Экз. № ___

Федеральное агентство по техническому регулированию и метрологии

Логотип национального органа по стандартизации

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 18044-

(проект, первая редакция)

Информационная технология
Методы и средства обеспечения безопасности

Менеджмент инцидентов информационной безопасности

ISO/IEC TR 18044:2004

Information technology – Security techniques – Information security incident management

(IDT)

Настоящий проект стандарта не подлежит применению до его принятия

Москва

2007

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения"

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России") и обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл") на основе собственного аутентичного перевода стандарта, указанного в п. 5

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от "___" _____ 200_ № _____

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт идентичен международному стандарту ИСО/МЭК ТО 18044:2004 "Финансовые услуги. Рекомендации по информационной безопасности" (ISO/IEC TR 18044:2005 *“Information technology – Security techniques – Information security incident management”*).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении С.

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "Национальные стандарты". Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Распространение настоящего стандарта на территории Российской Федерации осуществляется с соблюдением правил, установленных Федеральным агентством по техническому регулированию и метрологии

Содержание

Введение

Никакие типовые политики информационной безопасности или защитные меры информационной безопасности (ИБ) не могут гарантировать полную защиту информации, информационных систем, сервисов или сетей. После внедрения защитных мер, вероятно, останутся слабые места, которые могут сделать обеспечение информационной безопасности неэффективным, и, следовательно, инциденты ИБ возможными. Инциденты ИБ могут оказывать прямое или косвенное негативное воздействие на бизнес-деятельность организации. Кроме этого, будут неизбежно выявляться новые, ранее не идентифицированные угрозы. Недостаточная подготовка организации к обработке таких инцидентов делает практическую реакцию на инциденты малоэффективной, и это потенциально увеличивает степень негативного воздействия на бизнес. Таким образом, для любой организации, серьезно относящейся к ИБ, важно применять структурный и плановый подход к следующему:

– обнаружению, оповещению об инцидентах ИБ и их оценке;

– реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после негативных воздействий (например, в областях поддержки и планирования непрерывности бизнеса);

– извлечению уроков из инцидентов информационной безопасности, введению превентивных защитных мер и, со временем, улучшению общего подхода к менеджменту инцидентов информационной безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология. Методы и средства обеспечения безопасности

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Information technology. Security techniques.
Information security incident management

Дата введения 200X-XX-0X

1 Область применения

Настоящий стандарт устанавливает рекомендации по менеджменту инцидентов информационной безопасности для руководителей подразделения по информационной безопасности, информационных систем, сервисов и сетей.

Настоящий стандарт состоит из 11 разделов и построен следующим образом. В разделе 1 приводится область применения, в разделе 2 – перечень ссылок, в разделе 3 – термины и определения. В разделе 4 представлены основы менеджмента инцидентов информационной безопасности, в разделе 5 – преимущества и ключевые вопросы. Далее, в разделе 6 приводятся примеры инцидентов ИБ и объясняются причины их возникновения. В разделе 7 описываются процессы планирования и подготовки к менеджменту инцидентов ИБ, включая составление документов. Функционирование системы менеджмента инцидентов ИБ описывается в разделе 8. Этап анализа менеджмента ИБ, включая изучение полученных уроков и улучшения (повышения) безопасности, а также системы менеджмента инцидентов ИБ, описываются в разделе 9. Этап улучшения, т. е., внедрение принятых улучшений в систему безопасности и систему менеджмента инцидентов ИБ, описывается в разделе 10. Настоящий стандарт завершается кратким резюме, представленным в разделе 11. Приложение А содержит примерные формы отчетов о событиях и инцидентах ИБ. Приложение В – некоторые примерные общие рекомендации для оценки негативных последствий инцидентов ИБ, включаемых в формы отчетов. За приложениями следует раздел ″Библиография″.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ИСО/МЭК 13335-1:2004, Методы и средства обеспечения безопасности ИТ – Менеджмент безопасности информационных и коммуникационных технологий – Часть 1: Понятия и модели для менеджмента безопасности информационных и коммуникационных технологий.

ИСО/МЭК 17799:2000, Информационная технология – Практические правила менеджмента информационной безопасности.

П р и м е ч а н и е – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования – на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом, следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В данном отчете применяются термины и определения, заимствованные из ИСО/МЭК 13335-1, ИСО/МЭК 17799 и приводимые ниже.

3.1 Планирование непрерывности бизнеса

Планирование непрерывности бизнеса является процессом обеспечения гарантии восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов. Процесс должен также обеспечивать уверенность в том, что восстановление бизнеса достигается с учетом заданных очередностей и интервалов времени, и дальнейшее восстановление всех функций бизнеса в исходное состояние.

Ключевые элементы этого процесса должны обеспечивать уверенность в том, что применяются необходимые плановые и средства и то, что они включают в себя информацию, процессы бизнеса, информационные системы и сервисы, голосовую связь и передачу данных, персонал и физические устройства.

3.2 Событие информационной безопасности

Событием ИБ является идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

3.3 Инцидент информационной безопасности

Инцидент информационной безопасности - событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операции и создания угрозы ИБ (примеры инцидентов ИБ даются в разделе 6).

3.4 Группа реагирования на инциденты информационной безопасности

Группа реагирования на инциденты информационной безопасности (ГРИИБ) является группой (командой) соответственно обученных и доверенных членов организации, которая обрабатывает инциденты ИБ во время их жизненного цикла. Иногда эта группа может дополняться внешними экспертами, например, из официально признанной группы реагирования на компьютерные инциденты или компьютерной группы быстрого реагирования (КГБР).

3.5 Дополнительные определения

См. также определения, содержащиеся в Глоссарии ИСО/МЭК СТК 1 ПК 27.

4 Исходные данные

4.1 Цели

В качестве основной части общей стратегии ИБ организации важно иметь структурированный, хорошо спланированный метод менеджмента инцидентов ИБ. Целями такого метода является обеспечение того, что:

– события ИБ могут быть обнаружены и эффективно обработаны, в частности, определены как относящиеся или не относящиеся к категории инцидентов ИБ[1)];

– идентифицированные инциденты ИБ оценены и разрешены (урегулированы) наиболее подходящим и результативным способом;

– негативные воздействия инцидентов ИБ на организацию и ее бизнес-операции можно минимизировать соответствующими защитными мерами, являющимися частью процесса реагирования на инцидент, возможно, наряду с применением соответствующих элементов из плана(ов) непрерывности бизнеса;

– из инцидентов ИБ и их менеджмента можно быстро извлечь уроки. Это делается с целью повышения шансов предотвращения инцидентов ИБ в будущем, улучшения внедрения и использования защитных мер ИБ, улучшения общей системы менеджмента инцидентов ИБ.

4.2 Процессы

Для достижения целей, описанных в 4.1 , менеджмент инцидентов ИБ состоит из четырех отдельных процессов:

– Планирование и подготовка;

– Использование;

– Пересмотр (анализ);

– Улучшение[2)].

(Необходимо отметить, что эти процессы аналогичны процессам модели PDCA, используемой в международных стандартах ИС 9000 и ИС 14000).

Примерное содержание этих процессов показано на рисунке 1, ниже.

4.2.1 Планирование и подготовка

Эффективный менеджмент инцидентов ИБ требует надлежащего планирования и подготовки. Чтобы реакция на инциденты ИБ была эффективной, необходимы следующие действия:

[1)] События ИБ могут быть результатом случайных или преднамеренных попыток компрометации защитных мер ИБ, но в большинстве случаев событие ИБ, само по себе, не означает, что попытка в действительности была успешной, и, следовательно, каким-то образом повлияла на конфиденциальность, целостность и (или) доступность, т. е., не все события ИБ будут отнесены к категории инцидентов ИБ.

[2)] Соответствующие процессы СМИБ называются: планирование, осуществление, проверка и действие (модель PDCA) (прим. переводч.)

– разработка и документирование политики менеджмента инцидентов ИБ, а также очевидная поддержка этой политики со стороны основных акционеров и, в особенности, высшего руководства;

– разработать и в полном объеме документировать систему менеджмента инцидентов ИБ для поддержки политики менеджмента инцидентов ИБ. Формы, процедуры и инструменты поддержки для обнаружения, оповещения, оценки и реагирования на инциденты ИБ, а также детали шкалы[1)] опасности инцидентов должны быть отражены в документации на систему. (Следует заметить, что в некоторых организациях такая система может называться планом реагирования на инциденты ИБ);

– обновлять политики менеджмента ИБ и рисков на всех уровнях, т. е., корпоративном, и для каждой системы, сервиса и сети, с учетом системы менеджмента инцидентов ИБ;

[1)] Должна быть определена шкала серьезности инцидентов с соответствующей классификацией. Эта шкала может состоять, например, из двух положений: «основные» и «незначительные». Так или иначе, положение на шкале основывается на фактических или предполагаемых негативных воздействий на бизнес-операции организации.

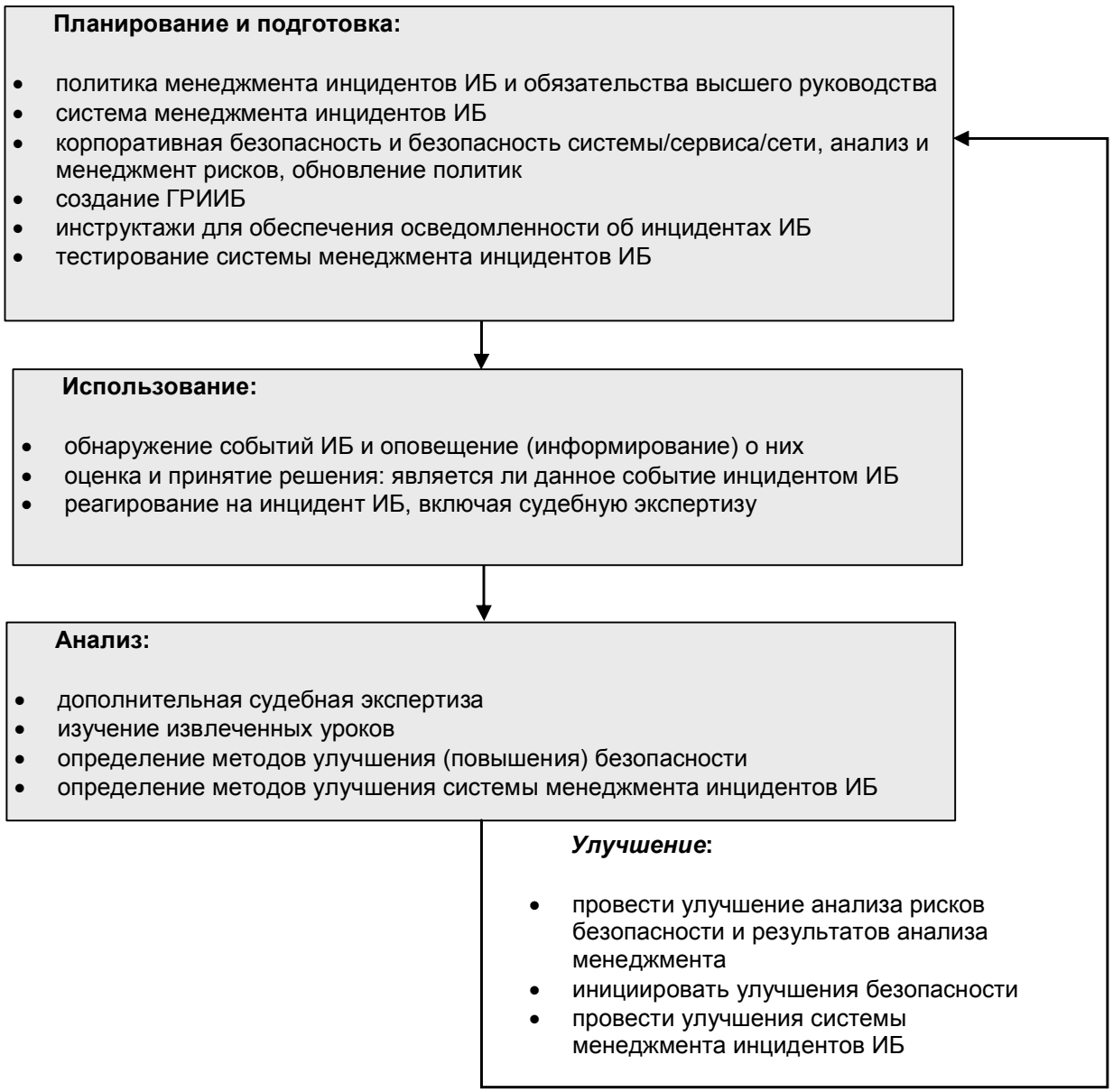

Рисунок 1 – Процессы менеджмента инцидентов ИБ

– создать в организации соответствующую организационную структуру менеджмента инцидентов ИБ, т. е., ГРИИБ, с определенными ролями и ответственностями персонала, способного адекватно реагировать на все известные типы инцидентов ИБ. В большинстве организаций ГРИИБ является действующей группой состоящей из его руководителя, поддерживаемого группой специалистов, специализирующихся на конкретных областях,, например, при отражении атак вредоносной программы привлекается специалист по инцидентам подобного типа;

– оповещать весь персонал организации посредством инструктажей и (или) иных способов о существовании системы менеджмента инцидентов ИБ, ее преимуществах и о том, как надлежащим образом сообщать о событиях ИБ. Должно проводиться соответствующее обучение персонала, ответственного за управление системой менеджмента инцидентов ИБ, лицами, принимающими решения по определению того, являются ли события инцидентами, и лицами, исследующими инциденты;

– тщательно тестировать систему менеджмента инцидентов ИБ.

Фаза "Планирование и подготовка" далее описывается в разделе 7.

4.2.2 Использование системы менеджмента инцидентов информационной безопасности

При использовании системы менеджмента инцидентов ИБ необходимы следующие процессы:

– обнаружение и сообщение о возникновении событий ИБ (человеком или автоматическими средствами);

– сбор информации, связанной с событиями ИБ, и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;

– реагирование на инциденты ИБ:

- немедленно, в реальном или почти реальном масштабе времени;
- если инциденты ИБ находятся под контролем, выполнять действия, которые могут потребоваться в более позднее время (например, при оказании помощи по полному восстановлению после катастрофы);
- если инциденты ИБ не находятся под контролем, то выполнять "антикризисные" действия (например, вызвать пожарную команду/подразделение или инициировать план непрерывности бизнеса);
- сообщать о наличии инцидентов ИБ и любые относящиеся к ним подробности персоналу своей организации, а также персоналу сторонних организаций (это может включать, по требованию, обострение инцидента с целью проведения дополнительных оценок и (или) принятия решения);
- судебная экспертиза;
- надлежащая регистрация всех действий и решений для последующего анализа;
- завершение решения проблемы инцидентов.

Этап "Использование" описывается далее в разделе 8.

4.2.3 Анализ

После разрешения/закрытия инцидентов ИБ необходимо предпринять следующие действия по анализу состояния ИБ:

– провести дальнейшую судебную экспертизу, если потребуется;

– изучить уроки, извлеченные из инцидентов ИБ;

– определить улучшения для внедрения защитных мер ИБ, как результат полученных уроков, извлеченных из одного или нескольких инцидентов ИБ;

– определить улучшения системы менеджмента инцидентов ИБ в целом, учитывая уроки, извлеченные из анализов гарантии качества предпринимаемого метода (например, из анализа результативности процессов, процедур, форм отчета и(или) организации.

Этап "Анализ" далее описывается в разделе 9.

4.2.4 Улучшение

Известно, что процессы менеджмента инцидентов ИБ являются итеративными, с регулярными улучшениями, вносимыми со временем в ряд элементов ИБ. Эти улучшения предлагаются на основе данных по инцидентам ИБ и реагированию на них, а также данных по динамике тенденций. Этап "Улучшение" включает:

– пересмотр имеющихся результатов анализа рисков ИБ и анализ менеджмента организации;

– улучшение системы менеджмента инцидентов ИБ и ее документации;

– инициирование улучшений в области безопасности, включая внедрение новых и (или) обновленных защитных мер ИБ.

Этап "Улучшение" далее описывается в разделе 10.

5 Преимущества и ключевые вопросы

В данном разделе представлена информация о:

– преимуществах, получаемых от оптимальной системы менеджмента инцидентов ИБ;

– ключевых вопросах, которые необходимо рассмотреть, чтобы убедить в преимуществах высшее корпоративное руководство и персонал, который будет предоставлять отчеты в систему и получать от нее информацию.

5.1 Преимущества

Любая организация, использующая структурный подход к менеджменту инцидентов ИБ, может извлечь из этого значительные преимущества, которые можно объединить в следующие группы:

– улучшение ИБ;

– уменьшение последствий негативных воздействий на бизнес, например, прерывание бизнеса и финансовые потери, как последствия инцидентов ИБ;

– концентрация внимания по вопросам предотвращения инцидентов;

– концентрация внимания на установление приоритетов и свидетельств;

– вклад в обоснование бюджета и ресурсов;

– обновление результатов менеджмента и анализа рисков на более совершенном уровне;

– предоставление материала для программ повышения осведомленности и обучения в области ИБ;

– предоставление входных данных для анализа политики ИБ и соответствующей документации.

Каждый из этих вопросов рассматривается ниже.

5.1.1 Улучшение безопасности

Структурный процесс обнаружения, оповещения, оценки и менеджмента инцидентов и событий ИБ позволяет быстро идентифицировать и реагировать на любое событие или инцидент ИБ, тем самым, улучшая общую безопасность за счет быстрого определения и реализации правильного решения, а также обеспечивая средства предотвращения подобных инцидентов ИБ в будущем.

5.1.2 Снижение негативных воздействий на бизнес

Структурный подход к менеджменту инцидентов ИБ может способствовать снижению уровня негативных воздействий на бизнес, связанных с инцидентами ИБ. Эти воздействия могут включать в себя непосредственные финансовые потери, а также долговременные потери, возникающие от ущерба, нанесенного репутации и кредитоспособности.

