ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК ТО 18044— 2007

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)

Издание официальное

БЗ 12—2007/462

Москва
Стандартинформ
2009

gost.e-ecolog.ru

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 пункте 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 27 декабря 2007 г. № 513-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК ТО 18044:2004 «Информационные технологии. Финансовые услуги. Рекомендации по информационной безопасности» (ISO/IEC TR 18044:2004 «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

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2009

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Общие положения . . . 2
4.1 Цели . . . 2
4.2 Этапы . . . 2
5 Преимущества структурного подхода и ключевые вопросы менеджмента инцидентов информационной безопасности . . . 5
5.1 Преимущества . . . 5
5.2 Ключевые вопросы . . . 6
6 Примеры инцидентов информационной безопасности и их причины . . . 10
6.1 Отказ в обслуживании . . . 10
6.2 Сбор информации . . . 11
6.3 Несанкционированный доступ . . . 12
7 Этап «Планирование и подготовка» . . . 12
7.1 Общее представление о менеджменте инцидентов информационной безопасности . . . 12
7.2 Политика менеджмента инцидентов информационной безопасности . . . 13
7.3 Программа менеджмента инцидентов информационной безопасности . . . 15
7.4 Политики менеджмента рисков и информационной безопасности . . . 17
7.5 Создание группы реагирования на инциденты информационной безопасности . . . 18
7.6 Техническая и другая поддержка реагирования на инциденты информационной безопасности . . . 19
7.7 Обеспечение осведомленности и обучение . . . 20
8 Этап «Использование» . . . 21
8.1 Введение . . . 21
8.2 Обзор ключевых процессов . . . 22
8.3 Обнаружение и оповещение о событиях информационной безопасности . . . 22
8.4 Оценка и принятие решений по событиям/инцидентам . . . 23
8.5 Реагирование на инциденты . . . 26
9 Этап «Анализ» . . . 32
9.1 Введение . . . 32
9.2 Дальнейшая правовая экспертиза . . . 32
9.3 Извлеченные уроки . . . 32
9.4 Определение улучшений безопасности . . . 32
9.5 Определение улучшений системы . . . 33
10 Этап «Улучшение» . . . 33
10.1 Введение . . . 33
10.2 Улучшение анализа рисков и менеджмента безопасности . . . 33
10.3 Осуществление улучшений безопасности . . . 33
10.4 Осуществление улучшений системы . . . 34
10.5 Другие улучшения . . . 34
Приложение А (справочное) Образец формы отчета о событиях и инцидентах информационной безопасности . . . 35
Приложение В (справочное) Примеры общих рекомендаций по оценке инцидентов информационной безопасности . . . 42
Приложение С (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам . . . 45
Библиография . . . 45

Введение

Типовые политики информационной безопасности или защитные меры информационной безопасности (ИБ) не могут полностью гарантировать 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 информационной безопасности — возможными. Инциденты информационной безопасности могут оказывать прямое или косвенное негативное воздействие на бизнес-деятельность организации. Кроме того, будут неизбежно выявляться новые, ранее не идентифицированные угрозы. Недостаточная подготовка конкретной 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 информационной безопасности, важно применять структурный и плановый подход к:

- обнаружению, оповещению об инцидентах информационной безопасности 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 улучшению общего подхода к менеджменту инцидентов информационной безопасности.

Положения настоящего стандарта содержат представление о менеджменте инцидентов информационной безопасности в организации с учетом сложившейся практики на международном уровне.

Настоящий стандарт предназначен для использования организациями всех сфер деятельности при обеспечении информационной безопасности в процессе менеджмента инцидентов. Его положения могут использоваться совместно с другими стандартами, в том числе стандартами, содержащими требования к системе менеджмента информационной безопасности и системе менеджмента качества организации.

