от планирования действий до принятия ответных мер в случае инцидента, информирования соответствующих должностных лиц и заинтересованных сторон, сбора доказательств и оценки произошедшего. В каком объеме эти процедуры должны быть зафиксированы в виде документов – решать самой компании в зависимости от масштабов бизнеса и действующего порядка. Главное – обеспечить осведомленность всех сотрудников о необходимом порядке действий;
- информирование об инцидентах. Стандарт определяет, что все (не только штатные сотрудники компании, но и подрядчики, привлекаемые для выполнения каких-либо работ) должны в обязательном порядке своевременно информировать ответственных лиц о соответствующих событиях ИБ (например, о выявленных ошибках персонала, нарушении требований нормативной документации, ошибках в работе ПО и оборудования и т. п.). Здесь важны три момента: корректная классификация событий ИБ (о чем следует оповещать), осведомленность персонала о том, кому и в каком случае следует передавать информацию, и «работоспособность» каналов передачи информации (чтобы она своевременно была доведена до ответственных лиц);
- информирование об уязвимостях ИБ. Данная мера на первый взгляд похожа на предыдущее требование, но носит не корректирующий, а превентивный характер и предназначена для предотвращения возможных инцидентов ИБ;
- оценка и принятие решений по инцидентам. Не всякое событие ИБ является инцидентом – все зависит от принятой классификации и проведенной оценки. В идеале для проведения такой оценки и принятия решений по инцидентам в компании должна существовать группа реагирования на инциденты (incident response team – ISIRT);
- реагирование на инциденты. Рекомендуется, чтобы процедура ответных действий на инциденты была документирована и включала такие действия, как сбор свидетельств, проведение экспертного анализа, эскалация (при необходимости), ведение необходимых записей, оповещение заинтересованных сторон, устранение обнаруженных уязвимостей, закрытие инцидента и оформление необходимой документации;
- извлечение уроков из произошедших инцидентов. Учиться, конечно, лучше на чужих ошибках, но если уж инцидент произошел, следует досконально изучить его причины и принять необходимые меры, чтобы по возможности предотвратить его повторное возникновение. В случае серьезных инцидентов стремление наступать на одни и те же грабли может иметь печальные последствия;
- сбор свидетельств. Данный процесс должен обеспечить наличие доказательной базы как для внутренних дисциплинарных процессов, так и при необходимости для судебного разбирательства. На этом этапе (или хотя бы при разработке соответствующих процедур) желательно привлечь юристов, поскольку данные вопросы выходят за рамки ответственности специалистов по ИБ.

Более подробное описание такого процессного подхода можно найти в стандарте ISO/IEC 27035:2011. По объему он гораздо солиднее (около 80 страниц) и посвящен исключительно вопросам управления инцидентами. Весьма интересны и полезны для применения справочные приложения, в них приведены описания примеров инцидентов, подходов к классификации и категорированию событий ИБ, отчетов о событиях ИБ и инцидентах.

Единственный минус стандартов серии ISO/IEC 27000 заключается в том, что их официальные версии распространяются на коммерческой основе и не имеют русскоязычного варианта.

В качестве бесплатной альтернативы (но тоже на английском языке) можно использовать руководство NIST 800-61. По объему это практически такой же документ, но стиль изложения несколько отличается от стандартов серии ISO/

IEC 27000 (впрочем, этот документ не имеет статуса стандарта). Да и характер документа более технический – как уже упоминалось ранее, инциденты в нем ограничиваются «инцидентами компьютерной безопасности». При этом основные идеи пересекаются со стандартом ISO/IEC 27035:2011, что не удивительно – руководство NIST 800-61 указано в его библиографии.