5.1.3 Концентрация внимания на предотвращении инцидентов

Использование структурного подхода к менеджменту инцидентов ИБ может помочь сконцентрировать внимание на предотвращении инцидентов внутри организации. Анализ данных, связанных с инцидентами позволит определить модели и тенденции, тем самым, способствуя более точной концентрации на предотвращении инцидентов и, следовательно, идентификации соответствующих действий для предотвращения возникновения инцидентов.

5.1.4 Усиление системы установления приоритетов и свидетельств

Структурный подход к менеджменту инцидентов ИБ создает прочную основу для системы установления приоритетов при проведении расследований инцидентов ИБ.

При отсутствии четких процедур, существует риск того, что деятельность по расследованию будет проводиться в активном режиме, когда реагирование на инциденты будет осуществляться по мере их появления, и на "окрик" соответствующего руководителя. Однако это может помешать осуществлению деятельности по расследованию там, где она действительно необходима, причем в последовательности, соответствующей идеальной установки приоритетов.

Четкие процедуры расследования инцидентов могут обеспечить уверенность в том, что сбор данных и их обработка очевидно правильны и допустимы юридически. Это имеет большое значение в случае возникновения судебного преследования или дисциплинарного взыскания. Однако, следует признать, что есть вероятность того, что действия, необходимые для восстановления после инцидента ИБ, могут подвергнуть риску целостность любого полученного свидетельства.

5.1.5 Бюджет и ресурсы

Хорошо определенный и структурированный подход к менеджменту инцидентов ИБ поможет обосновать и упростить распределение бюджетов и ресурсов внутри подразделений организации. Кроме того, выгоды получает и сама система менеджмента инцидентов ИБ. Такие выгоды связаны с:

– использованием менее квалифицированного персонала для идентификации и фильтрации ложных сигналов тревоги;

– обеспечением лучшего руководства действий квалифицированного персонала;

– привлечением квалифицированного персонала только для тех процессов, где требуется его навыки, и только на той стадии процесса, где его содействие необходимо.

Кроме того, структурный подход к менеджменту инцидентов ИБ может включать в себя процедуру "отметки времени", так что обеспечивает возможность делать "количественные" оценки обработки инцидентов ИБ в организации. Это сделает возможным, например, получение информации о времени разрешения инцидентов с различными приоритетами на различных платформах. При наличии узких мест в процессе менеджмента инцидентов ИБ, эти узкие места они также должны быть идентифицируемы.

5.1.6 Менеджмент и анализ рисков ИБ

Использование структурного подхода к менеджменту инцидентов ИБ способствует:

– сбору лучших данных для идентификации и определения характеристик различных типов угроз и связанных с ними уязвимостей;

– предоставление данных о частоте возникновения идентифицированных типов угроз.

Данные, полученные о негативных последствиях воздействия инцидентов ИБ на бизнес, будут полезны для анализа воздействия на него. Данные о частоте возникновения различных типов угроз намного повысят качество оценки угроз. Аналогично, данные об уязвимостях намного повысят качество будущих оценок уязвимостей.

Такие данные значительно улучшат результаты анализа менеджмента и анализа рисков ИБ.

5.1.7 Осведомленность в вопросах ИБ

Структурный подход к менеджменту инцидентов ИБ дает сконцентрированную информацию о программах обеспечения осведомленности в вопросах ИБ. Эта сконцентрированная информация является источником реальной примерной информации, способной продемонстрировать, что инциденты ИБ действительно происходят именно в данной организации и не всегда "где-то у других". Этим также демонстрируют выгоды быстрого получения информации, необходимой для принятия решений. Более того, подобная осведомленность в вопросах ИБ позволяет снизить вероятность ошибки, паники/растерянности в случае возникновения инцидента ИБ.

5.1.8 Входные данные для пересмотра политики ИБ

Информация, представляемая системой менеджмента инцидентов ИБ, может обеспечить ценные входные данные для анализов результативности и последующего усовершенствования политик ИБ (и другой документации, связанной с ИБ). Это относится к политикам и другой документации как на уровне организации, так и для отдельных систем, сервисов и сетей.

5.2 Ключевые вопросы

Обратная связь менеджмента инцидентов ИБ обеспечивает уверенность персонала в том, что его работа остается сфокусированной на реальных рисках для систем, сервисов и сетей организации. Эта важная обратная связь не может быть результативной, реализована, если инциденты ИБ обрабатываются по мере их появления на специально разработанной основе. Такая связь может быть более результативной в случае структурной, хорошо спроектированной системы менеджмента инцидентов ИБ, которая применяет общую структуру для всех частей организации. Данная структура должна непрерывно обеспечивать получение от системы более полных результатов и представлять надежную основу для быстрого определения возможных условий инцидента ИБ до его появления, и которые иногда называются "тревожными сигналами".

Менеджмент и аудит системы менеджмента ИБ обеспечивают основу доверия, необходимого для расширения совместной работы с персоналом и снижения недоверия относительно сохранения анонимности, безопасности и доступности полезных результатов. Например, руководящий и рабочий персонал должны быть уверены в том, что "тревожные сигналы" сообщат своевременную, точную и полную информацию относительно ожидаемого инцидента.

При внедрении систем менеджмента инцидентов ИБ организациям следует избегать таких потенциальных проблем, как отсутствие полезных результатов и озабоченности, касающейся вопросов, связанных с неприкосновенностью информации о персональных данных. Необходимо убедить заинтересованные стороны в том, что для предотвращения появления таких проблем были предприняты определенные шаги.

Таким образом, для построения оптимальной системы менеджмента инцидентов ИБ нужно рассмотреть большое число ключевых вопросов, включая:

- обязательства руководства;

– осведомленность;
– правовые и нормативные аспекты;
– эксплуатационную результативность и качество;
– анонимность;
– конфиденциальность;
– доверие к работе;
– типологию.

Каждый из этих вопросов обсуждается ниже.

5.2.1 Обязательства менеджмента (руководства)

Обеспечение непрерывной поддержки со стороны менеджмента жизненно необходимо для принятия структурного подхода к менеджменту инцидентов ИБ. Персонал должен распознавать инциденты и знать, что делать, и осознавать большие преимущества такого подхода для организации. Однако это станет маловероятным при отсутствии поддержки со стороны руководства. Эту мысль надо внушить руководству, чтобы организация занималась обеспечением ресурсами и поддержкой способности реагирования на инциденты.

5.2.2 Осведомленность

Другим важным элементом принятия структурного подхода к менеджменту инцидентов ИБ является осведомленность. Пока будет потребность в участии пользователей, они вряд ли будут эффективно участвовать в работе организации, если не будут осведомлены о том, какую выгоду они и их подразделение получат от участия в структурном подходе к управлению инцидентами информационной безопасности.

Любая система менеджмента инцидентов ИБ должна сопровождаться документом с определением программы осведомленности, включающим следующее:

– преимущества, получаемые от структурного подхода к менеджменту инцидентов ИБ, как для организации, так и для ее персонала;

– информацию об инцидентах, хранящуюся в базе данных событий/инцидентов ИБ, и выходные данные из нее;

– стратегию и механизмы программы обеспечения осведомленности, которая, в зависимости от организации, может быть отдельной программой или частью более широкой программы обеспечения осведомленности в вопросах ИБ.

5.2.3 Правовые и нормативные аспекты

Следующие правовые и нормативные аспекты менеджмента инцидентов ИБ должны быть рассмотрены в политике менеджмента инцидентов ИБ и в соответствующей системе.

Обеспечение адекватной защиты персональных данных и неприкосновенность персональной информации. В странах, где существует специальное законодательство, защищающее конфиденциальность и целостность данных, этот аспект часто ограничен контролем персональных данных. Поскольку инциденты ИБ обычно связаны с неким лицом, то такая информация личного характера может потребовать соответствующей регистрации и управления. Следовательно, при структурном подходе к менеджменту инцидентов ИБ следует учитывать соответствующую защиту информации о персональных данных. Этот факт включает следующее:

– лица, имеющие доступ к личным данным, не должны лично знать тех людей, информация о которых изучается;

– лица, имеющие доступ к личным данным, должны подписать соглашение об их неразглашении до того, как получат доступ к этим данным;

– информация о персональных данных должна использоваться исключительно для тех целей, для которых она была получена, т. е., для расследования инцидентов ИБ.

Соответствующее хранение записей. Некоторые федеральные законы требуют, чтобы компании вели соответствующие записи своей деятельности для анализа в процессе ежегодного аудита организации. Подобные требования существуют для правительственных организаций. В некоторых странах от организаций требуется информирование или создание архивов для обеспечения правопорядка (например, в любом случае совершения серьезного преступления или проникновение в засекреченную правительственную систему).

Защитные меры для обеспечения выполнения коммерческих договорных обязательств. Там, где существуют обязывающие требования по предоставлению услуг по менеджменту инцидентов ИБ (например, требования ко времени реагирования), организация должна гарантировать предоставление соответствующей ИБ для обеспечения выполнения таких обязательств при любых обстоятельствах. (В связи с этим, если организация заключает контракт со сторонней организацией (см. 7.5.4), например, КГБР, должна быть гарантия, что все требования, включая время реагирования, включены в контракт со сторонней организацией).

Правовые вопросы, связанные с политиками и процедурами. Необходима проверка политик и процедур, связанных с системой менеджмента инцидентов ИБ, на наличие правовых и нормативных вопросов, например, имеются ли уведомления о дисциплинарных взысканиях и (или) судебные иски, принимаемые к лицам, создающим инциденты. В некоторых странах вопрос с увольнением решить довольно трудно.

Проверка на законность непризнания. Все непризнания действий, предпринятых группой менеджмента инцидентов ИБ или внешним вспомогательным персоналом, должны быть проверены на законность.

Включение в контракты со сторонним персоналом всех необходимых аспектов. Контракты со сторонним вспомогательным персоналом, например, КГБР, должны тщательно проверяться на наличие отказов за несение ответственности за нарушение обязательств неразглашения, доступности услуг и от последствий за неправильные консультации.

Соглашения о неразглашении. От членов группы менеджмента инцидентов ИБ могут потребовать подписать соглашения о неразглашении как при устройстве на работу, так и при увольнении. В некоторых странах такие соглашения могут не иметь юридической силы; данный аспект необходимо подвергать проверке.

Требования применения закона. Необходимо, обеспечить ясность вопросов, связанных с возможностью того, что правоприменяющие органы на законном основании могут затребовать информацию от системы менеджмента инцидентов ИБ. Может случиться так, что такая ясность потребуется на минимальном уровне, требуемом законом, по которому инциденты должны документироваться, и насколько долго документация должна храниться.

Аспекты ответственности. Необходимо уточнить вопросы потенциальной ответственности и соответствующих необходимых защитных мер. Примерами событий, связанных с вопросами ответственности, являются следующие:

– если некоторый инцидент может повлиять на деятельность другой организации (например, раскрытие общей информации), но она вовремя не оповещается и несет ущерб;

– если в продукции обнаружена новая уязвимость, но поставщик не был уведомлен об этом, в результате имел место главный инцидент, который позже нанес сильное воздействие на одну или несколько организаций;

– если не было сделано сообщение в конкретной стране, где, от организаций требуется информирование или создание архивов для правоохранительных агентств касательно всех случаев, которые могут повлечь за собой тяжкое преступление или вторжение в правительственные системы с ограниченным доступом или часть важной государственной инфраструктуры;

– если информация раскрыта, то это может указывать на то, что некое лицо или некоторая организация могли быть причастны к атаке. Это может нанести ущерб репутации и бизнесу отдельного лица или организации;

– если информация раскрыта, то это может быть результатом сбоя в определенном элементе ПО, но впоследствии оказывается, что это не так.

Специальные нормативные требования. Там, где это предусмотрено специальным и нормативными требованиями, об инцидентах следует сообщать в обозначенный орган, например, как это требуется в атомной промышленности.

Наказания или внутренние дисциплинарные процедуры. Должны применяться соответствующие защитные меры ИБ, включая гарантированно защищенные от неумелого обращения журналы аудита, пригодные для успешного преследования в судебном порядке или проведения дисциплинарных процедур внутри организации в отношении злоумышленников, вне зависимости от того, были ли эти атаки техническими или физическими. В поддержку вышесказанного необходимо собрать свидетельства, как это требуется в федеральных судах или других дисциплинарных органах. Необходимо показать, что:

– документация является полной и не подвергалась подделке;

– копии электронного свидетельства доказуемо идентичны оригиналу;

– все системы ИТ, от которых собирались свидетельства, во время регистрации работали в штатном режиме.

Правовые аспекты, связанные с методами мониторинга. Последствия использования методов мониторинга должны быть рассмотрены в контексте соответствующего национального законодательства. Законность различных методов может меняться в зависимости от страны. Например, в некоторых странах необходимо информировать людей о ведении мониторинга, включая методы наблюдения. Необходимо учесть несколько факторов, включающие, кто/что подвергается мониторингу. Они/оно подвергаются мониторингу, и когда ведется мониторинг, необходимо также заметить, что мониторинг/наблюдение в контексте систем обнаружения вторжений (СОВ) специально рассматривается в ТО 18043.

Определение политик использования и сообщение о ней. Приемлемая практика/использование политики в пределах организации должна быть определена, документирована и доведена до сведения всех предполагаемых пользователей. (Например, пользователи должны быть проинформированы о приемлемой политике использования, о чем они дают письменное подтверждение в том, что они понимают и принимают эту политику при поступлении в организацию или получении доступа к информационным системам.)

5.2.4 Эффективность эксплуатации и качества

Эффективность эксплуатации и качества структурного подхода к менеджменту инцидентов ИБ зависит от ряда факторов, включающих в себя обязательность уведомления об инцидентах, качество уведомления, простота использования, скорость и обучение. Не-

которые из этих факторов призваны убедить, что пользователи осведомлены о важности менеджмента инцидентов ИБ и мотивированы сообщать об инцидентах. Что касается скорости, то время, потраченное людьми на сообщение об инциденте – не единственный фактор, важно также учитывать время, требуемое для обработки данных и распространения обработанной информации (особенно в случае с сигналами тревог).

Для минимизации задержек, соответствующие программы обеспечения осведомленности и обучения пользователей должны дополняться поддержкой "горячей линии", которая обеспечивается сотрудниками, осуществляющими менеджмент инцидентов ИБ.

5.2.5 Анонимность

Вопрос анонимности является основополагающим для успеха менеджмента инцидентов ИБ. Пользователи должны быть уверены, что информация, которую они сообщают относительно инцидентов ИБ, полностью защищена, а при необходимости обезличена, чтобы ее невозможно было связать со своей организацией или ее частью без их полного согласия.

Система менеджмента инцидентов ИБ должна учитывать ситуации, когда важно обеспечить анонимность лица или организации, сообщающих о потенциальных инцидентах ИБ при особых обстоятельствах. Каждая организация должна иметь положения, которые четко иллюстрируют последствия анонимности или ее отсутствия для лиц и организаций, сообщающих о потенциальном инциденте ИБ. ГРИИБ может потребоваться дополнительная информация, не связанная с той, что получена от информирующего лица или организации. Более того, важная информация об инциденте ИБ может быть получена от лица, первым заметившего его.

5.2.6 Конфиденциальность

Система менеджмента инцидентов ИБ может содержать конфиденциальную информацию, и лицам, занимающимся инцидентами, может потребоваться доступ к ней. Поэтому во время обработки должна быть обеспечена анонимность этой информации или персонал должен подписывать соглашение о конфиденциальности (неразглашении) при получении доступа к ней. Если события ИБ регистрируются через систему менеджмента обобщенных проблем, то чувствительные детали могут также опускаться. В случае регистрации событий информационной безопасности через обобщенную систему менеджмента проблем, могут быть пропущены подробности, обладающие свойством ограниченного доступа.

Кроме того, система менеджмента инцидентов ИБ должна обеспечивать контроль за передачей сообщений об инцидентах сторонними организациями, включая СМИ, партнеров по бизнесу, потребителей, правоприменяющие организации и общественность.

5.2.7 Доверие к работе

Любая группа специалистов менеджмента инцидентов ИБ должна быть способна эффективно удовлетворять функциональные, финансовые, правовые и политические потребности организации и быть в состоянии соблюдать осторожность в организации при управлении инцидентами ИБ. Деятельность группы менеджмента инцидентов ИБ должна также подвергаться независимому аудиту, чтобы убедиться в эффективном удовлетворении требований бизнеса. Далее, эффективным способом реализации другого аспекта независимости является отделение цепочки сообщений о реагировании на инцидент от оперативного линейного руководства, и возложение на высшее руководство непосредственных обязанностей по управлению реакциями на инциденты. Финансирование работы группы также должно быть отдельным, чтобы избежать чрезмерного влияния.

5.2.8 Типология

Общая типология, отражающая общую структуру подхода к менеджменту инцидентов ИБ, является одним из ключевых факторов обеспечения последовательных надежных результатов. Типология, вместе с общепринятыми метриками и стандартной структурой баз данных, обеспечивает возможность сравнивать результаты, улучшать предупреждающую информацию и получать более точное представление об угрозах и для информационных систем[1)] и их уязвимостях.

6 Примеры инцидентов информационной безопасности и их причины

Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием ошибки или природных явлений) и могут вызываться как техническими, так и физическими средствами. Их последствиями могут быть такие события, как несанкционированные изменения информации, ее уничтожения или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. События ИБ, о которых не было сообщено, которые не были определены как инциденты, не могут быть исследованы, и не могут быть применены защитные меры для предотвращения повторного появления этих событий.

Последующие описания выбранных примеров инцидентов ИБ и их причин даются *только с целью иллюстрации*. Важно заметить, что эти примеры ни в коем случае не являются исчерпывающими.

6.1 Отказ в обслуживании

Отказ в обслуживании является обширной категорией инцидентов, имеющих одну общую черту. Подобные инциденты приводят к сбоям в системах, сервисах или сетях, которые не могут продолжать работу с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

Существует два основных типа инцидентов "отказ в обслуживании", создаваемых техническими средствами: уничтожение ресурсов и истощение ресурсов.