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 — 2008—07—01

1 Область применения

В настоящем стандарте содержатся рекомендации по менеджменту инцидентов информационной безопасности в организациях для руководителей подразделений по обеспечению информационной безопасности (ИБ) при применении информационных технологий (ИТ), информационных систем, сервисов и сетей.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие международные стандарты:

ИСО/МЭК 13335-1:2004 Информационная технология — Методы обеспечения безопасности — Управление безопасностью информационных и телекоммуникационных технологий — Часть 1 — Концепция и модели управления безопасностью информационных и телекоммуникационных технологий

ИСО/МЭК 17799:2000 Информационная технология — Практические правила управления информационной безопасностью

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ ИСО/МЭК 13335-1, ИСО/МЭК 17799, а также следующие термины с соответствующими определениями.

3.1 **планирование непрерывности бизнеса** (business continuity planning): Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов.

Примечание — Данный процесс должен также обеспечивать восстановление бизнеса с учетом заданных очередностей и интервалов времени и дальнейшее восстановление всех функций бизнеса в рабочее состояние. Ключевые элементы этого процесса должны обеспечивать применение и тестирование необходимых планов и средств и включение в них информации, бизнес-процессов, информационных систем и сервисов, речевой связи и передачи данных, персонала и физических устройств.

Издание официальное

3.2 **событие информационной безопасности** (information security event): 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** (information security incident): Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

Примечание — Примеры инцидентов ИБ приведены в разделе 6.

3.4 **группа реагирования на инциденты информационной безопасности (ГРИИБ)** (Information Security Incident Response Team (ISIRT)): Группа обученных и доверенных членов организации.

Примечание — Данная группа обрабатывает инциденты ИБ во время их жизненного цикла и иногда может дополняться внешними экспертами, например, из общепризнанной группы реагирования на компьютерные инциденты или компьютерной группы быстрого реагирования (КГБР).

4 Общие положения

4.1 Цели

В качестве основы общей стратегии ИБ организации необходимо использовать структурный подход к менеджменту инцидентов ИБ. Целями такого подхода является обеспечение следующих условий:

- события ИБ должны быть обнаружены и эффективно обработаны, в частности, определены как относящиеся или не относящиеся к инцидентам ИБ[1)];

- идентифицированные инциденты ИБ должны быть оценены, и реагирование на них должно быть осуществлено наиболее целесообразным и результативным способом;

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

- из инцидентов ИБ и их менеджмента необходимо 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 Этапы

Для достижения целей в соответствии с пунктом 4.1 менеджмент инцидентов ИБ подразделяют на четыре отдельных этапа:

1) планирование и подготовка;
2) использование;
3) анализ;
4) улучшение.

Примечание — Этапы менеджмента инцидентов ИБ аналогичны процессам модели PDCA, используемой в международных стандартах ИСО 9000 [4] и ИСО 14000 [5].

Основное содержание этих этапов показано на рисунке 1.

[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, то есть не все события ИБ будут отнесены к категории инцидентов ИБ.