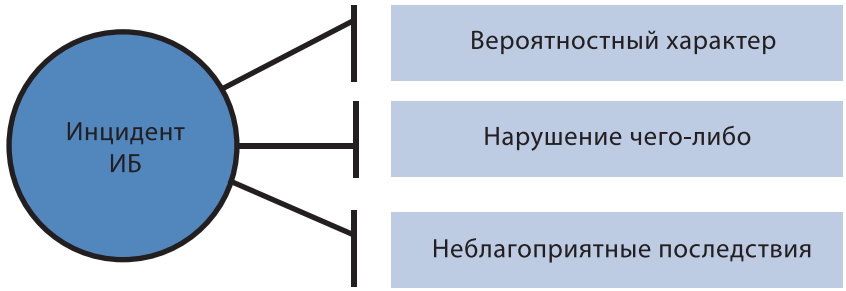

Рисунок. *Свойства инцидента ИБ*

Подходы отраслевых стандартов

При разработке процесса управления инцидентами можно обратить внимание и на отраслевые стандарты. Даже если компания не относится к числу организаций, работающих в данной отрасли, основные моменты по управлению инцидентами, а также какие-то идеи можно почерпнуть и из отраслевых стандартов.

Так, банковская сфера всегда лидировала в применении передового опыта в области ИБ и в адаптации зарубежных стандартов. Совсем недавно (1 июня 2014 г.) были введены рекомендации в области стандартизации Банка России «Менеджмент инцидентов информационной безопасности» (РС БР ИББС-2.5-2014). Документ сравнительно небольшой – около 30 страниц и рекомендован к применению организациями банковской системы Российской Федерации. Однако даже в этом, только что введенном в действие документе, заметно отставание от международных стандартов: в качестве одного из источников в библиографии указан ГОСТ Р ИСО/МЭК ТО 18044-2007, который идентичен международному стандарту ISO/IEC TR 18044:2004, а этот стандарт еще три года назад был заменен ISO/IEC 27035:2011. Тем не менее у РС БР ИББС-2.5-2014 есть неоспоримые плюсы: документ доступен бесплатно и на русском языке.

В заключение несколько слов о том, почему стоит управлять инцидентами. На самом деле вариантов может быть множество:

1. Сокращение возможного ущерба от реализации инцидентов и предотвращение их возникновения в дальнейшем. Грамотная и своевременная реакция на инциденты поможет своевременно локализовать проблему, чтобы влияние на бизнес было минимальным.
2. Сбор статистики для адекватной оценки рисков информационной безопасности. Отсутствие статистических данных – одна из проблем, на которую ссылается большинство специалистов, когда речь заходит об оценке рисков. Понятно, что о произошедших инцидентах мало кто хочет распространяться, хотя нередко для имиджа компании лучше оповестить о произошедшем заинтересованных лиц (клиентов, партнеров и др.) самостоятельно. Для западных компаний это одна из норм ведения бизнеса, но все равно иногда журналисты узнают о какой-то крупной утечке конфиденциальной информации или сбое в работе систем первыми и преподносят эту новость так, как считают нужным. В любом случае ведение такой статистики для собственных нужд компании несомненно принесет пользу.
3. Постоянный мониторинг событий. Иногда несколько, на первый взгляд, незначительных и не связанных между собой мелких инцидентов могут привести к серьезному ущербу для компании. Если у специалистов будут необходимые данные, такие настораживающие события вполне возможно вовремя отследить – будь то сбои в работе техники или проявления человеческого фактора. Кроме того, ведение постоянного мониторинга событий – обязательное требование многих нормативных документов.
4. Выявление проблемных мест в системе обеспечения информационной безопасности (в том числе и в эффективности функционирования СУИБ как части этой системы). Причем в данном случае должно насторожить как большое количество сообщений о каком-то виде инцидентов, так и полное отсутствие информации о них. Если данные об инцидентах не поступают – это может свидетельствовать не об отсутствии инцидентов как таковых, а о неверной настройке средств защиты, ошибках в классификации, непонятных процедурах реагирования на инциденты, отсутствии осведомленности у персонала.
5. Выполнение требований соответствующих стандартов и нормативных документов. Конечно, это не самая лучшая мотивация, так как при этом с высокой степенью вероятности подход к процессу управления инцидентами будет формальным – выполнить необходимый минимум и не более того. Тем не менее даже такой подход может послужить отправной точкой для уже осознанного процесса, когда помимо формального соответствия требованиям компания научится извлекать из этого дополнительную выгоду.

Говорить о реализации полноценного процесса управления инцидентами без автоматизации процессов и использования соответствующих специализированных продуктов и решений в современных условиях не приходится. Однако менять приоритетность задач не стоит: прежде всего следует определить, каким образом будет осуществляться управление, и только потом – какие технические решения способны в этом помочь. ■