Некоторыми типичными примерами таких преднамеренных технических инцидентов "отказ в обслуживании" являются следующие:

– зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

– передача данных в непредвиденном формате в систему, сервис или сеть в попытке разрушить или нарушить нормальную работу;

– одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать ее ресурсы (т. е., замедлить ее работу, блокировать ее или разрушить).

Одни технические инциденты "отказ в обслуживании" могут создаваться случайно, например, в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного программного обеспечения, а другие инциденты могут быть преднамеренными. Некоторые технические инциденты "отказ в обслуживании" инициируются намеренно, чтобы разрушить систему или сервис, снизить производительность

[1)] Определение общей типологии не является целью данного документа. Читателю рекомендуется обратиться к другим источникам за этой информацией.

сети, тогда как инциденты являются всего лишь побочными продуктами другой вредоносной деятельности. Например, некоторые наиболее распространенные методы скрытого сканирования и идентификации могут приводить к полному разрушению старых или ошибочно сконфигурированных систем или сервисов при их сканировании. Следует заметить, что многие преднамеренные технические инциденты "отказ в обслуживании" часто выполняются анонимно (т. е., источник атаки "ложный"), поскольку они обычно не рассчитывают на злоумышленника, получающего какую-либо информацию от атакуемой сети или системы.

Инциденты "отказ в обслуживании", создаваемые нетехническими средствами, приводящие к потере информации, сервиса и (или) устройств обработки могут, например, вызываться следующим:

– нарушение физических систем безопасности, приводящие к хищениям, или преднамеренным нанесением ущерба, или разрушением оборудования;

– случайное нанесение ущерба аппаратуре и (или) ее местоположению от огня или воды/наводнения;

– экстремальные условия окружающей среды, например, высокая температура (выход из строя кондиционера);

– неправильное функционирование или перегрузка системы;

– неконтролируемые изменения в системе;

– неправильное функционирование программного или аппаратного обеспечения.

6.2 Сбор информации

В общих чертах, категория инцидентов "сбор информации" включает действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, запущенных на идентифицированных целях атаки. Инциденты такого типа предполагают проведение разведки с целью определения следующего:

– существования некоторой цели получения представления о топологии сети, вокруг нее, и с кем обычно эта цель сообщается;

– потенциальных уязвимостей цели или уязвимости непосредственной сетевой среды, которые можно использовать.

Типичными примерами атак, направленных на сбор информации техническими средствами являются следующие:

– сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);

– отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;

– зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;

– сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов (например, электронная почта, FTP, Web и т. д.) и версий программного обеспечения этих сервисов;

– сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов (горизонтальное сканирование).

В некоторых случаях технический сбор информации расширяется до несанкционированного доступа, если, например, злоумышленник, отыскивая уязвимости, пытается также получить несанкционированный доступ. Обычно это осуществляется автоматиче-

скими хакерскими приборами, которые не только ищут уязвимости, но и автоматически пытаются использовать уязвимые системы, сервисы и (или) сети.

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводящие к следующему:

– прямому или косвенному раскрытию или модификации информации;

– хищению интеллектуальной собственности, хранимой в электронной форме;

– нарушению учетности, например, при регистрации учетных записей;

– неправильному использованию информационных систем (например, с нарушением закона или политики организации),

могут вызываться, например, следующим образом:

– нарушениями физической защиты безопасности, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные, например, ключи шифрования;

– неудачно и (или) неправильно конфигурированными операционными системами по причине неконтролируемых системных изменений в системе, или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

6.3 Несанкционированный доступ

Данная категория инцидентов включает инциденты, которые не вошли в первые две категории. В общих чертах, эта категория инцидентов состоит из фактических несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети. Некоторые примеры технического несанкционированного доступа включают в себя:

– попытки извлечь файлы, содержащие пароли;

– атаки переполнения буфера с целью получения привилегированного (например, на уровне системного администратора) доступа к сети;

– использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;

– попытки повысить привилегии доступа к ресурсам или информации по сравнению с теми, которые пользователь или администратор уже имеют легитимно.

Инциденты несанкционированного доступа, создаваемые нетехническими средствами, которые приводят к прямому или косвенному раскрытию или модификации информации, к нарушениям учетности или неправильному использованию информационных систем, могут вызываться следующими факторами:

– разрушением физической защиты безопасности с последующим несанкционированным доступом к информации;

– неудачно и (или) неправильно сконфигурированной операционной системы по причине неконтролируемых изменений в системе, или неправильного функционирования программного или аппаратного обеспечения, приводящих к результатам, подобным тем, которые описаны в последнем абзаце подраздела 6.2, указанного выше.

7 Планирование и подготовка

Этап планирования и подготовки менеджмента инцидентов ИБ включает:

– документирование политики обработки и сообщений о событиях и инцидентах ИБ и соответствующей системы (включая родственные процедуры)

– создание подходящей структуры менеджмента инцидентов ИБ в организации и подбор соответствующего персонала;

– учреждение программы обучения и проведения инструктажа с целью обеспечения осведомленности.

После завершения этого этапа, организация полностью готова к надлежащей обработке инцидентов ИБ.

7.1 Обзор

Для результативного и эффективного ввода в эксплуатацию, после необходимого планирования необходимо выполнить ряд подготовительных действий. Эти действия включают в себя:

– формулирование и осуществление политики менеджмента инцидентов ИБ, а также получение от высшего руководства утверждения этой политики (см. раздел 7.2 ниже);

– определение и документирование подробной системы менеджмента инцидентов ИБ (см. подраздел 7.3 ниже).

Документация должна содержать следующие элементы:

- шкалу опасности для классификации инцидентов ИБ. Как указано в п. 4.2.1, такая шкала может состоять, например, из двух положений: "опасно" и "безопасно". В любом случае положение шкалы основано на фактическом или предполагаемом ущербе для бизнес-операций организации;
- формы отчетов[1)] о событиях[2)] и инцидентах[3)] ИБ (примеры форм даны в Приложении А), соответствующие документированные процедуры и действия связанные с корректными процедурами использования данных и системы, сервисов и (или) сетевого резервирования, планами непрерывности бизнеса;
- операционные процедуры для ГРИИБ с документированными обязанностями и распределением функций среди назначенных ответственных лиц[4)] для ведения различных видов деятельности, например таких как:
    - отключение пораженной системы, сервиса и (или) сети, при определенных обстоятельствах по согласованию с соответствующим руководством ИТ и (или) бизнеса и в соответствии с предварительным соглашением;
    - оставление пораженной системы, сервиса и (или) сети, находящейся в работающем состоянии;
    - ведение мониторинга потока данных, выходящих, входящих или находящихся в пределах пораженной системы, сервиса и (или) сети;

[1)] Если возможно, эти формы должны быть в электронной форме (например, на безопасной веб-странице) со ссылкой на базу данных, хранящую электронную информацию о событиях/инцидентах ИБ. В современном мире бумажная система требовала бы слишком много времени и была бы неэффективной.

[2)] Форма заполняется лицом, делающим сообщение (т.е. необязательно членом группы менеджмента инцидентов ИБ

[3)] Эта форма используется персоналом менеджмента инцидентов ИБ, заполняется первоначальной информацией о событии ИБ, содержит текущие записи оценки инцидента и пр. до полного разрешения инцидента. На каждой стадии в базу данных событий/инцидентов ИБ включаются обновления. Запись, сделанная в базе данных, содержащая "заполненную" форму или сведения о событиях/инцидентах ИБ, затем используется при расследовании инцидента.

[4)] В небольших организациях одно и тоже лицо может выполнять несколько ролей.

- активация нормальных действий и процедур планирования непрерывности бизнеса и резервирования согласно политике безопасности системы, сервиса и (или) сети;
- ведение мониторинга и поддержка безопасности хранения свидетельств в электронном виде на случай их востребования для судебного преследования или внутреннего дисциплинарного взыскания внутри организации;
- передача подробностей об инциденте ИБ сотрудникам своей организации и сторонним лицам или организациям;

– тестирование использования системы менеджмента инцидентов ИБ, ее процессов и процедур (см. п. 7.3.5, ниже);

– обновление политик менеджмента и анализа рисков ИБ, корпоративной политики ИБ, специальных политик ИБ для систем, сервисов и (или) сетей включая ссылки на менеджмент инцидентов ИБ для обеспечения регулярного анализа этих политик в контексте с выходными данными из системы менеджмента инцидентов ИБ (см. подраздел 7.4, ниже);

– создание ГРИИБ с соответствующей программой обучения для ее персонала (см. подраздел 7.5, ниже);

– технические и другие средства для поддержки системы менеджмента инцидентов безопасности ИБ (и деятельность ГРИИБ) (см. подраздел 7.6, ниже);

– проектирование и разработка программы обеспечения осведомленности о менеджменте инцидентов ИБ (см. подраздел 7.7, ниже), ознакомление с этой программой всего персонала организации (и повторное проведение ознакомления в дальнейшем в случае кадровых изменений).

В следующих подразделах описывается каждый вид этой деятельности, включая содержание каждого требуемого документа.

7.2 Политика менеджмента инцидентов информационной безопасности

7.2.1 Назначение

Политика менеджмента инцидентов ИБ предназначена для всех лиц, имеющих авторизованный доступ к информационным системам организации и относящимся к ним помещениям.

7.2.2 Аудитория

Политика менеджмента инцидентов ИБ должна быть утверждена высшим должностным лицом организации с подтвержденными документированными обязательствами, полученными от всего высшего руководства. Политика должна быть доступна для каждого работника и подрядчика и доведена в виде инструктажа и обучения с целью обеспечения осведомленности в области ИБ (см. подраздел 7.7, ниже).

7.2.3 Содержание

Политика менеджмента инцидентов ИБ должна отражать (содержать) следующие вопросы:

– значимость менеджмента инцидентов ИБ для организации, а также обязательств высшего руководства относительно поддержки менеджмента и его системы;

– обзор процедур обнаружения событий ИБ, оповещения и сбора соответствующей информации, и то, как эта информация должна использоваться для определения инцидентов ИБ. Этот обзор должен содержать перечень возможных типов событий ИБ, а

также информацию о том, как сообщать о них, что сообщать, где и кому, а также как обращаться с совершенно новыми типами событий ИБ;

– обзор оценки инцидентов ИБ, включая перечень ответственных лиц, что должно быть сделано, уведомление и дальнейшие действия;

– краткое изложение видов деятельности, следующих за подтверждением того, что некоторое событие ИБ является инцидентом ИБ. Они должны состоять из следующих видов:

- немедленная реакция;
- судебная экспертиза;
- передачи информации соответствующему персоналу или сторонними организациями;
- установление факта, что инцидент ИБ находится под контролем;
- последующие реакции;
- объявление "кризиса";
- критерии эскалации;
- установление ответственного лица (виновного);

– ссылки на необходимость правильной регистрации всех видов деятельности для последующего анализа и ведение непрерывного мониторинга для обеспечения безопасного хранения свидетельств в электронном виде на случай их востребования для судебного или дисциплинарного взыскания внутри организации;

– деятельность после разрешения инцидента ИБ, включая извлечение уроков и улучшение процесса, следующего за инцидентами ИБ;

– подробности хранения документации о системе, включая процедуры;

– обзор ГРИИБ, включающий следующие вопросы:

- структура ГРИИБ в организации и идентификация основного персонала, включая лиц, ответственных за:
  - краткое информирование высшего руководства об инцидентах;
  - проведение расследований и действия после объявления "кризиса" и т. п.;
  - связь со сторонними организациями (при необходимости);
- положение о менеджменте ИБ, область деятельности ГРИИБ и полномочия, в рамках которых она будет ее осуществлять. Как минимум, это положение должно включать в себя формулировку целевого назначения, определение сферы деятельности ГРИИБ и подробности об организаторе ГРИИБ и его полномочиях;

– формулировка целевого направления ГРИИБ, сфокусированная на основной деятельности группы. Чтобы стать группой реагирования на инциденты ИБ, группа должна участвовать в оценке инцидентов ИБ, реагировании на них и их управление, а также в их успешном разрешении. Особенно важны цели и назначение группы, для которых требуется четкое и однозначное определение:

– определение сферы деятельности ГРИИБ. Обычно в сферу деятельности ГРИИБ организации входят все информационные системы, сервисы и сети организации. В других случаях для организации может, по некоторым соображениям, потребоваться сужение сферы действия [ГРИИБ]. При этом необходимо четко документировать то, что входит и что не входит в сферу ее деятельности;

– личность организатора (старшее должностное лицо (член правления), старший руководитель), который санкционирует действия ГРИИБ и уровни полномочий, переданные ГРИИБ. Знание всего этого поможет всему персоналу организации понять предпосылки создания и структуру ГРИИБ, что и является жизненно важной информацией для построения доверия к ГРИИБ. Нужно заметить, что перед обнародованием этих деталей, необходимо проверить их на законность. В некоторых обстоятельствах раскрытие полномочий группы может послужить причиной появления претензий по нарушению обстоятельств;

– обзор программы обеспечения осведомленности и обучения менеджменту инцидентов ИБ;

– перечень правовых и нормативных аспектов, предполагаемых к рассмотрению (см. п. 5.2.3).

7.3 Система менеджмента инцидентов информационной безопасности

7.3.1 Назначение

Система менеджмента инцидентов ИБ предназначена для создания подробной документации, описывающей процессы и процедуры обработки инцидентов и оповещения (информирования) о таких инцидентах. Система менеджмента ИБ приводится в действие при обнаружении события ИБ. Она использует руководство для:

– реагирования на события ИБ;

– определения того, являются ли события ИБ инцидентами ИБ;

– менеджмент инцидентов ИБ до их завершения;

– извлечения уроков, а также внедрение необходимых улучшений системы и (или) безопасности в целом;

– реализации установленных улучшений.

7.3.2 Аудитория

Система менеджмента инцидентов ИБ предназначена для всего персонала организации, включая лиц, ответственных за:

– обнаружение и оповещение о событиях ИБ, которые могут быть служащими, состоящими в штате организации, или работающим по контракту;

– оценку и реагирование на события ИБ и инциденты ИБ, которые участвуют в извлечении уроков на этапе разрешения инцидентов ИБ и в улучшения ИБ и самой системы менеджмента инцидентов ИБ. Это члены группы обеспечения эксплуатации (или подобной группы), ГРИИБ, руководства, персонала отделов по связям с общественностью и юридических представителей.

Следует также учитывать пользователей сторонних организаций, которые сообщают об инцидентах ИБ и связанных с ними уязвимостях, и, кроме того, государственные и коммерческие организации, предоставляющие информацию об инцидентах ИБ и уязвимостях.

7.3.3 Содержание

Документация системы менеджмента инцидентов ИБ должна содержать:

– обзор политики менеджмента инцидентов ИБ;

– обзор системы менеджмента инцидентов ИБ в целом;

– детальные процессы и процедуры[1)], информацию о соответствующих сервисных программах и шкалах, связанных со следующим:

- на этапе "Планирование и подготовка":
  - с обнаружением и оповещением о появлении событий ИБ (человеком или автоматическими средствами);
  - со сбором информации о событиях ИБ;
  - с проведением оценки событий ИБ (включая эскалацию, если потребуется), используя согласованную шкалу опасности событий/инцидентов, и определением могут ли они изменить свою категорию на категорию инцидентов ИБ;
- на этапе "Использование" (когда инциденты ИБ подтверждены):
  - с оповещением сотрудников своей организации и сторонних лиц или организаций о наличии инцидентов ИБ или любых важных деталях, касающихся инцидентов;
  - с осуществлением немедленного реагирования, которое может включать активизацию процедур восстановления и (или) передачу сообщений соответствующему персоналу в соответствии с анализом и подтвержденными степенями шкалы опасности;
  - с проведением судебной экспертизы, при необходимости по степеням шкалы опасности инциденту ИБ, и изменение этих степеней, при необходимости;
  - с установлением факта контроля над инцидентами ИБ;
  - с выполнением дополнительных реакций, если требуется, включая те, что могут потребоваться позже (например, полное восстановление после нанесения ущерба после бедствия);
  - если инциденты ИБ не контролируются, то с реализацией антикризисных действий (например, с вызовом пожарной команды или активизацией плана непрерывности бизнеса);
  - с эскалацией дальнейшей оценки и (или) принятием дальнейших решений, если потребуется;
  - с обеспечением уверенности в том, что вся деятельность зарегистрирована, как положено, для последующего анализа;
  - с обновлением базы данных событий/инцидентов ИБ.

  (Документация системы менеджмента инцидентов ИБ должна обеспечивать возможность реагирования на инциденты ИБ как немедленно, так и по прошествии времени. В обоих случаях все инциденты ИБ должны оцениваться как можно раньше на предмет возможного негативного воздействия, (например, крупномасштабное бедствие может произойти через некоторое время после первого инцидента ИБ). Более того, некоторые виды реагирования могут быть необходимы для полностью непредвиденных инцидентов ИБ, когда требуются специальные защитные меры. Даже в такой ситуации в документации системы должны быть общие рекомендации действий, которые могут стать необходимы);

[1)] Организация может принимать решения, включать ли все процедуры в документацию системы, или все они или некоторые подробно изложены в дополнительных документах.