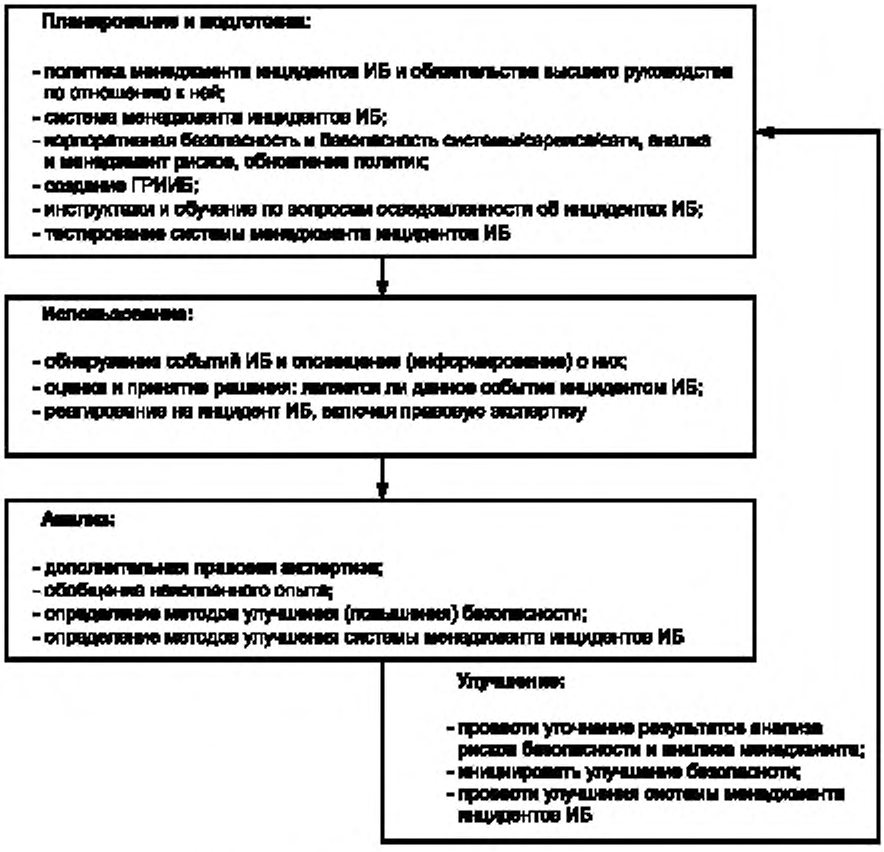


Рисунок 1 — Этапы менеджмента инцидентов ИБ

4.2.1 Планирование и подготовка

Эффективный менеджмент инцидентов ИБ нуждается в надлежащем планировании и подготовке. Для обеспечения эффективности реакции на инциденты ИБ необходимо:

- разработать и документировать политики менеджмента инцидентов ИБ, а также получить очевидную поддержку этой политики заинтересованными сторонами 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 обнаружения, оповещения, оценки и реагирования на инциденты ИБ, а также градации шкалы[1)] серьезности инцидентов должны быть отражены в документации на конкретную систему. (Следует отметить, что в некоторых организациях такая система может называться «Планом реагирования на инциденты ИБ»);

- обновить политики менеджмента ИБ и рисков на всех уровнях, то есть на корпоративном и для каждой системы, сервиса и сети отдельно с учетом системы менеджмента инцидентов ИБ;

[1)] Необходимо иметь определенную шкалу серьезности инцидентов с соответствующей классификацией. Эта шкала может состоять, например, из двух положений: «значительные» и «незначительные». Выбор градаций шкалы должен основываться на фактических или предполагаемых негативных воздействиях на бизнес-операции организации.

- создать в организации соответствующее структурное подразделение менеджмента инцидентов ИБ, то есть ГРИИБ, с заданными обязанностями и ответственностью персонала, способного адекватно реагировать на все известные типы инцидентов ИБ. В большинстве организаций ГРИИБ является группой, состоящей из специалистов по конкретным направлениям деятельности, например, при отражении атак вредоносной программы привлекают специалиста по инцидентам подобного типа;

- ознакомить весь персонал организации посредством инструктажей и (или) иными способами с существованием системы менеджмента инцидентов ИБ, ее преимуществами и с надлежащими способами сообщения о событиях ИБ. Необходимо проводить соответствующее обучение персонала, ответственного за управление системой менеджмента инцидентов ИБ, лиц, принимающих решения по определению того, являются ли события инцидентами, и лиц, исследующих инциденты;

- тщательно тестировать систему менеджмента инцидентов ИБ.

Этап «Планирование и подготовка» — в соответствии с разделом 7.