- на этапе "Анализ":
  - с проведением дальнейшей судебной экспертизы, если потребуется;
  - с идентификацией и документированием уроков, извлеченных из инцидентов ИБ;
  - с анализом и определением улучшений ИБ в результате полученных уроков;
  - с анализом состояния эффективности процессов и процедур реагирования на инциденты ИБ, оценки и восстановления после каждого инцидента ИБ и с определением улучшений системы менеджмента инцидентов ИБ в целом (как результат полученных уроков);
  - с обновлением базы данных событий/инцидентов ИБ;
- на этапе "Улучшение" – на основе полученных уроках, улучшать:
  - результаты анализа рисков ИБ и менеджмента ИБ;
  - систему менеджмента инцидентов ИБ (например, процессы и процедуры, форму оповещения (информирования) и (или) структуру организации);
  - общую безопасность, с внедрением новых и (или) улучшенных защитных мер;

– описание шкалы опасности событий/инцидентов (например, крупномасштабный, значительный, экстренный, незначительный, не экстренный) и соответствующее руководство;

– руководство для решения о необходимости развития эскалации в ходе каждого процесса, кто должен ее проводить и какими процедурами. Каждый, оценивающий событие или инцидент ИБ, должен знать на основе руководства из документации системы менеджмента инцидентов ИБ, когда при нормальных обстоятельствах необходимо переходить к эскалации для кого. Кроме того, возможны непредвиденные обстоятельства, когда это может стать также необходимостью. Например, инцидент ИБ минимальной опасности может развиться в значительную опасность или в "кризисную" ситуацию, если он неправильно обработан, или инцидент ИБ минимальной опасности, не обработанный в течение недели, может стать крупномасштабным инцидентом ИБ. В руководстве должны быть определены типы событий ИБ и инцидентов, типы развития и лица, которые могут проводить эскалацию;

– процедуры, которым необходимо следовать для того, чтобы все виды деятельности были зарегистрированы надлежащим образом в соответствующей форме и чтобы анализ журнала регистраций проводится назначенным персоналом;

– процедуры и механизмы поддержания режима контроля изменений, который включает в себя отслеживание событий и инцидентов ИБ, обновление отчета об инцидентах ИБ и обновление самой системы;

– процедуры судебной экспертизы;

– процедуры и руководство по использованию систем обнаружения вторжений (СОВ), обеспечивающие уверенность в том, что связанные с ними правовые и нормативные аспекты были учтены (см. п. 5.2.3). Руководство должно включать обсуждение преимуществ и недостатков действий по наблюдению за злоумышленником. Дополнительная информация по СОВ содержится в ИСО/МЭК ТО 15947 "Структура системы обнаружения вторжений в сфере ИТ" и ИСО/МЭК ТО 18043 "Рекомендации по выбору, развертыванию и эксплуатации систем обнаружения вторжений (СОВ) ";

– структура организации системы;

– компетенция и обязанности ГРИИБ в целом и отдельных ее членов;

– важная контактная информация.

7.3.4 Процедуры

Перед тем, как приступить к работе с системой менеджмента инцидентов ИБ, важно, иметь в наличие документированные и проверенные процедуры. В документе каждой процедуры должны указываться лица, ответственные за ее использование и менеджмент по обстановке: или из группы эксплуатационной поддержки и (или) из ГРИИБ. Такие процедуры должны включать процедуры обеспечения сбора и надежного хранения электронных свидетельств, что такое безопасное хранение непрерывно контролируются на случай судебного преследования или дисциплинарного взыскания внутри организации. Более того, должны существовать документированные процедуры, включающие в себя не только деятельность группы эксплуатационной поддержки и ГРИИБ, но и лиц, проводящих судебную экспертизу, и "кризисную" деятельность, если они не задействованы где-либо еще, например, в план непрерывности бизнеса. Очевидно, что эти документированные процедуры должны быть полностью соответствовать документированной политике менеджмента инцидентов ИБ и другой документации системы менеджмента инцидентов ИБ.

Важно понимать, что не все процедуры должны быть общедоступными. Например, нежелательно, чтобы весь персонал организации знал о работе ГРИИБ внутри организации, чтобы взаимодействовать с ней. ГРИИБ должна обеспечивать "общедоступное" руководство, включая информацию, полученную из результатов анализа инцидентов ИБ, которая находится в легкодоступной форме, например, в Интранете организации. Более того, может быть также важно не раскрывать некоторые детали системы менеджмента инцидентов ИБ, чтобы «инсайдер» (злоумышленник внутри организации) не мог вмешаться в процесс расследования. Например, если банковский служащий, который присваивает денежные средства, осведомлен о некоторых деталях системы, то он может лучше скрывать свою деятельность от расследователей или иным образом препятствовать обнаружению и расследованию или восстановлению после инцидента ИБ.

Содержание рабочих процедур зависит от многих критериев, особенно связанных с природой известных потенциальных событий и инцидентов ИБ, и типами затрагиваемых активов информационных систем и их средой. Так, некая рабочая процедура может быть связана с определенным типом инцидентов, или с типом продукции (например, межсетевые экраны, базы данных, операционные системы, приложения), или со специфической продукцией. В каждой рабочей процедуре должно быть четко определено, какие шаги должны быть предприняты и кем. Она должна отражать опыт, полученный как из внутренних, так и внешних источников (например, государственные или коммерческие КГБР, или аналогичные группы, а также поставщики).

Для обработки типов событий и инцидентов ИБ, должны существовать рабочие процедуры, которые уже известны. Необходимы также рабочие процедуры, которым надо следовать, когда тип обнаруженного инцидента или события неизвестен. В этом случае следует рассмотреть следующее:

– процесс оповещения для обработки таких "исключительных случаев";

– руководство, определяющее время для получения одобрения со стороны менеджмента, с целью избежания задержки реакции на инцидент;

– предварительно одобренное делегирование принятия решения без обычного процесса одобрения.

7.3.5 Тестирование системы

Для выявления потенциальных дефектов и проблем, которые могут возникнуть в процессе менеджмента событий и инцидентов ИБ необходимо запланировать регулярные проверки и тестирование процессов и процедур менеджмента инцидентов ИБ. Любые изменения, возникающие в результате анализа реакций, должны подвергаться строгой проверке и тестированию перед реализацией в практику.

7.4 Политики менеджмента рисков и информационной безопасности

7.4.1 Назначение

Целью включения содержания менеджмента инцидентов ИБ в общие политики менеджмента рисков и ИБ, и в специальные политики ИБ систем, сервисов и сетей является следующее:

- описание значимости менеджмента инцидентов ИБ, особенно, системы оповещения и обработки инцидентов ИБ;
- указать обязательства высшего руководства относительно необходимости надлежащей подготовки и реагированию на инциденты ИБ, т. е., относительно системы менеджмента инцидентов ИБ;
- обеспечение согласованность различных политик;
- обеспечить плановое, систематическое и спокойное реагирование на инциденты ИБ, тем самым, минимизируя негативное воздействие инцидентов.

7.4.2 Содержание

Общие политики менеджмента рисков и ИБ, и специальные политики ИБ для систем, сервисов или сетей должны обновляться с тем, чтобы они точно соответствовали общей политике менеджмента инцидентов ИБ и соответствующей системе. В соответствующие разделы необходимо включить обязательства высшего руководства и описание следующего:

- политики;
- процессов системы и соответствующей инфраструктуры;
- требования по обнаружению, оповещению, оценке и управлению инцидентами;

и четко обозначать персонал, ответственный за авторизацию и (или) проведение определенных значимых действий (например, за перевод информационной системы в режим off-line или даже отключение системы).

Кроме того, в политиках должно быть требование о создании соответствующих механизмов анализа для обеспечения использования любой информации, полученной в результате процессов обнаружения, мониторинга и разрешения инцидентов ИБ в качестве входных данных для обеспечения уверенности в непрерывности результативности общих политик менеджмента рисков ИБ, а также специальных политик ИБ для систем, сервисов и сетей.

7.5 Создание группы реагирования на инциденты информационной безопасности

7.5.1 Назначение

Целью создания ГРИИБ является выделение в организации подходящего персонала для оценки, реагирования на инциденты ИБ и извлечение уроков из них, а также для обеспечения необходимой координации, менеджмента, обратной связи и процесса пере-

дачи информации. ГРИИБ может внести вклад в снижение физического и финансового ущерба, а также снижение ущерба репутации организации, который иногда связан с инцидентами ИБ.

7.5.2 Члены группы реагирования на инциденты информационной безопасности и ее структура

Размер, структура и состав ГРИИБ должны соответствовать размеру и структуре организации. Хотя ГРИИБ может представлять собой изолированную группу или отдел, ее члены могут выполнять и другие обязанности, что способствует привлечению сотрудников из различных подразделений организации. Как говорилось в п.4.2.1 и п.7.1, во многих случаях ГРИИБ может быть действующей группой, возглавляемой старшим руководителем. Старшему руководителю оказывают помощь специалисты по конкретным вопросам, например, по отражению атак вредоносных программ, которые привлекаются в зависимости от типа инцидента ИБ. В зависимости от размера организации члены ГРИИБ могут также выполнять несколько ролей внутри ГРИИБ. В ГРИИБ могут также привлекаться служащие из различных частей организации (например, бизнеса, ИТ/телекоммуникаций, аудита, отдела кадров и маркетинга).

Члены группы должны быть доступны для контакта так, что имена членов и их заместителей и способ контакта с ними должны быть в организации ясными и доступными. Например, в документации системы менеджмента инцидентов ИБ должны быть точно указаны необходимые детали, включая любые документы по процедурам и формам отчетов, но не в изложениях политики.

Руководитель ГРИИБ должен:

– иметь право немедленно принимать решение о том, какие меры предпринять относительно инцидента;

– как правило, иметь специальную линию для оповещения высшего руководства, которая не отделена от обычных функций бизнеса;

– обеспечить необходимый уровень знаний и мастерства для всех членов ГРИИБ, а также необходимость его поддержания;

– поручать расследование каждого инцидента наиболее подходящему члену группы.

7.5.3 Отношения с другими подразделениями

Руководитель ГРИИБ и члены его группы должны обладать уровнем полномочий, позволяющим предпринимать необходимые действия, предположительно подходящие для реагирования на инцидент ИБ. Однако, действия, которые могут оказать неблагоприятное влияние на всю организацию в отношении финансов или репутации, должны согласовываться с высшим руководством. Поэтому важно уточнить соответствующий орган в отношении системы и политики менеджмента инцидентов ИБ, которого руководитель ГРИИБ оповещает о серьезных инцидентах ИБ.

Полномочия должны быть отражены в политике и в системе менеджмента инцидентов ИБ.

Процедуры и ответственности при общении со СМИ также должны быть согласованы с высшим руководством и документированы. Эти процедуры должны определять:

– кто в организации будет общаться с представителями средств массовой информации;

– как это подразделение организации будет взаимодействовать с ГРИИБ.

7.5.4 Отношения со сторонними лицами и организациями

Необходимо установить отношения между ГРИИБ и соответствующими сторонними лицами и организациями. К сторонним лицам и организациям могут относиться:

– сторонний вспомогательный персонал, работающий по контракту, например, из КГБР;

– ГРИИБ сторонних организаций, а также компьютерные группы быстрого реагирования на инциденты или КГБР;

– правоприменяющие организации;

– другие аварийные службы (например, пожарная бригада/отделение);

– соответствующие государственные организации;

– юридический персонал;

– официальные лица по связям с общественностью и (или) представителями СМИ;

– партнеры по бизнесу;

– потребители;

– общественность.

7.6 Техническая и другая поддержка

Быстрое и эффективное реагирование на инциденты ИБ будет достижимо гораздо легче, когда все необходимые технические и другие средства поддержки приобретены, подготовлены и протестированы. Это включает:

– доступ к деталям активов организации (предпочтительно иметь обновленный перечень активов) и информацию по их связям с функциями бизнеса;

– доступ к документированной стратегии непрерывности бизнеса и соответствующим планам;

– документированные и опубликованные процессы связей;

– использование электронной базы данных событий/инцидентов ИБ и технических средств для быстрого пополнения и обновления базы данных, анализа ее информации и упрощения реагирования (хотя общепризнанно, что иногда могут возникать случаи, когда сделанные вручную записи также оказываются востребованными или используются организацией);

– адекватные меры по обеспечению непрерывности бизнеса для базы данных событий/инцидентов ИБ.

Технические средства, используемые для быстрого пополнения и обновления баз данных, для анализа их информации и облегчения реагирования на инциденты ИБ, должны поддерживать:

– быстрое получение отчетов о событиях и инцидентах ИБ;

– уведомление ранее отобранного персонала (подходящих сторонних лиц) соответствующими средствами (например, через электронную почту, факс, телефон и т. д.), т. е., таким образом, запрашивая поддержку надежной контактной базы данных (которая должна быть всегда легкодоступной и должна включать бумажные и другие копии) и средство передачи информации безопасным способом там, где это необходимо;

– соблюдение предосторожностей, соответствующих оцененным рискам, избежание прослушивания электронной связи, реализуемой через Интернет или не через Интернет, во время атаки на систему, сервис и (или) сеть;

– соблюдение предосторожностей, соответствующих оцененным рискам, для сохранения доступности электронной связи, реализуемой через Интернет или не через Интернет, во время атаки на систему, сервис и (или) сеть;

– обеспечение сбора всех данных об информационной системе, сервисе и (или) сети и всех обрабатываемых данных;

– использование криптографического контроля целостности, если это соответствует оцененным рискам, для определения наличия изменений и какие части системы, сервиса и(или) сети и какие данные были изменены;

– упрощение архивирования и защиты собранной информации (например, применяя цифровые подписи к записям в журнале регистрации или другие свидетельства при хранении в режиме off-line на таких постоянных носителях, как CD или DVD ROM);

– подготовка распечаток (например, журналов регистрации), демонстрирующих развитие инцидента, процесс разрешения инцидента, и обеспечивающих сохранность информации;

– восстановление штатного режима работы информационной системы, сервиса и (или) сети с помощью:

- оптимальных процедур резервирования;
- четких и надежных резервных копий;
- тестирования резервных копий;
- контроля вредоносных программ;
- исходных носителей информации с системным и прикладным программным обеспечением;
- чистых, надежных и обновленных исправлений («патчей») для систем и приложений, согласованные с соответствующим планом непрерывности бизнеса.

Атакованная информационная система, сервис и (или) сеть могут функционировать неправильно. Поэтому, насколько это возможно и насколько это соизмеримо с оцененными рисками, никакое техническое средство (программное или аппаратное обеспечение), которое необходимо для реагирования на инцидент ИБ, не должно полагаться в своей работе на системы, сервисы и (или) сети, используемые в организации. По возможности, они должны быть полностью автономными.

Все технические средства должны быть тщательно отобраны, правильно внедрены и должны регулярно тестироваться (включая тестирование сделанных резервных копий).

Следует заметить, что технические средства, описанные в данном подразделе, не включают технические средства, используемые непосредственно для обнаружения инцидентов ИБ и вторжений, и для автоматического оповещения соответствующих лиц. Такие технические средства описаны в "Структуре IDS" (ТО 15947) и в ТО 13335, особенно в части 2, "Менеджмент безопасности информационных и коммуникационных технологий" (MICTS).

7.7 Обеспечение осведомленности и обучение

Менеджмент инцидентов ИБ – это процесс, который включает в себя не только технические средства, но также и людей, и, следовательно, этот процесс должен поддерживаться людьми, соответствующим образом обученными для работы в организации и осведомленными в вопросах безопасности информации.

Осведомленность и участие всего персонала организации очень важны для обеспечения успеха структурного подхода к менеджменту инцидентов ИБ. Поэтому роль ме-

неджмента инцидентов ИБ должна активно поддерживаться как часть общей программы обучения и обеспечения осведомленности в вопросах ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала, включая новых служащих, пользователей сторонних организаций и подрядчиков. Должна существовать специальная программа обучения для группы обеспечения эксплуатации, для членов ГРИИБ, а при необходимости, для персонала, ответственного за ИБ, и специальных администраторов. Следует заметить, что для каждой группы, непосредственно участвующей в менеджменте инцидентов, могут потребоваться различные уровни обучения, зависящие от типа, частоты и значимости их взаимодействия с системой менеджмента инцидентов ИБ.

Инструктажи, проводимые с целью обеспечения осведомленности, должны включать:

– основы работы системы менеджмента инцидентов ИБ, включая ее сферу действия и технологию работ по менеджменту инцидентов и событий ИБ;

– [инструкции] способ оповещения о событиях и инцидентах ИБ;

– защитные меры для обеспечения конфиденциальности источников, если это необходимо;

– соглашения об уровне сервиса системы;

– сообщение о результатах – при каких условиях будут информированы источники;

– любые ограничения, накладываемые соглашениями о неразглашении;

– полномочия организации менеджмента инцидентов ИБ и ее линия оповещения;

– кто и как получает отчеты от системы менеджмента инцидентов ИБ.

В некоторых случаях желательно специально включить подробности обеспечения осведомленности о менеджменте инцидентов ИБ в другие программы обучения (например, в программы ориентирования персонала или в общие корпоративные программы обеспечения осведомленности в вопросах ИБ). Этот подход к обеспечению осведомленности может обеспечить ценную информацию, связанную с определенными группами людей, и может улучшить эффективность и результативность программы обучения.

До ввода в эксплуатацию системы менеджмента инцидентов ИБ весь соответствующий персонал должен ознакомиться с процедурами обнаружения и оповещения о событиях ИБ, а избранный персонал должен быть очень компетентным в отношении последующих процессов. За этим должны последовать регулярные инструктажи для обеспечения осведомленности и курсы обучения. Обучение должно сопровождаться специальными упражнениями и тестированием членов группы обеспечения эксплуатации и ГРИИБ, а также персонала, ответственного за ИБ, и специальных администраторов.

8 Использование

8.1 Введение

Менеджмент инцидентов ИБ во время эксплуатации состоит из двух главных этапов: "Использование" и "Анализ", за которыми следует этап "Улучшение", когда осуществляются любые усовершенствования, идентифицированные в результате извлечения уроков из инцидентов ИБ. Эти этапы и связанные с ними процессы были представлены в подразделе 4.2. В данном разделе рассматривается этап "Использование", этап "Пересмотр" – в разделе 9, а этап "Улучшение" – в разделе 10. Эти три раздела и соответствующие процессы показаны на рисунке 2.

8.2 Обзор ключевых процессов

В этапе "Использование" ключевыми процессами являются:

– обнаружение события ИБ и оповещение о нем одним из членов персонала/заказчиком организации или автоматически, (например, сигналом тревоги от межсетевого экрана);

– сбор информации о событии ИБ и проведение первичной оценки персоналом[1)] группы обеспечения эксплуатации организации с целью определения, является ли событие инцидентом ИБ или ложным сигналом тревоги;

[1)] Не следует ожидать, что персонал группы обеспечения эксплуатации будет иметь квалификацию экспертов в сфере безопасности.