4.2.2 Использование системы менеджмента инцидентов информационной безопасности

При использовании системы менеджмента инцидентов ИБ необходимо осуществить следующие процессы:

- обнаружение и оповещение 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, выполнить менее срочные действия (например, способствующие полному восстановлению после катастрофы);

- если инциденты ИБ не находятся под контролем, то выполнить «антикризисные» действия (например, вызвать пожарную команду/подразделение или инициировать выполнение плана непрерывности бизнеса);

- сообщить о наличии инцидентов ИБ и любые относящиеся к ним подробности персоналу своей организации, а также персоналу сторонних организаций (что может включить в себя, по мере необходимости, распространение подробностей инцидента с целью дальнейшей оценки и (или) принятия решений);

- правовую экспертизу;

- надлежащую регистрацию всех действий и решений для последующего анализа;

- разрешение проблемы инцидентов.

Этап «Использование» — в соответствии с разделом 8.

4.2.3 Анализ

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

- провести дополнительную правовую экспертизу (при необходимости);

- изучить уроки, извлеченные из инцидентов ИБ;

- определить улучшения для внедрения защитных мер ИБ, полученные из уроков, извлеченных из одного или нескольких инцидентов ИБ;

- определить улучшения для системы менеджмента инцидентов ИБ в целом, учитывая уроки, извлеченные из результатов анализа качества предпринимаемого подхода (например, из анализа результативности процессов, процедур, форм отчета и (или) организации).

Этап «Анализ» — в соответствии с разделом 9.

4.2.4 Улучшение

Необходимо подчеркнуть, что процессы менеджмента инцидентов ИБ являются итеративными, с постоянным внесением улучшений с течением времени в ряд элементов ИБ. Эти улучшения предлагаются на основе данных об инцидентах ИБ и реагировании на них, а также данных о динамике тенденций. Этап «Улучшение» включает в себя:

- 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» — в соответствии с разделом 10.

5 Преимущества структурного подхода и ключевые вопросы менеджмента инцидентов информационной безопасности

В данном разделе представлена информация:

- о преимуществах, получаемых от качественной системы менеджмента инцидентов ИБ;
- о ключевых вопросах, которые необходимо рассмотреть с целью убеждения в этих преимуществах высшего корпоративного руководства и персонала, предоставляющего отчеты в систему и получающего от нее информацию.

5.1 Преимущества

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

- улучшение ИБ;
- снижение негативных воздействий на бизнес, например, прерывание бизнеса и финансовые убытки как последствия инцидентов ИБ;
- усиление внимания к вопросам предотвращения инцидентов;
- усиление внимания к установлению приоритетов и сбору доказательств;
- вклад в обоснование бюджета и ресурсов;
- обновление результатов менеджмента и анализа рисков на более высоком уровне;
- предоставление материала для программ повышения осведомленности и обучения в области ИБ;
- предоставление входных данных для анализа политики ИБ и соответствующей документации.

Каждое из этих преимуществ рассматривается ниже.

5.1.1 Улучшение безопасности

Структурный процесс обнаружения, оповещения, оценки и менеджмента инцидентов и событий ИБ позволяет быстро идентифицировать любое событие или инцидент ИБ и реагировать на них, 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, связанных с инцидентами ИБ, на бизнес. Последствия этих воздействий могут включать в себя немедленные финансовые убытки, а также долговременные потери, возникающие от ущерба, нанесенного репутации и кредитоспособности организации.

5.1.3 Усиление внимания к предотвращению инцидентов

Использование структурного подхода к менеджменту инцидентов ИБ может способствовать усилению внимания к предотвращению инцидентов внутри организации. Анализ данных, связанных с инцидентами, позволяет определить модели и тенденции появления инцидентов, тем самым способствуя усилению внимания к предотвращению инцидентов и, следовательно, определению соответствующих действий по предотвращению возникновения инцидентов.

5.1.4 Усиление внимания к системе 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 расследования проводятся в непостоянном режиме, когда реагирование на инциденты осуществляется по мере их появления или как реакция на самое «громогласное» распоряжение соответствующего руководителя. Это может помешать проведению расследования в последовательности, соответствующей идеальному установлению приоритетов там, где оно действительно необходимо.