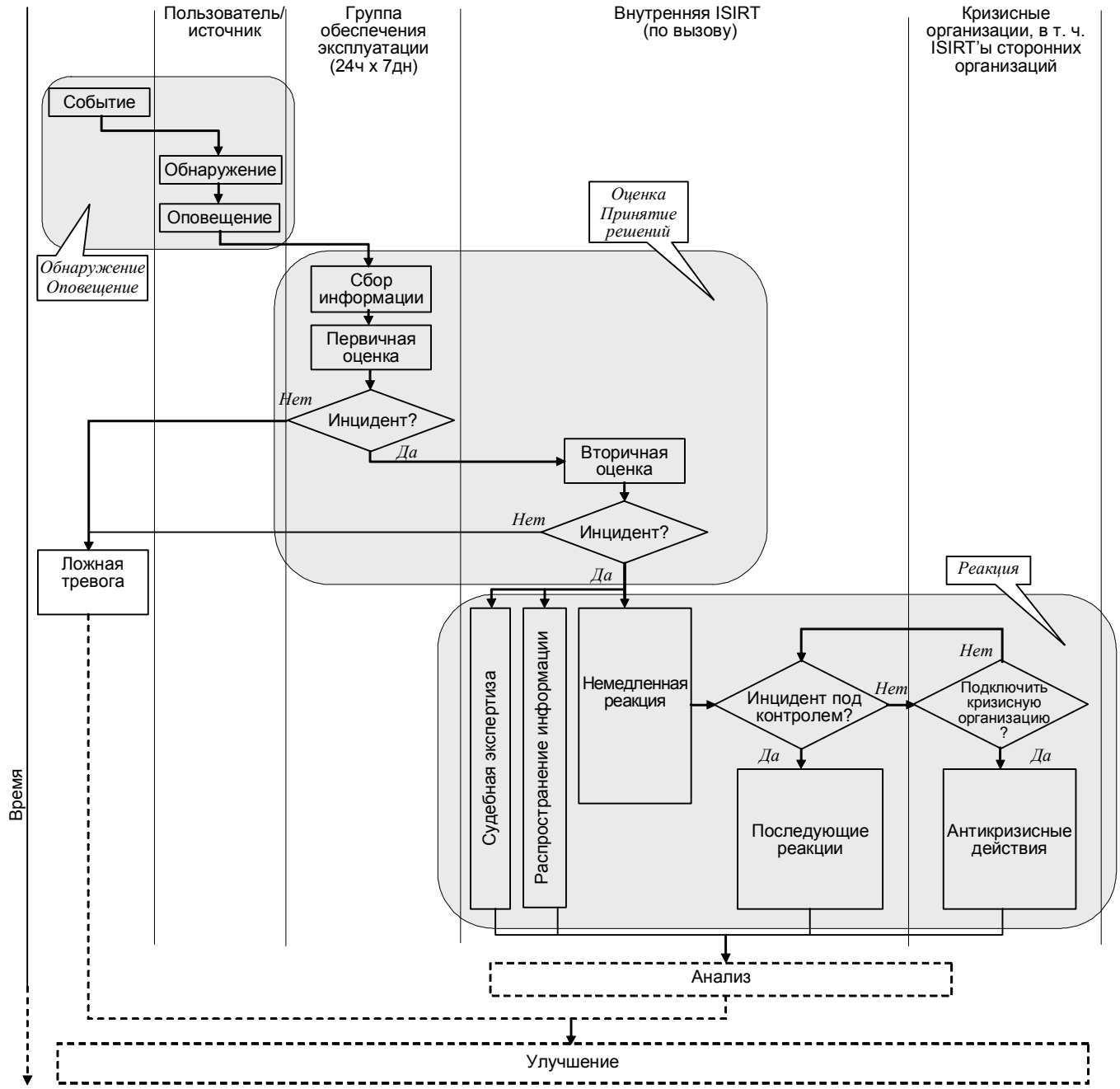

Рисунок 2 – Блок – схема последовательности операций обработки событий и инцидентов ИБ (процесс «Использование»)

– проведение вторичной оценки ГРИИБ с целью, во-первых, подтвердить, что событие является инцидентом ИБ, и если это так, то инициировать немедленную реакцию, а также начать необходимую судебную экспертизу и действия по передаче информации;

– анализ, выполняемый ГРИИБ с целью определения нахождения инцидента под контролем:

- при положительном варианте, инициируются дальнейшие необходимые реакции и обеспечивается готовность всей информации для действий по анализу последствий инцидента;
- при отрицательном ответе инициируются антикризисные действия с привлечением соответствующего персонала, например, руководителя и группы обеспечения непрерывности бизнеса организации;

– расширение дальнейших оценок и (или) принятия решений, проводимое в течение всего этапа по требованию;

– обеспечение надлежащей регистрации всеми причастными лицами, в особенности, членами ГРИИБ, всей деятельности для последующего анализа;

– обеспечение сбора и надежного хранения электронных свидетельств постоянного контроля за хранением этих свидетельств на случай судебного преследования по суду или внутреннего дисциплинарного взыскания;

– обеспечение поддержки режима контроля изменений, включающий в себя отслеживание инцидентов ИБ и обновления отчетов по инцидентам, с тем, чтобы база данных событий/инцидентов ИБ находилась в актуальном состоянии.

Вся собранная информация, касающаяся событий или инцидентов ИБ, должна храниться в базе данных событий/инцидентов ИБ, управляемой ГРИИБ. Информация, сообщаемая в течение каждого процесса, должна как можно более полной в любое время, чтобы обеспечить самую твердую основу для оценок и принятия решений, а также, естественно, для предпринимаемых действий.

После того, как событие ИБ было обнаружено и о нем было сообщено, целями следующих процессов будут являться:

– распределение ответственности за деятельность, связанную с менеджментом инцидентов, среди соответствующей иерархии персонала с оценкой, принятием решений и действиями, с привлечением персонала, как ответственного, так и не ответственного за безопасность;

– обеспечение формальных процедур, которым должно следовать каждое названное лицо, включая анализ и корректировку сделанных отчетов, оценку ущерба и оповещение соответствующего персонала (действия каждого лица зависят от типа и опасности инцидента);

– использование рекомендаций для тщательного документирования событий ИБ, а позднее, если событие будет отнесено к категории инцидентов ИБ, то и последующих действий и обновления базы данных событий/инцидентов ИБ.

Рекомендации:

– по обнаружению и оповещению о событиях ИБ дается в подразделе 8.3;

– по оценке и принятию решений (является ли событие инцидентом ИБ) дается в подразделе 8.4;

– по реагированию на инциденты ИБ дается в подразделе 8.5 и включает в себя:

- немедленные реакции;
- анализ с целью определения, находится ли инцидент ИБ под контролем;
- последующие реакции;
- антикризисные действия;
- судебную экспертизу;
- распространение информации;
- комментарий по вопросам эскалации;
- регистрацию деятельности.

8.3 Обнаружение и оповещение

События ИБ могут быть обнаружены непосредственно неким лицом или лицами, заметившими нечто, являющееся причиной беспокойства, и имеющее технический, физи-

ческий или процедурный характер. Обнаружение может осуществляться, например, детекторами огня/дыма или с помощью охранной сигнализации, путем передачи сигналов тревоги в заранее определенные места (для осуществления человеком определенных действий). Технические события ИБ могут обнаруживаться автоматически, например, сигналы тревоги, производимые устройствами анализа записей аудита, межсетевыми экранами, системами обнаружения вторжений, антивирусными программами, в каждом случае с заранее установленными параметрами.

Какой бы ни была причина обнаружения события ИБ, лицо, заметившее нечто необычное или оповещенное автоматическими средствами, несет ответственность за начало процесса обнаружения и оповещения. Это может быть любой член персонала организации, работающий постоянно или по контракту. Это лицо должно следовать процедурам и использовать форму отчета о событиях ИБ, определенную системой менеджмента инцидентов ИБ, чтобы привлечь внимание, прежде всего, группы обеспечения эксплуатации и менеджмента. Таким образом, существенно важно, чтобы весь персонал был ознакомлен и имел доступ к рекомендациям, касающимся оповещения сообщения о возможных событиях ИБ различных типов, включая формы отчета и подробности о персонале, который должен оповещаться в каждом случае. (Важно, чтобы весь персонал, по крайней мере, был осведомлен о форме отчета, что способствовало бы его пониманию системы менеджмента инцидентов ИБ).

Обработка события ИБ зависит от того, что оно собой представляет, а также от последствий и воздействий, которые могут являться его результатом. Для многих людей принятие такого решения будет находиться за пределами их компетентности. Поэтому лицо, сообщающее о событии ИБ, должно заполнить форму отчета так, чтобы сообщить как можно больше информации, доступной ему в тот момент, при необходимости, связываясь со своим руководителем. Предпочтительно, чтобы эта форма была в электронном виде (например, в представлении электронной почты или web), чтобы ее можно было передать безопасным образом в надлежащую группу обеспечения и эксплуатации (работающую, предпочтительно 24 часа в сутки по 7 дней в неделю), а копию сообщения – руководителю ГРИИБ. Пример формы отчета сообщения о событии ИБ приводятся в Приложении А.

Следует подчеркнуть, что при заполнении отчетной формы важны не только точность, но и своевременность. Задерживать представление формы отчета о событии ИБ по причине уточнения ее содержания является плохой практикой. Если сообщающее лицо не уверено в данных какого-либо поля в форме отчета, то она должна быть представлена с соответствующей пометкой, а уточнение можно прислать позже. Также следует признать, что некоторые механизмы электронного оповещения (например, электронная почта) сами являются очевидными целями атаки.

Если существуют проблемы или считается, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например, с электронной почтой), включая случаи, когда считается возможным, что если система подвергается атаке, и формы отчета могут считываться несанкционированными лицами, то тогда должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть на́рочные, телефон, текстовые сообщения. Такие альтернативные средства должны использоваться особенно тогда, когда на ранних стадиях исследования становится очевидно, что событие ИБ, по всей вероятности, будет переведено в категорию инцидента ИБ, особенно инцидента, который может быть значительным.

Следует заметить, что хотя в большинстве случаев о событии ИБ должна сообщать группа обеспечения эксплуатации для дальнейших действий; могут быть случаи, когда событие ИБ может быть обработано на месте происшествия с помощью местного руководства. Событие ИБ можно быстро распознать как ложную тревогу или можно разрешить,

придя к удовлетворительному результату. В этих случаях форма отчетов должна быть заполнена и отправлена местному руководству, а также группе обеспечения эксплуатации и ГРИИБ с целью регистрации, т. е., в базу данных событий/инцидентов ИБ. В этом случае лицо, сообщающее о завершении события ИБ, должно иметь право внести некоторую информацию, требуемую для заполнения формы отчета об инцидентах ИБ. В этом случае такая форма отчета об инциденте должна быть заполнена и отправлена по инстанции.

8.4 Оценка и принятие решений относительно событий/инцидентов

8.4.1 Первичная оценка и предварительное решение

В группе обеспечения эксплуатации принимающее лицо должно подтвердить получение заполненной формы отчета, ввести ее в базу данных событий/инцидентов ИБ и проанализировать ее. Далее оно должно попытаться получить любые уточнения от сообщившего о событии ИБ и собрать любую дополнительную информацию, требуемую и считающуюся доступной, как от сообщившего, так и от других лиц. Затем, представитель группы обеспечения эксплуатации должен провести оценку и определить, подходит ли это событие под категорию инцидента ИБ или является ложной тревогой. Если событие ИБ определяется как ложная тревога форму необходимо заполнить и передать ГРИИБ для записи в базу данных и дальнейшего анализа, а также для создания копии для сообщившего лица и его/ее местного руководителя.

Информация и другие свидетельства, собранные на этом этапе, могут потребоваться в будущем для дисциплинарного или судебного разбирательства. Лицо или лица, выполняющие задачи сбора и оценки информации, должны быть обучены выполнению требований, касающихся сбора и сохранения свидетельств.

Дополнительно к дате(ам) и времени действий необходимо полностью документировать следующее:

- то, что было увидено и сделано (включая использованные средства) и почему;
- место положения хранения свидетельства (доказательства);
- то, как свидетельство архивировано (если это необходимо);
- как была выполнена верификация свидетельства (если это необходимо);
- детали хранения материалов и последующего доступа к ним.

Если событие ИБ определено как вероятный инцидент ИБ, а сотрудник группы обеспечения эксплуатации имеет соответствующий уровень компетентности, то может проводиться дальнейшая оценка. В результате могут потребоваться корректирующие действия, например, идентификация дополнительных "аварийных" защитных мер и обращение за помощью в их реализации к соответствующему лицу. Может оказаться так, что событие ИБ будет определено как инцидент ИБ, причем значительный (по шкале опасности, принятой в организации), необходимо проинформировать непосредственно руководителя ГРИИБ. Может быть очевидной, необходимость объявления "кризисной ситуации", и, следовательно, надо сообщить, например, руководителю непрерывности бизнеса в целях возможной активизации плана непрерывности бизнеса; руководитель ГРИИБ и высшее руководство должны быть также проинформированы об этом. Однако, наиболее вероятна ситуация, когда инцидент ИБ "передается" непосредственно ГРИИБ для дальнейшей оценки и выполнения соответствующих действий.

Каким бы ни был определен следующий шаг, сотрудник группы обеспечения эксплуатации должен заполнить форму отчета по возможности наиболее подробно. Пример, формы отчета по инциденту ИБ приводится в Приложении А. Форма отчета должна со-

держать информацию в описательном виде, где, по возможности, необходимо подтверждать и характеризовать следующее:

- что представляет собой инцидент ИБ;
- что явилось его причиной, чем или кем он был вызван;
- на что он влияет или может повлиять;
- воздействие или потенциальное воздействие инцидента ИБ на бизнес организации;
- указание на вероятную значительность или незначительность инцидента ИБ (по шкале опасности, принятой в организации);
- как он обрабатывался до этого времени.

При рассмотрении потенциального или фактического негативного воздействия на бизнес организации инцидента типа:

- неавторизованное раскрытие информации;
- неавторизованная модификация информации;
- отказа от информации;
- недоступности информации и(или) сервиса;
- уничтожение информации и(или) сервиса

в первую очередь необходимо определить, какая из нижеследующих категорий имеет отношение к делу.

Примерными категориями потерь являются:

- финансовые потери/прерывание бизнес-операций;
- коммерческие и экономические интересы;
- информация, содержащая персональные данные;
- правовые и нормативные обязательства;
- менеджмент и бизнес-операции;
- потеря престижа организации.

Для категорий, которые сочтены значимыми, должны использоваться соответствующие рекомендацию по определению (см. Приложение В) потенциальных или фактических воздействий для внесения их в отчет по инцидентам ИБ.

Если инцидент ИБ был разрешен, то отчет должен содержать детали предпринятых защитных мер и любых извлеченных уроков (например, защитные меры, которые должны быть приняты для предотвращения повторного появления инцидента или подобных инцидентов).

После наиболее подробного заполнения, по мере возможности, форма отчета, должна быть представлена ГРИИБ для ввода в базу данных инцидентов и событий ИБ и анализа в будущем.

Если расследование продолжается больше недели, то должен быть составлен промежуточный отчет.

Подчеркивается, что сотрудник группы обеспечения эксплуатации, оценивающий инцидент ИБ, основываясь на руководстве, содержащемся в документации системы менеджмента инцидентов ИБ, должен быть осведомлен о следующем:

- когда и кому необходимо направлять материалы;
- что при всех действиях, выполняемых группой обеспечения эксплуатации, необходимо следовать документированным процедурам контроля изменений.

Если существуют проблемы или считается, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например, с электронной почтой), включая случаи, когда считается возможным, что если система подвергается атаке, и формы отчета могут считываться несанкционированными лицами, то тогда должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть на́рочные, телефон, текстовые сообщения. Такие средства должны использоваться особенно тогда, когда оказывается, что инцидент ИБ является значительным.

8.4.2 Вторичная оценка и подтверждение инцидента

Вторичная оценка, а также подтверждение или какое-либо другое решение, относительно того, можно ли категорировать событие ИБ как инцидент ИБ, должны входить в обязанности ГРИИБ. Принимающее лицо в ГРИИБ должно:

– зарегистрировать прием формы отчета, заполненной, по возможности наиболее подробно, группой обеспечения эксплуатации;

– ввести эту форму в базу данных событий/инцидентов ИБ;

– обратиться за уточнениями к группе обеспечения эксплуатации;

– проанализировать содержание отчетной формы;

– собрать любую нужную информацию, которая требуется и доступна, от группы обеспечения эксплуатации, от лица, заполнившего отчетную форму о событии ИБ или откуда-либо еще.

Если все еще остается некая неопределенность относительно аутентичности инцидента ИБ или полноты полученной информации, то сотрудник ГРИИБГРИИБ должен провести вторичную оценку для определения того, является ли инцидент реальным или это ложная тревога. Если инцидент ИБ определен как ложная тревога, отчет о событии ИБ должен быть завершен, добавлен в базу данных событий/инцидентов ИБ и передан руководителю ГРИИБ. Копии отчета должны быть посланы группе обеспечения эксплуатации, лицу, сообщившему о событии, и его/ее местному руководителю.

Если инцидент ИБ определяется как реальный, то сотрудник ГРИИБ, при необходимости привлекая коллег, должен провести дальнейшую оценку. Целью оценки является максимально быстрое подтверждение:

– что представляет собой инцидент ИБ, что явилось его причиной, чем или кем он был вызван, на что он повлиял или мог повлиять, воздействие или потенциальное воздействие инцидента ИБ на бизнес организации, указание на вероятную значительность/незначительность инцидента (по шкале опасности, принятой в организации);

– в отношении намеренной технической атаки [злоумышленника] на некоторую информационную систему, сервис и (или) сеть, например:

- как глубоко проник нарушитель в систему, сервис и (или) сеть и какой уровень контроля он имеет;
- к каким данным получил доступ нарушитель, были ли они скопированы, изменены или разрушены;
- какое программное обеспечение было скопировано, изменено или разрушено нарушителем;

– в отношении намеренной физической атаки нарушителя на любую информационную систему аппаратной части, сервиса и (или) на сеть, и (или) на физическое место расположение, например:

- каковы прямой и косвенный эффекты от нанесенного физического ущерба (безопасность физического доступа не существует?);

– в отношении инцидентов ИБ, косвенно созданных действиями человека, прямой и косвенный эффекты (например, стал ли физический доступ возможным по причине пожара, уязвимость информационной системы является следствием неправильного функционирования программного обеспечения, линии связи или ошибки оператора);

– как обрабатывался инцидент ИБ до сих пор.

При анализе потенциального или фактического негативного влияния инцидента ИБ на бизнес организации вследствие:

– несанкционированного раскрытия информации;

– несанкционированной модификации информации;

– отказа от информации;

– недоступности информации и (или) сервиса;

– разрушения информации и (или) сервиса,

необходимо подтвердить, какие последствия имели место. Примерные категории:

– финансовые потери/разрушение бизнес-операций;

– коммерческие и экономические интересы;

– информация, содержащая персональные данные;

– правовые и нормативные обязательства;

– менеджмент и бизнес-операции;

– потеря престижа организации.

Заполняющие формы отчета должны использовать рекомендации соответствующей категории (см. Приложение В) при оценке потенциальных или фактических воздействий для внесения их в отчет по инцидентам ИБ.

8.5 Реакция на инциденты

8.5.1 Немедленная реакция

8.5.1.1 Обзор

В огромном большинстве случаев следующей деятельностью сотрудника ГРИИБ является определение действий при немедленной реакции на инцидент ИБ, запись деталей в форму отчета по этому инциденту и в базу данных событий/инцидентов ИБ, а также указание о требуемых действиях соответствующим лицам и группам. Результатом может быть принятие аварийных защитных мер (например, отключение/закрытие пораженной информационной системы, сервиса и (или) сети после согласования с соответствующим ИТ и (или) бизнес-руководством и (или) определение дополнительных постоянных защитных мер и уведомления о действиях надлежащих лиц и групп. Если это еще не выполнено, то нужно определить значимость инцидента ИБ по шкале опасности, принятой в организации, и если опасность значительная, то об этом должно быть уведомлено непосредственно соответствующее высшее руководство. Если очевидно, что должна быть объявлена "кризисная ситуация", то, например руководитель, отвечающий за непрерывность бизнеса, должен быть оповещен о возможной активизации плана непрерывности бизнеса, причем необходимо проинформировать руководителя ГРИИБ и высшее руководство.

8.5.1.2 Примерные действия

Примером действий, связанных с немедленной реакцией в случае намеренной атаки на информационную систему, сервис и (или) сеть может быть: оставление их подключенными к Интернету и другим сетям с целью:

– позволить значимым приложениям бизнеса функционировать правильно;

– собрать о злоумышленнике как можно больше информации, при условии, что он (она) не знает, что находится под наблюдением.

Однако, при принятии такого решения, нужно учесть следующие факторы:

– злоумышленник может почувствовать, что находится под наблюдением, и может предпринять действия, наносящие дальнейший ущерб пораженной системе, сервису и (или) сети и данным;

– нарушитель может разрушить информацию, которая может быть полезной для его отслеживания.

Важно, чтобы было технически возможно быстро и надежно отключить и (или) закрыть атакованную информационную систему, сервис и (или) сеть, если решение об этом будет принято. Однако должны быть внедрены соответствующие средства аутентификации, с тем, чтобы это не могли сделать неавторизованные лица.

Следующее соображение заключается в том, что предотвращение повторного проявления инцидента обычно имеет большую важность, и всегда можно было сделать вывод о том, что нарушитель выявил слабое место, которое должно быть устранено, и. выгоды отслеживания нарушителя не оправдывают затраченных на это усилий. Это особенно справедливо, когда нарушитель на самом деле не является таковым, и не нанес большого, или вообще никакого ущерба.

Что касается инцидентов ИБ, которые были вызваны чем-то другим, кроме намеренной атаки, то их источник должен быть идентифицирован. Может оказаться необходимым отключить информационную систему, сервис и (или) сеть или изолировать соответствующую часть и отключить ее, получив предварительно согласие соответствующего руководства ИТ и (или) бизнеса, на время внедрения защитных мер. На это может потребоваться много времени, если слабое место окажется значительным для структуры информационной системы, сервиса и (или) для сети, или если слабое место окажется критической.

Другой реакцией может быть активизация методов наблюдения (например, "приманки", "горшки с медом", см. ТО18043). Это должно осуществляться на основе процедур, документированных для системы менеджмента инцидентов ИБ.

Информация, которая могла быть повреждена инцидентом ИБ, должна быть проверена членом ГРИИБ по резервным записям на предмет изменения, стирания или вставок в информацию. Может оказаться необходимым проверить целостность журналов регистрации, поскольку осмотрительный нарушитель может подделать их с целью сокрытия своих следов.

8.5.1.3 Обновление информации об инцидентах

Каким бы ни был следующий шаг, сотрудник ГРИИБ должен обновить отчет об инциденте ИБ как можно в большем объеме, добавить его в базу данных событий/инцидентов ИБ и, при необходимости, оповестить руководителя ГРИИБ и других лиц. Обновляться может следующая информация:

– что представляет собой инцидент ИБ;

– что явилось его причиной, чем или кем он был вызван;

– на что он воздействует или мог воздействовать;

– фактическое воздействие или потенциальное воздействие инцидента ИБ на бизнес организации;

– изменения в указании на вероятную значительность или незначительность инцидента ИБ (по шкале опасности, принятой в организации);

– как он обрабатывался до этого времени.

Если инцидент ИБ разрешен, то отчет должен содержать детали предпринятых защитных мер и любых извлеченных уроков (например, дополнительные защитные меры, которые следует предпринять для предотвращения повторного появления данного инцидента или подобных инцидентов). Обновленный отчет следует добавить в базу данных событий/инцидентов и уведомить руководителя ГРИИБ и других лиц, по требованию.

Подчеркивается, что ГРИИБ отвечает за обеспечение безопасного хранения всей информации, относящейся к данному инциденту ИБ, с целью проведения дальнейшего анализа и возможно принимаемого судом в качестве доказательства. Например, для инцидента ИБ, ориентированного на ИТ, после первичного обнаружения инцидента все непостоянные данные должны быть собраны до того, как пораженная система ИТ, сервис и (или) сеть будут закрыты для полного судебного расследования. Собранная информация включает в себя содержимое контанта памяти, кэша и регистров, детали любых функционирующих процессов и:

– в зависимости от характера инцидента ИБ необходимо полное дублирование пораженной системы, сервиса и (или) сети на случай судебного разбирательства, или резервное копирование низкого уровня журналов и важных файлов;

– необходимо собрать и проанализировать журналы соседних систем, сервисов и (или) сетей, например, маршрутизаторов и межсетевых экранов;

– вся собранная информация должна храниться безопасным образом на носителе только для чтения;

– при выполнении дублирования на случай судебного разбирательства должны присутствовать не менее двух лиц, для заявления и подтверждения, что все действия были проведены согласно соответствующему нормативному законодательству;

– необходимо документировать и хранить вместе с исходными носителями информации и описания сервисных команд, использованных для выполнения внешнего дублирования.

Член ГРИИБ также является ответственным, если это возможно на данной стадии, за возврат пораженных устройств (имеющих или не имеющих отношение к ИТ) в безопасное рабочее состояние, которое не подвержено компрометации той же самой атаки.

8.5.1.4 Дальнейшие действия

Если член ГРИИБ определяет реальность инцидента ИБ, то дополнительными важными действиями должны быть следующие:

– проведение судебной экспертизы;

– информирование лиц, ответственных за передачу информации внутри организации и за ее пределами о фактах и предложениях о том, что надо передать.

После, по возможности, наиболее подробного заполнения отчета об инциденте ИБ он должен быть введен в базу данных событий/инцидентов ИБ и передан руководителю ГРИИБ.

Если расследование продолжается дольше установленного периода времени, в этом случае составляется промежуточный отчет.

Член ГРИИБ, оценивающий инцидент ИБ, на основании руководства, содержащегося в документации системы менеджмента инцидентов ИБ, должен знать:

- когда и кому необходимо направлять материалы;
- при осуществлении какой-либо деятельности ГРИИБ необходимо следовать документированным процедурам контроля изменений.

Если существуют проблемы или считается, что они существуют с обычными устройствами связи (например, с электронной почтой), включая случаи, когда система, возможно, подвергается атаке, и:

- принято решение, что инцидент ИБ является значительным; и (или)
- определена "кризисная ситуация",

то тогда следует перейти на аварийный режим и, в первую очередь, сообщить об инциденте ИБ ответственным лицам лично по телефону или текстовым сообщением.

При необходимости, руководитель ГРИИБ, вместе с руководителем ИБ организации и соответствующим старшим руководителем/членом правления должны связаться со всеми соответствующими лицами, как внутри организации, так и за пределами (см. п.п. 7.5.3 и 7.5.4).

Для быстрой и эффективной организации связи, необходимо заранее установить надежный метод передачи информации, не зависящий полностью от системы, сервиса или сети, на которые может воздействовать инцидент ИБ. Эти меры предосторожности могут включать назначение резервных консультантов или представителей на случай отсутствия кого-либо из основных руководителей.

8.5.2 Находится ли инцидент под контролем?

После того, как член ГРИИБ инициировал немедленную реакцию, соответствующую судебную экспертизу и деятельность по передаче информации, необходимо быстро убедиться, находится ли инцидент ИБ под контролем. При необходимости, член ГРИИБ может проконсультироваться с коллегами, руководителем ГРИИБ и (или) другими лицами или группами.

Если, подтверждается, что инцидент ИБ, находится под контролем, то член ГРИИБ должен перейти к другим необходимым дальнейшим действиям по реагированию, судебной экспертизе и передаче информации (см. п.п. 8.5.3, 8.5.5 и 8.5.6), чтобы привести инцидент ИБ к завершению и восстановить нормальную работу пораженной информационной системы.

Если не подтверждается, что инцидент ИБ находится под контролем, член ГРИИБ должен инициировать "антикризисные" действия (см. п. 8.5.4 ниже).

8.5.3 Последующая реакция

Определив, что инцидент ИБ находится под контролем и не является объектом "антикризисной ситуации", член ГРИИБ должен определить нужны ли дальнейшие реакции в отношении данного инцидента, и какие, если они потребуются. Это может включать в себя восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Затем член ГРИИБ должен(на) занести детали в форму отчета инцидента ИБ и базу данных событий/инцидентов ИБ, а также проинформировать ответственных за завершение соответствующих действий. После успешного завершения этих действий, детали должны быть занесены в форму отчета этого инцидента ИБ и в базу данных событий/инцидентов ИБ, а затем инцидент должен быть закрыт, и соответствующий персонал должен быть проинформирован об этом.

Некоторые реакции должны быть направлены на предотвращение повторения или появления подобного инцидента ИБ. Например, если определено, что причиной инцидента ИБ является отказ аппаратурной части или программы обеспечения ИТ, из-за отсутствия установленных необходимых исправлений ("патчей"), то в этом случае необходимо немедленно связаться с поставщиком. Если причиной инцидента ИБ была известная уязвимость ИТ, то она должна быть устранена соответствующим обновлением ИБ. Любые проблемы, связанные с конфигурацией ИТ и выявленные инцидентом ИБ, должны быть решены. Другими мерами снижения возможности повторения или появления подобного инцидента ИБ могут быть изменение системных паролей и отключение неиспользуемых сервисов.

Другая деятельность по реагированию может включать в себя мониторинг системы, сервиса и (или) сети ИТ. После оценки инцидента ИБ может оказаться целесообразным ввести дополнительные защитные меры мониторинга для содействия в обнаружении необычных или подозрительных событий, которые могут быть симптомами последующих инцидентов ИБ. Такой мониторинг может также вскрыть инцидент ИБ на бóльшую глубину и идентифицировать другие системы ИТ, которые были скомпрометированы.

Может возникнуть необходимость в документировании в соответствующем плане непрерывности бизнеса активизацию специальных реакций. Это применимо к инцидентам ИБ, как связанным, так и не связанным с ИТ. Такие реакции должны предусматриваться для всех аспектов бизнеса, не только непосредственно связанных с ИТ, но также связанных и с поддержкой ключевых функций бизнеса и последующего восстановления, включая голосовые телекоммуникации, а также кадровые вопросы и физические устройства.

Последней областью деятельности является восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Восстановление пораженных систем(ы), сервисов(а) и (или) сетей(и) до безопасного рабочего состояния может быть достигнуто путем применения "патчей" для известных уязвимостей или отключением скомпрометированных элементов. Если по причине уничтожения журналов регистрации инцидентом ИБ становится неизвестным полный объем инцидента, тогда может потребоваться полная перестройка системы, сервиса и (или) сети. Также может потребоваться активизация части соответствующего плана непрерывности бизнеса.

Если инцидент ИБ не связан с ИТ, например, спровоцирован пожаром, наводнением или взрывом, то выполняются действия по восстановлению, соответствующие действиям, документированным в соответствующем плане непрерывности бизнеса.

8.5.4 "Антикризисные действия"

Как обсуждалось в п. 8.5.2, может случиться так, что когда ГРИИБ будет определять, контролируется ли инцидент ИБ, то может оказаться, что инцидент ИБ не находится под контролем и должен обрабатываться в режиме "антикризисные действия", при котором используется предварительно разработанный план.

Лучшие варианты обработки всех возможных типов инцидентов ИБ, которые могут повлиять на доступность/разрушение и, до некоторой степени, на целостность информационной системы, идентифицироваться в стратегии непрерывности бизнеса организации. Эти варианты должны быть непосредственно связаны с приоритетами бизнеса организации и соответствующими временными рамками восстановления, и, следовательно, с максимально приемлемым временем простоя для ИТ, речевой связи, персонала и размещения. В стратегии должны быть определены следующие необходимые факторы:

– предупреждающие, поддерживающие меры обеспечения непрерывности бизнеса и устойчивости к внешним изменениям;

– организационная структура и обязанности, связанные с управлением планирования непрерывности бизнеса;

– структура и основные положения плана (планов) непрерывности бизнеса.

План (планы) непрерывности бизнеса и защитные меры для поддержки активизации этого(их) плана(ов), протестированных и признанных удовлетворительными, создают основу для ведения наиболее "кризисных" действий, для которых они предназначены.

Другие типы возможных "антикризисных действий" включают, но не ограничиваются, активизацией:

– средств пожаротушения и процедур эвакуации;

– средств предотвращения наводнения и процедур эвакуации;

– средств избежания взрыва бомбы и соответствующих процедур эвакуации;

– работы специалистов по расследованию мошенничества в информационных системах;

– работы специалистов по расследованию технических атак.

8.5.5 Судебная экспертиза

Если при предыдущей оценке было определено, что в доказательных целях требуется судебная экспертиза – фактически в контексте значимого инцидента ИБ, судебная экспертиза проводится ГРИИБ. В экспертизе необходимо использовать следственные методы и средства, основанные на ИТ и поддерживаемые документированные процедурами, с целью проведения более подробного анализа определенного инцидента ИБ, чем это было сделано ранее в процессе менеджмента инцидентов ИБ. Такой анализ должен проводиться структурным образом и идентифицировать то, что может быть использовано как свидетельство для внутренних дисциплинарных процедур или для судебных процессов.

Средства, необходимые для проведения судебной экспертизы, могут категорировать технические (например, средства аудита, средства восстановления свидетельств), процедурные, кадровые средства и защищенные судебные помещения. Каждое действие судебной экспертизы должно быть полностью документировано, включая соответствующие фотографии, отчеты об анализе следов аудита, журналы восстановления данных. Квалификация лица или лиц, проводящих судебную экспертизу, должна документироваться наряду с результатами квалификационного тестирования. Любая другая информация, которая может продемонстрировать объективность и логический характер экспертизы, также должна документироваться. Все записи, и о самих инцидентах ИБ, и о деятельности, связанной с судебной экспертизой, и т. д., и соответствующие носители информации должны храниться в физически защищенной среде и контролироваться процедурами так, чтобы к ним был невозможен доступ неавторизованных лиц с целью модификации или создания недоступности данных. Средства судебной экспертизы, основанные на ИТ, должны отвечать стандартам, чтобы их точность не могла быть оспорена в судебном порядке, и, конечно, они должны поддерживаться в актуальном состоянии, учитывая изменения в технологии. Физическая среда ГРИИБ должна создавать доказуемые условия, которые гарантируют такую обработку свидетельств, которая не может быть оспорена. Очевидно, что должно быть достаточное количество персонала, если необходимо по вызову обеспечивать реагирование в любое время.

Со временем, несомненно, возникнут требования анализа свидетельств в контексте многообразия инцидентов ИБ, включая мошенничество, кражу и вандализм. Следовательно, для содействия ГРИИБ потребуется большое количество средств, основанных на ИТ, и вспомогательным процедурам для вскрытия информации, "спрятанной" в информационной системе, сервисе и(или) сети, включая информацию, которая, на первый взгляд,

кажется стертой, зашифрованной или поврежденной. Эти средства должны учитывать все известные аспекты, связанные с известными типами инцидентов ИБ (и конечно, они должны быть документированными в процедурах ГРИИБ).

В современных условиях для судебной экспертизы часто требуется охват с сетевой структурой, в которой расследование должно охватывать всю операционную среду, включая множество серверов (файловый, печати, связи, электронной почты и т. д.), а также средства удаленного доступа. Имеется много инструментов, включая средства поиска текстов, программное обеспечение изображений и пакеты программ для судебной экспертизы. Подчеркивается, что главной целью процедур судебной экспертизы является сохранение свидетельства в неприкосновенности и его проверке на предмет противостояния любым оспариванием в суде и, что судебная экспертиза должна выполняться на точной копии исходных данных, чтобы избежать сомнений в исходной целостности носителей в ходе аналитической работы.