Четкие процедуры расследования инцидентов могут обеспечить правильность и правовую допустимость сбора данных и их обработки. Это имеет большое значение в случае инициирования судебного преследования или дисциплинарного разбирательства. Однако следует признать вероятность того, что действия, необходимые для восстановления после инцидента ИБ, могут подвергнуть риску целостность собранных свидетельств.

5.1.5 Бюджет и ресурсы

Хорошо продуманный структурный подход к менеджменту инцидентов ИБ способствует обоснованию и упрощению распределения бюджетов и ресурсов внутри подразделений организации. Кроме того, выгоды получает и сама система менеджмента инцидентов ИБ. Такие выгоды связаны со следующими условиями:

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

- обеспечением лучшего руководства действиями квалифицированного персонала;

- привлечением квалифицированного персонала только для тех процессов, где требуются 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 приостановки «отметки времени» с целью возможности выполнения «количественных» оценок обработки инцидентов ИБ в организации. Это делает возможным, например, предоставление информации о времени разрешения инцидентов с различными приоритетами на различных платформах. При наличии слабых мест в процессе менеджмента инцидентов ИБ эти слабые места также должны быть идентифицируемыми.

5.1.6 Менеджмент и анализ рисков ИБ

Использование структурного подхода к менеджменту инцидентов ИБ способствует:

- сбору более качественных данных для идентификации и определения характеристик различных типов угроз и связанных с ними уязвимостей;

- предоставлению данных о частоте возникновения идентифицированных типов угроз.

Полученные данные о негативных последствиях инцидентов ИБ для бизнеса будут полезны для анализа этих последствий. Данные о частоте возникновения различных типов угроз намного повысят качество оценки угроз. Аналогично, данные об уязвимостях намного повысят качество будущих оценок уязвимостей.

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

5.1.7 Осведомленность в вопросах ИБ

Структурный подход к менеджменту инцидентов ИБ предоставляет узконаправленную информацию о программах обеспечения осведомленности в вопросах ИБ. Эта информация является источником реальных примеров, на которых можно показать, что инциденты ИБ действительно происходят именно в данной организации, а не где-либо еще. Таким образом можно продемонстрировать выгоды быстрого получения информации о решениях. Более того, подобная осведомленность в вопросах ИБ позволяет снизить вероятность ошибки, возникновения паники и (или) растерянности у людей в случае появления инцидента ИБ.

5.1.8 Входные данные для анализа политики ИБ

Информация, предоставляемая системой менеджмента инцидентов ИБ, может обеспечить ценные входные данные для анализа результативности и последующего улучшения 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

Наличие обратной связи, по которой поступает информация о том, как осуществляется менеджмент инцидентов ИБ, помогает сохранять нацеленность действий персонала на борьбу с реальными рисками для систем, сервисов и сетей организации. Эта важная обратная связь не может быть эффективно реализована через процесс реагирования на инциденты ИБ, поскольку инциденты ИБ происходят нерегулярно. Обратная связь может быть более результативной при наличии структурированной, хорошо продуманной системы менеджмента инцидентов ИБ, применяющей общую структуру для всех подразделений организации. Данная общая структура должна непрерывно обеспечивать получение от системы как можно более полных результатов и представлять собой надежную основу для быстрого определения возможных условий возникновения инцидента ИБ до его появления, а также выдавать соответствующие сигналы оповещения.

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

При внедрении систем менеджмента инцидентов ИБ организациям следует избегать таких потенциальных проблем, как отсутствие положительных результатов и беспокойства по поводу вопросов, связанных с проблемами неприкосновенности персональных данных. Необходимо убедить заинтересованные стороны в том, что для предотвращения появления вышеупомянутых проблем были предприняты определенные шаги.

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

- обязательства руководства;
- осведомленность;
- правовые и нормативные аспекты;
- эксплуатационную эффективность и качество;
- анонимность;
- конфиденциальность;
- независимость деятельности ГРИИБ;
- типологию.

Каждый из этих вопросов будет рассмотрен ниже.