Общий процесс судебной экспертизы должен охватывать следующие виды деятельности:

– обеспечение защиты целевой системы, сервиса и (или) сети в процессе проведения судебной экспертизы от превращения их в недоступные, изменения или иной компрометации, включая введение вирусов, и обеспечение отсутствия или минимальности воздействий на обеспечение нормальной работы;

– назначение приоритетов "добычи" и "свидетельств", т. е., рассмотрение их от наиболее изменчивых до наименее изменчивых (это в большой степени зависит от характера инцидента ИБ);

– идентификация всех нужных файлов в целевой системе, сервисе и (или) сети, включая нормальные файлы, файлы, кажущиеся уничтоженными, но не являющиеся таковыми, файлы, защищенные паролем или иным образом, и зашифрованные файлы;

– восстановление как можно бóльшего числа уничтоженных файлов и других данных;

– раскрытие IP-адресов, имен хостов, сетевых маршрутов и информации Web - сайтов;

– извлечение содержимого "скрытых", временных и файлов подкачки, использованных как программным обеспечением операционной системой, так и прикладным программным обеспечением;

– доступ к содержимому защищенных или зашифрованных файлов (если не запрещено законом);

– анализ всех возможно значимых данных, найденных в специальных (обычно, недоступных) областях памяти на дисках;

– анализ времени доступа к файлу, его изменения и создания;

– анализ журналов регистрации системы/сервиса/сети и приложений;

– определение деятельности пользователей и (или) приложений в системе/сервисе/сети;

– анализ электронной почты на наличие исходной информации и ее содержания;

– выполнение проверок целостности файлов для обнаружения файлов, содержащих "Троянского коня" и файлов, которые первоначально не было в системе;

– анализ, по возможности, физических свидетельств, например, отпечатков пальцев, ущерба имуществу, видеонаблюдения, журналов регистрации системы сигнализации, журналов регистрации доступа по пропускам и опроса свидетелей;

– обработки и хранения добытых потенциальных свидетельств таким образом, чтобы избежать их повреждения или приведения в негодность, чтобы конфиденциальный материал не смогли увидеть неавторизованные лица. Следует подчеркнуть, что сбор свидетельств всегда должен проводиться в соответствии с правилами судопроизводства или слушания дела, для которого данное свидетельство может быть представлено;

– выводы о причинах инцидента ИБ, требуемых действиях и интервале времени, для их выполнения, с приведением свидетельств, включая список соответствующих файлов, включенных в приложение к главному отчету;

– если требуется, обеспечение экспертной поддержки для любого дисциплинарного или правового действия.

Метод(ы), которому(ым) необходимо следовать, должен(ны) документироваться в процедурах ГРИИБ.

ГРИИБ должна обладать достаточно разнообразными мастерством, навыками для обеспечения обширной области технических знаний (включая средства и методы, которые, возможно, будут использоваться нарушителем), опытом проведения анализа/расследования (с учетом защиты используемых свидетельств), знанием правовых и нормативных положений и текущей осведомленности о тенденциях, касающихся инцидентов ИБ.

8.5.6 Распространение информации

Во многих случаях, когда ГРИИБ подтвердила реальность инцидента ИБ, возникает необходимость проинформировать определенных лиц как внутри организации (вне обычных линий связи между ГРИИБ и руководством), так и за ее пределами, включая прессу. Для этого могут потребоваться несколько этапов, например, когда инцидент ИБ подтверждается как реальный, когда он находится под контролем и это подтверждается, когда он определен для "кризисной деятельности", когда инцидент заканчивается, а также когда анализ инцидента завершается и делаются выводы.

Для поддержки такой деятельности, когда существует потребность весьма разумно подготовить заранее определенную информацию так, чтобы ее можно было быстро адаптировать к обстоятельствам конкретного инцидента ИБ и предоставить прессе и (или) другим средствам массовой информации. Если некоторая информация, относящаяся к инцидентам ИБ, предоставляется прессе, то это должно быть сделано в соответствии с политикой распространения информации организации. Информация, подлежащая распространению, должна быть проанализирована соответствующими сторонами, которые могут быть представлены высшим руководством, координаторами по связям с общественностью и персоналом ИБ.

8.5.7 Эскалация

Могут возникнуть обстоятельства, когда решение вопросов придется передать либо высшему руководству, другой группе внутри организации, либо лицу/группе сторонней организации. Речь может идти о принятии решения относительно рекомендуемых действий, относящихся к инциденту ИБ или о дальнейшей оценке с целью определения требуемых действий. Эскалация может потребоваться вслед за процессами оценки, описанными в подразделе 8.4, или же она может происходить в ходе этих процессов, если некая существенная проблема становится очевидной на ранней стадии. В документации системы менеджмента инцидентов ИБ должно быть руководство для тех, кому, вероятно, в некоторый момент придется принимать решение об эскалации, т. е., для группы обеспечения эксплуатации и для членов ГРИИБ.

8.5.8 Регистрация деятельности и контроль изменений

Следует подчеркнуть, что все, кто причастен к оповещению (информированию) и менеджменту инцидентов ИБ, должны надлежащим образом регистрировать все действия для дальнейшего анализа. Информация об этих действиях должна вноситься в форму отчета об инцидентах ИБ и в базу данных событий/инцидентов ИБ, непрерывно обновляться в течение жизненного цикла инцидента ИБ, от первой формы отчета до завершения анализа инцидента. Эта информация должна храниться доказуемо безопасно с обеспечением соответствующего режима резервирования. Кроме того, все изменения, вносимые в процессе отслеживания инцидента, обновления форм отчета и баз данных событий/инцидентов ИБ должны выполняться в соответствии с формально принятой системой контроля изменений.

9 Анализ

9.1 Введение

После того, как инцидент ИБ был разрешен и его завершение согласовано, необходимо провести дальнейшую судебную экспертизу и анализ с целью определения извлеченных уроков и потенциальных улучшений общей безопасности и системы менеджмента инцидентов ИБ.

9.2 Дальнейшая судебная экспертиза

После завершения инцидента иногда может по-прежнему сохраняться необходимость проведения судебной экспертизы с целью определения свидетельств. Она должна проводиться ГРИИБ с использованием того же множества средств и процедур, как которые предлагается в п. 8.5.5.

9.3 Полученные уроки

После завершения инцидента ИБ важно, чтобы уроки, извлеченные из его обработки, можно было быстро в дальнейшем идентифицировать и предпринять соответствующие им действия. Уроки могут рассматриваться с точки зрения:

– новых или измененных требований к защитным мерам ИБ. Это могут быть технические или нетехнические, включая физические меры защиты. В зависимости от полученных уроков, требования могут включать необходимость быстрого обновления материалов и проведения инструктажа с целью обеспечения осведомленности в вопросах безопасности (для пользователей, а также для другого персонала), быстрого анализа и выпуска руководств и (или) стандартов по безопасности;

– и (или) изменения в системе менеджмента инцидентов ИБ и ее процессах, формах отчета и базе данных событий/инцидентов ИБ.

Кроме того, в этой деятельности необходимо выйти за рамки отдельного инцидента ИБ и проверить наличие тенденций/образцов, которые сами по себе могут помочь определить потребность в защитных мерах или изменениях в подходе. Разумной практикой является также проведение после инцидента ИБ, связанного с ИТ, ориентированного на проведение тестирования ИБ, в особенности, оценки уязвимостей.

Поэтому, необходимо анализировать базы данных событий/инцидентов ИБ на регулярной основе для того, чтобы:

– определять тенденции/образцы;

– определять проблемные области;

– определять, где можно предпринять превентивные меры для снижения вероятности появления инцидентов в будущем.

Соответствующая информация, получаемая в процессе обработки инцидента ИБ, должна направляться для анализа тенденций/образцов. Это может в значительной мере способствовать раннему определению инцидентов ИБ и обеспечивать предупреждение о том, какие следующие инциденты ИБ могут возникнуть, на основе предшествующего опыта и документированном знании.

Необходимо также использовать информацию об инцидентах ИБ и соответствующих уязвимостях, полученная от государственных и коммерческих КГБР и от поставщиков.

Тестирование безопасности и оценка уязвимостей информационной системы, сервиса и (или) сети, следующие за инцидентом ИБ, не должны ограничиваться только информационной системой, сервисом и (или) сетью, которые были затронуты этим инцидентом ИБ. Они должны быть распространено на любые связанные с ними информационные системы, сервисы и (или) сети. Полная оценка уязвимостей используется для того, чтобы выявить существование уязвимостей, задействованные в ходе этого инцидента ИБ на других информационных системах, сервисах и (или) сетях, и исключить вероятность появления новых уязвимостей.

Важно подчеркнуть, что оценка уязвимостей должна выполняться регулярно и что повторная оценка уязвимостей, проводимая после инцидента ИБ, должна являться частью данного непрерывного процесса оценки (а не его заменой).

Необходимо выпускать итоговый анализ инцидентов ИБ для обсуждения его на каждом совещании руководства организации по вопросам ИБ и (или) совещании другого рода, определенного в общей организационной политике ИБ.

9.4 Идентификация улучшений безопасности

В процессе анализа, проведенного после разрешения инцидента ИБ, могут быть определены необходимые новые или пересмотренные защитные меры. Рекомендации и соответствующие им требования к защитным мерам могут оказаться такими, что их немедленное внедрение невозможно по финансовым или эксплуатационным причинам; в таком случае они должны быть отражены в более долгосрочных целях организации. Например, по финансовым соображениям невозможно за короткое время осуществить переход к более надежным межсетевым экранам, но необходимо внести решение этого вопроса в долговременные цели ИБ организации (см. подраздел 10.3 ниже).

9.5 Идентификация улучшений системы

После разрешения инцидента руководитель ГИИБ или назначенное лицо должны проанализировать все произошедшее, чтобы оценить и определить степень результативности полной реакции на инцидент ИБ. Подобный анализ имеет целью определить, какие части системы менеджмента инцидентов ИБ работали успешно и определить потребность в каких-либо улучшениях.

Важным аспектом анализа, проводимого после реакции на инцидент, является возвращение информации и знаний обратно в систему менеджмента инцидентов ИБ. Если опасность инцидента достаточно высока, то вскоре после разрешения инцидента должно быть назначено совещание всех заинтересованных сторон, пока информация еще свежа в памяти людей. На этом собрании должны рассматриваться следующие факторы:

– Работали ли должным образом процедуры, принятые в системе менеджмента инцидентов ИБ?

– Существуют ли процедуры или методы, которые способствовали бы обнаружению инцидентов?

– Были ли определены процедуры или средства, которые использовались бы в процессе реагирования?

– Применялись ли процедуры, помогающие восстановлению информационных систем после идентификации инцидента?

– Была ли передача информации об инциденте всех причастных сторон эффективной в процессе обнаружения, сообщения и реагирования?

Результаты совещания должны быть документированы, и соответствующим образом осуществлены некоторые согласованные действия (см. подраздел 10.4 ниже).

10 Улучшение

10.1 Введение

Этап "Улучшение" охватывает внедрение рекомендаций этапа "Анализ", т. е., рекомендаций по улучшению результатов менеджмента и анализа рисков ИБ, по улучшению безопасности и системы менеджмента инцидентов ИБ. Каждая из этих тем рассматривается ниже.

10.2 Улучшение анализа рисков и менеджмента безопасности

В зависимости от опасности и воздействия инцидента ИБ, при оценке результатов анализа рисков ИБ и менеджмента ИБ может потребоваться принятие в расчет новых угроз и уязвимостей. Результатом завершения обновленного анализа рисков ИБ и анализа менеджмента ИБ может возникнуть необходимость введения измененных или новых защитных мер.

10.3 Внедрение улучшений безопасности

Следуя рекомендациям, сделанным в процессе этапа "Анализ" (см. подраздел 9.4 выше), необходимо осуществить анализ ряда инцидентов ИБ и внедрить обновленные и (или) новых защитных мер. Как обсуждалось ранее в подразделе 9.3, это могут быть технические (включая физические) защитные меры, которые могут включать в себя потребность быстрого обновления материала для проведения инструктажей с целью обеспечения осведомленности в вопросах безопасности (для пользователей и другого персонала), и быстрого анализа и выпуска рекомендаций и (или) стандартов по безопасности. Далее, информационные системы, сервисы и сети организации должны регулярно анализировать на предмет уязвимостей с целью определения уязвимостей и обеспечения процесса непрерывного улучшения систем/сервисов/сетей.

В то время, когда может проводиться анализ связанных с безопасностью процедур и документации сразу после инцидента, наиболее вероятно, что это потребуется как более поздняя реакция. После инцидента ИБ необходимо обновить, если потребуется, политики и процедуры ИБ, чтобы учесть собранную информацию и любые проблемные вопросы, обнаруженные в процессе менеджмента инцидента. Долговременной целью ГРИИБ вместе с руководителем ИБ организации является обеспечение распространения в организации этих обновлений политики и процедур ИБ.

10.4 Внедрение улучшений системы

Области, обозначенные для улучшения системы менеджмента инцидентов ИБ (см. подраздел 9.5), должны быть проанализированы, и обоснованные изменения внесены в обновление документации системы. Изменения в процессах, процедурах и в формах отчета системы менеджмента инцидентов ИБ должны быть тщательно проверены и протестированы до введения в эксплуатацию.

10.5 Другие улучшения

Другие улучшения на этапе "Анализ" могли быть определены, например, изменения в политиках, стандартах и процедурах ИБ, а также изменения в конфигурациях аппаратного и программного обеспечения.

11 Резюме

Настоящий технический отчет дает общее представление о менеджменте инцидентов ИБ, выгодах от принятия системы менеджмента инцидентов ИБ и ключевые проблемы, связанные с ее принятием. В отчете подробно описываются четкие этапы планирования и документирования системы и политики менеджмента инцидентов ИБ, наряду с соответствующими процессами и процедурами управления инцидентами ИБ и деятельность после разрешения инцидента.

Приложение А
(информативное)

Примерные формы отчета о событиях и инцидентах ИБ

Отчеты о событиях и инцидентах ИБ

Рекомендации по заполнению

Назначением этих форм (форм отчета о событиях и инцидентах ИБ) является обеспечение информации о событии ИБ, а затем, если оно определено как инцидент, то и об инциденте ИБ для определенных лиц.

Если Вы подозреваете, что событие ИБ развивается или уже произошло, особенно такое, которое может нанести существенные потери или ущерб собственности или репутации организации, то Вы должны ***немедленно*** заполнить и передать форму отчета о событии ИБ (см. первую часть данного Приложения А) в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная Вами информация будет использована для начала соответствующего процесса оценки, которая определяет, должно ли это событие категорироваться как инцидент ИБ или нет, и в случае положительного ответа будут приняты необходимые корректирующие меры для предотвращения или ограничения потерь или ущерба. Поскольку этот процесс по своему характеру является критичным по времени, то ***необязательно заполнять все поля в форме отчета в данный момент времени***.

Если Вы являетесь членом группы обеспечения эксплуатации, просматривающим уже заполненные/частично заполненные формы, то Вы должны решить, надо ли категорировать данное событие как инцидент ИБ. Если надо, то Вы должны заполнить форму для инцидента ИБ насколько возможно подробно направить и передать и форму для события, и инцидент ИБ ГРИИБ. Независимо от того, будет ли событие ИБ категорировано как инцидент или нет, в любом случае база данных событий/инцидентов ИБ должна быть обновлена.

Если Вы являетесь сотрудником ГРИИБ, просматривающим формы для событий и инцидентов ИБ, переданные членом группы обеспечения эксплуатации, то форма инцидента ИБ должна далее обновляться по мере прогресса в исследовании, и соответствующие обновления должны проводиться в базе данных событий/инцидентов ИБ.

При заполнении форм, пожалуйста, соблюдайте следующие рекомендации:

– если возможно, то формы должны заполняться и передаваться в электронном виде[1)]. (Если существуют проблемы или считается, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например, электронная почта), включая случаи, когда система, возможно, подвергается атаке, и формы отчета могут быть прочитаны неавторизованными лицами, тогда должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть на́рочные, телефон или текстовые сообщения.);

– представляйте информацию, основанную только на фактах, в которой Вы уверены, ничего не придумывайте для того, чтобы заполнить все поля. Где уместно включить

[1)] Если возможно, то эти формы должны быть в электронном виде (например, на безопасной web-странице) с привязкой к электронной базе данных событий/инцидентов ИБ. В современном мире, основанная на бумажной документации система является слишком медленной и далеко не самой эффективной в эксплуатации.

информацию, которую Вы не можете подтвердить, четко укажите, что это неподтвержденная информация и почему Вы считаете, что она верная;

– вы должны подробно указать, как можно с Вами связаться. Очень скоро или спустя некоторое время может возникнуть необходимость контакта с Вами для дальнейшей информации, касающейся Вашего отчета;

Если позже Вы обнаружите, что некоторая представленная Вами информация неточна, неполна или ошибочна, то Вы должны внести поправки в Ваш отчет и представить его повторно.

Отчет о событии ИБ

Дата события
Номер события:[12)]

Стр. 1 из 1

(Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:

Информация о сообщающем лице

Фамилия _____ Адрес _____
Организация _____ _____
Телефон _____ Электронная почта _____
_____

Описание события ИБ

Описание события:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на бизнес
- Любые идентифицированные уязвимости

Детали события ИБ

Дата и время возникновения события
Дата и время обнаружения события

Дата и время сообщения о событии

Закончилось ли событие? *(отметить квадрат)* Да ☐ Нет ☐
Если «да», то уточнить, как долго длилось событие в днях/часах/минутах

[12)] (Номера событий назначаются руководителем ГРИИБ организации.)

Отчет об инциденте ИБ

Дата инцидента

Стр. 1 из 5

Номер инцидента[13)]

:

(Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:

Информация о сотруднике группы обеспечения эксплуатации

Фамилия	_____	Адрес	_____
Телефон	_____	Электронная почта	_____

Информация о сотруднике ISIRT

Фамилия	_____	Адрес	_____
Телефон	_____	Электронная почта	_____

_____

Описание инцидента ИБ

Дальнейшее описание инцидента:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на бизнес
- Любые идентифицированные уязвимости

Детали инцидента ИБ

Дата и время возникновения инцидента

Дата и время обнаружения инцидента

Дата и время сообщения об инциденте

Закончился ли инцидент? *(отметить квадрат)* Да □ Нет □

Если «да», то уточнить, как долго длился инцидент в днях/часах/минутах. Если «нет», то уточнить, как долго он уже длится

[13)] (Номера инцидентов назначаются руководителем ГРИИБ организации и привязываются к номеру(ам) соответствующих событий.)

Отчет об инциденте ИБ

Тип инцидента ИБ

(Отметить один квадрат, затем заполнить соответствующие поля ниже)

Действительный ☐ **Попытка** ☐ **Подозрение** ☐

(Один из) **Намеренная** ☐ *(указать типы угрозы)*

Хищение (TH)	☐	Хакерство/Логическое проникновение (HA)	☐
Мошенничество (FR)	☐	Неправильное использование ресурсов (MI)	☐
Саботаж/физический ущерб (SA)	☐	Другой ущерб (OD)	☐
Вредоносная программа (MC)	☐		

Определить:

(Один из) **Случайная** ☐ *(указать типы угрозы)*

Отказ аппаратуры (HF)	☐	Другие природные события (NE)	☐
Отказ ПО (SF)	☐	*Определить:*	
Отказ связи (CF)	☐	Потеря существенных сервисов (LE)	☐
Пожар (HE)	☐	Недостаточное кадровое обеспечение (SS)	☐
Наводнение (FL)	☐	Другие случаи (OA)	☐

Определить:

(Один из) **Ошибка** ☐ *(указать типы угрозы)*

Операционная ошибка (OE)	☐	Ошибка пользователя (UE)	☐
Ошибка аппаратной поддержки (HE)	☐	Ошибка конструкции (DE)	☐
Ошибка поддержки ПО (SE)	☐	Другие случаи (включая истинные заблуждения) (OA)	☐

Определить:

Неизвестно ☐

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы, ,используя сокращения, приведенные выше)

Определить:

Отчет об инциденте ИБ

Пораженные активы

Пораженные активы (если есть) *(Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности)*

Информация/Данные _____

Аппаратура _____

Программное обеспечение _____

Средства связи _____

Документация _____

Негативное воздействие/влияние инцидента на бизнес

Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на бизнес по шкале 1÷10, используя сокращения (указатели категорий): (FD) – финансовые потери/разрушение бизнес-операций, (CE) – коммерческие и экономические интересы, (PI) – информация, содержащая персональные данные, (LR) – правовые и нормативные обязательства(это необходимо сличить с английским оригиналом),(MO) – менеджмент и бизнес-операции, (LG) – потеря престижа (см. примеры в Приложении В*). Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»*

		Значимость	**Указатели**	**Стоимость**
Нарушение конфиденциальности *(т. е., несанкционированное раскрытие)*	☐			
Нарушение целостности *(т. е., несанкционированная модификация)*	☐			
Нарушение доступности *(т. е., недоступность)*	☐			
Нарушение неотказуемости	☐			
Уничтожение	☐			

Полные стоимости восстановления после инцидента

(Где возможно, необходимо указать общие расходы на восстановление после инцидента в целом по шкале 1÷10 для «значимости» и в деньгах для «стоимости»)	**Значимость**	**Указатели**	**Стоимость**

Отчет об инциденте ИБ

Разрешение инцидента

Дата начала расследования инцидента _____

Фамилия лица (лиц), проводившего (их) расследование инцидента _____

Дата окончания инцидента _____

Дата окончания воздействия _____

Дата завершения расследования инцидента _____

Ссылка и место хранения отчета о расследовании _____

Причастные лица

(Один из)

Лицо (PE) ☐

Организованная группа (GR) ☐

Легально учрежденная организация/учреждение (OI) ☐

Случайность (AC) ☐

Нет виновного (NP) ☐
Например, природные факторы, отказ оборудования, ошибка человека

Описание нарушителя

Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода(CG) ☐

Политика/Терроризм (PT) ☐

Развлечение/хакерство (PH) ☐

Реванш (RE) ☐

Другие мотивы (OM) ☐
Определить:

Действия, <u>предпринятые</u> для разрешения инцидента

(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением…»)

Действия, запланированные для разрешения инцидента

(например, см. выше)

Прочие действия

(например, по-прежнему требуется проведение расследования для другого персонала)

Отчет об инциденте ИБ

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный ☐ **Незначительный** ☐

(Укажите любые другие заключения) _____

Ознакомленные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации).

Руководитель ИБ	☐	Руководитель ГРИИБ	☐
Местный руководитель (уточнить, какого подразделения)	☐	Руководитель информационных систем	☐
Автор отчета	☐	Руководитель автора отчета	☐
Полиция	☐	Другое лица	☐

(например, справочная служба, отдела кадров, менеджмента, внутреннего аудита, регулятивного органа, сторонняя КСБР)

Определить:

Привлеченные лица

Инициатор	Аналитик	Аналитик
Подпись _____	Подпись _____	Подпись _____
Фамилия _____	Фамилия _____	Фамилия _____
Роль _____	Роль _____	Роль _____
Дата _____	Дата _____	Дата _____

Аналитик	Аналитик	Аналитик
Подпись _____	Подпись _____	Подпись _____
Фамилия _____	Фамилия _____	Фамилия _____
Роль _____	Роль _____	Роль _____
Дата _____	Дата _____	Дата _____

Приложение В
(информативное)

Примерные общие рекомендации по оценке инцидентов ИБ

В.1 Введение

В данном приложении представляются *примерные* рекомендации по оценке и категорированию негативных последствий инцидентов ИБ, и каждая рекомендация имеет шкалу от1 до10 (1 – низкий, 10 – высокий). (На практике могут использоваться другие шкалы, например, от1 до 5. Каждая организация должна принять шкалу, наиболее подходящую для ее среды.)

Прежде, чем читать рекомендации, изложенные ниже, необходимо отметить следующие пояснения:

– в некоторых рекомендациях, представленных ниже, содержатся указания "нет записи". Сделано это из-за того, что рекомендации сформулированы таким образом, что негативные последствия, приведенные для каждого из смежных уровней и выраженных по шкале 1–10, в значительной мере сходны во всех показанных шести категориях. Однако, на некоторых уровнях (по шкале 1–10) для некоторых категорий считается, что по причине отсутствия достаточного различия в смежных записях о последствиях на более низких уровнях недостаточно сведений, чтобы делать необходимую запись, в этом случае делается примечание "нет записи". Аналогично, на более высоких уровнях некоторых категорий считается, что негативные последствия для этих уровней не могут быть серьезней негативных последствий, показанных для самого высокого уровня, и, следовательно, для этих уровней действует примечание "нет записи". (Таким образом, было бы логически некорректно выбросить пункты, отмеченные как "нет записи", и сохранить);

– для рекомендаций, изложенных ниже, в которых применяются финансовые показатели, используемые диапазоны кажутся странными. Перед использованием эти рекомендации должны быть дополнены нормированием колебания по курсу валюты, подходящей для организации.

Таким образом, при использовании ниже перечисленных рекомендаций при рассмотрении негативных для бизнеса организации последствий инцидента ИБ, являющихся следствием:

– несанкционированного раскрытия информации;
– несанкционированного изменения информации;
– отказа от информации;
– недоступности информации и (или) сервиса;
– уничтожения информации и (или) сервиса,

в первую очередь необходимо определить, какая из нижеследующих категорий имеет отношение к делу. Для категорий, считающихся таковыми, необходимо применять рекомендации по категорированию для определения фактического негативного воздействия на бизнес-операции ("значимость") с целью занесения в форму отчета об инциденте ИБ.

В.2 Финансовые убытки/нарушение хода бизнес-операций

Последствия несанкционированного раскрытия и модификации, изменения смысла переданной информации, а также недоступности, уничтожение такой информации могут

привести к финансовым убыткам, например, в результате снижения цен на акции, мошенничества или разрыва контракта по причине бездействия или запоздалых действий. Аналогично, последствиями недоступности или уничтожение любой информации может быть нарушение бизнес-операций. На исправление ситуации и (или) восстановление после таких инцидентов потребуются время и усилия. Они в некоторых случаях могут быть значительными и должны приниматься во внимание. Для использования общего знаменателя, время восстановления должно быть вычислено в единицах рабочего времени персонала и преобразовано в финансовые затраты. Эти затраты должны быть вычислены исходя из средней стоимости человеко-месяца по соответствующей градации/уровню внутри организации. Предлагается руководствоваться следующим рекомендациями:

1) результат в финансовых убытках/затратах x_1 или меньше;
2) результат в финансовых убытках/затратах между x_1+1 и x_2;
3) результат в финансовых убытках/затратах между x_2+1 и x_3;
4) результат в финансовых убытках/затратах между x_3+1 и x_4;
5) результат в финансовых убытках/затратах между x_4+1 и x_5;
6) результат в финансовых убытках/затратах между x_5+1 и x_6;
7) результат в финансовых убытках/затратах между x_6+1 и x_7;
8) результат в финансовых убытках/затратах между x_7+1 и x_8;
9) результат в финансовых убытках/затратах более x_8;
10) организация выходит из бизнеса.

B.3 Коммерческие и экономические интересы

Коммерческая и экономическая информация нуждается в защите и оценивается с учетом ее значимости для конкурентов или по воздействию, которое оказывает ее компрометация на коммерческие интересы. Предлагается руководствоваться следующим рекомендациями:

1) представляет интерес для конкурента, но не имеет коммерческой значимости (ценности);

2) представляет интерес для конкурента при значимости y_1 или меньше (коммерческий оборот);

3) представляет интерес для конкурента при значимости между y_1+1 и y_2 (оборот), или является причиной финансовых убытков, или потери заработка, или облегчает получение незаконной прибыли или вызывает нарушение обязательств по поддержанию достоверности информации, поставляемой третьими сторонами;

4) представляет интерес для конкурента при значимости между y_2+1 и y_3 (оборот);

5) представляет интерес для конкурента при значимости между y_3+1 и y_4 (оборот);

6) представляет интерес для конкурента при значимости более y_4+1 (оборот);

7) *нет записи*[14)];

8) *нет записи*;

9) может существенно подорвать коммерческие интересы или финансовое состояние организации;

[14)] Термин "нет записи" означает, что соответствующие этому уровню последствия не вводятся.

10) *нет записи*.

B.4 Информация, содержащая персональные данные

В местах хранения и обработки информации, содержащей персональные данные физических лиц, морально и этически корректно, а при некоторых обстоятельствах юридически необходимо, чтобы она была защищена от несанкционированного раскрытия, которое может привести, в лучшем случае, к чувству дискомфорта, а в худшем случае, к судебному преследованию, например, в соответствии с требованием законодательства в части защиты персональных данных. Равно как необходимо, чтобы информация, содержащая персональные данные, была всегда корректной, поскольку несанкционированное её изменение, приводящее к появлению некорректных данных, может иметь такое же последствие, как и её несанкционированное раскрытие. Также важно, чтобы информация, содержащая персональные данные, не могла быть доступной или быть уничтоженной, поскольку это может привести к неправильным решениям или к бездействию в нужное время, что может иметь такое же воздействие, что и несанкционированное раскрытие или модификация. Предлагается руководствоваться следующим рекомендациями:

1) незначительный ущерб (беспокойство) для отдельного лица (гнев, расстройство, разочарование), но не нарушение правовых или нормативный требований;

2) ущерб (беспокойство) для отдельного лица (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

3) нарушение правовых, нормативных или этических требований, а также опубликованных (заявленных) намерений относительно защиты информации, приводящее к чувству незначительного дискомфорта отдельного лица;

4) нарушение правовых, нормативных или этических требований, а также опубликованных намерений относительно защиты информации, приводящее к чувству значительного дискомфорта отдельного лица или незначительным проблемам для группы лиц;

5) нарушение правовых, нормативных или этических требований, а также опубликованных намерений относительно защиты информации, приводящее к серьезным проблемам отдельного лица;

6) нарушение правовых, нормативных или этических требований, а также опубликованных намерений относительно защиты информации, приводящее к серьезным проблемам для группы лиц;

7) *нет записи*;

8) *нет записи*;

9) *нет записи*;

10) *нет записи*.

B.5 Правовые и нормативные обязательства

Данные, хранимые и обрабатываемые организацией, могут иметь правовые и нормативные обязательства, или храниться и обрабатываться, чтобы позволить организации соответствовать этим обязательствам. Несоблюдение таких обязательств, намеренное или ненамеренное, может привести к правовым или административным мерам, предпринимаемым в отношении лиц, работающих в данной организации. Результатом этих мер могут быть штрафы и (или) тюремное заключение. Предлагается руководствоваться следующим рекомендациями:

1) *нет записи;*

2) *нет записи;*

3) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу z_1 или меньше;

4) предупреждение, гражданский иск или уголовное преступление, приводящее к финансовому ущербу/штрафу между z_1+1 и z_2;

5) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между z_2+1 и z_3 или тюремному заключению сроком до двух лет;

6) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между z_3+1 и z_4 или тюремному заключению сроком от двух до десяти лет;

7) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу или тюремному заключению сроком более десяти лет;

8) *нет записи;*

9) *нет записи;*

10) *нет записи.*

B.6 Менеджмент и бизнес-операции

Информация может быть такой, что ее компрометация нанесет ущерб эффективности работы организации. Например, информация, связанная с изменением в политике, будучи раскрытой, может спровоцировать общественную реакцию такой степени, что реализация этой политики станет невозможной. Модификация, изменение смысла переданной информации или недоступность информации, касающейся финансовых аспектов или компьютерного программного обеспечения, могут также иметь серьезные последствия для работы организации. Кроме того, отказ от обязательств может иметь негативные последствия для бизнеса. Предлагается руководствоваться следующим рекомендациями:

1) неэффективная работа одного подразделения организации;

2) *нет записи;*

3) подрыв надлежащего руководства организации и ее работы;

4) *нет записи;*

5) задержка эффективной разработки или функционирования политик организации;

6) невыгодное положение организации при коммерческих или политических переговорах с другими организациями;

7) серьезная задержка разработки или функционирование главных политик организации, или закрытие или другое существенное прерывание важных операций;

8) *нет записи;*

9) *нет записи;*

10) *нет записи.*

B.7 Потеря престижа

Несанкционированное раскрытие, отказ от обязательств или модификация, а также недоступность информации могут привести к потере престижа организации, с последую-

щим возможным нанесением ущерба ее репутации, потери доверия и другим негативным последствиям. Предлагается руководствоваться следующим рекомендациями:

1) *нет записи;*

2) локальное недовольство внутри организации;

3) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к скандальной извесности местного/регионального характера;

4) *нет записи;*

5) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к некоторой скандальной известности в национальном масштабе;

6) *нет записи;*

7) значительное негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к скандальной извесности в мировом масштабе;

8) *нет записи;*

9) *нет записи;*

10) *нет записи.*

Приложение С

(справочное)

Сведения о соответствии национальных стандартов ссылочным международным стандартам

Т а б л и ц а С.1

Обозначение ссылочного международного стандарта	Обозначение и наименования соответствующего национального стандарта
ИСО/МЭК 13335-1:2004	ГОСТ Р ИСО/МЭК 13335.1-2005 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационных и телекоммуникационных технологий. Часть 1. Концепция и модели управления безопасностью информационных и телекоммуникационных технологий
ИСО/МЭК 13335-2	*
ИСО/МЭК 17799:2000	ГОСТ Р ИСО/МЭК 17799-2006 Информационная технология. Методы обеспечения безопасности. Руководство по управлению безопасностью информации
ИСО/МЭК ТО 15947-2002	*
ИСО/МЭК 18043	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта	

Библиография

[1] ИСО/МЭК ТО 13335-3 Информационная технология – Рекомендации относительно менеджмента безопасности ИТ – Часть 3: Методы и средства, применяемые для менеджмента безопасности ИТ

[2] ИСО/МЭК ТО 15947-2002 Информационная технология – Методы и средства обеспечения безопасности – Структура обнаружения вторжения в сфере ИТ

[3] ИСО/МЭК 18028 Методы и средства обеспечения безопасности ИТ – Безопасность сетей в сфере ИТ

[4] ИСО/МЭК 18043 Методы и средства обеспечения безопасности ИТ – Рекомендации по выбору, развертыванию и эксплуатации систем обнаружения вторжения (IDS) (тип документа за № 4029, подлежащего одобрению NP на SC27 к 24.09.2004)

[5] Руководство ИСО/МЭК 73-2002, Менеджмент риска – Словарь – Рекомендации по использованию в стандартах

[6] Справочник по обеспечению безопасности сайтов целевой группы инженерной поддержки Internet (IETF)

Internet Engineering Task Force (IETF) Site Security Handbook, http://www.ietf.org/rfc/rfc2196.txt? number=2196

[7] Ожидания, связанные с реагированием на инциденты компьютерной безопасности – Общепринятая практика, июнь 1998 г.

Expectations for Computer Security Incident Response – Best Practice, June 98, ftp://ftp.isi.edu/in-notes/rfc2350. txt

[8] Специальная публикация NIST 800-3, ноябрь 1991 г., Создание группы реагирования на инциденты компьютерной безопасности (CSIRC)

NIST Special Publication 800-3 Nov ‘91, Establishing a Computer Incident Response Capability (CSIRC), http://csrc.nist.gov/publications/nistpubs/800-3/800-3. pdf

---

УДК ОКС 01.040.01

Т00

Ключевые слова: менеджмент инцидентов информационной безопасности, группа реагирования на инциденты информационной безопасности, событие информационной безопасности, система менеджмента информационной безопасности

Председатель ТК 362
начальник ГНИИИ ПТЗИ ФСТЭК России
В.Г.Герасименко

"____" апреля 2007 г.

Ответственный секретарь ТК 362,
начальник 14 отдела ГНИИИ ПТЗИ ФСТЭК России
Ю.Г.Кирсанов

"____" апреля 2007 г.

Научный сотрудник 14 отдела
ГНИИИ ПТЗИ ФСТЭК России В.В.Стрекалов

"____" апреля 2007 г.