5.2.1 Обязательства руководства

Для принятия структурного подхода к менеджменту инцидентов ИБ жизненно необходима постоянная поддержка со стороны руководства. Персонал организации должен распознавать инциденты ИБ и знать свои действия при их возникновении, а также осознавать большие преимущества структурного подхода для организации. Однако этого может быть недостаточно при отсутствии поддержки со стороны руководства. Необходимо донести до руководства, что организация должна выполнять обязательства по обеспечению ресурсами и поддержке способности реагирования на инциденты.

5.2.2 Осведомленность

Другой важной проблемой принятия структурного подхода к менеджменту инцидентов ИБ является осведомленность. Несмотря на потребность в пользователях для участия в работе организации, вряд ли можно рассчитывать на их эффективное участие в работе организации при отсутствии осведомленности 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 обеспечения осведомленности, включающим в себя:

- преимущества структурного подхода к менеджменту инцидентов ИБ как для организации, так и для ее персонала;
- информацию об инцидентах, хранящуюся в базе данных событий и (или) инцидентов ИБ, и выходные данные из нее;
- стратегию и механизмы для программы обеспечения осведомленности, которая в зависимости от типа организации может быть отдельной программой или частью более широкой программы осведомленности в вопросах ИБ.

5.2.3 Правовые и нормативные аспекты

В политике менеджмента инцидентов ИБ и соответствующей системе необходимо учитывать следующие правовые и нормативные аспекты менеджмента инцидентов ИБ.

Обеспечение адекватной защиты персональных данных и неприкосновенность персональной информации

В странах, где существует специальное законодательство, защищающее конфиденциальность и целостность данных, оно часто ограничено контролем за персональными данными. Поскольку инциденты ИБ обычно возникают в результате деятельности персонала или посторонних лиц, то может потребоваться соответствующая регистрация информации личного характера и управление ею. Следовательно, при структурном подходе к менеджменту инцидентов ИБ следует учитывать необходимость в соответствующей защите персональных данных, а также следующие условия:

- лица, имеющие доступ к персональным данным, не должны лично знать тех людей, информация о которых изучается;
- лица с доступом к личным данным должны подписать соглашение об их неразглашении до того, как получат доступ к ним;
- персональные данные должны использоваться исключительно для тех целей, для которых они были получены, то есть для расследования инцидентов ИБ.

Соответствующее хранение записей

Некоторые федеральные законы Российской Федерации требуют от компаний ведения соответствующих записей своей деятельности для анализа в процессе ежегодного аудита организации. Такие же требования существуют для правительственных организаций. В некоторых странах от организаций требуется составление отчетов или создание архивов для правоохранительных органов (например, в случае совершения серьезного преступления или проникновения в правительственную систему, содержащую конфиденциальную информацию).

Наличие защитных мер для обеспечения выполнения коммерческих договорных обязательств

При наличии обязывающих требований по предоставлению услуг по менеджменту инцидентов ИБ (например требования ко времени реагирования) организация должна предусматривать обеспечение соответствующей ИБ в целях обеспечения выполнения этих обязательств при любых обстоятельствах (в связи с этим в случае заключения организацией контракта со сторонней организацией (см. 7.5.4), например КГБР, необходимо включение всех необходимых требований, наряду с временем реагирования, в контракт со сторонней организацией).

Правовые вопросы, связанные с политиками и процедурами

Необходима проверка политик и процедур, связанных с системой менеджмента инцидентов ИБ, на предмет наличия правовых и нормативных проблем, например, имеются ли уведомления о дисциплинарных взысканиях и (или) судебном преследовании сотрудников, виновных в создании инцидентов, так как в некоторых странах увольнение сотрудников является довольно сложным процессом.

Проверка на законность непризнания ответственности

Все заявления об ограничении ответственности за действия, предпринятые 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 предмет внесения в контракт ответственности за нарушение обязательств по неразглашению, доступности услуг и последствия неправильных консультаций.

Соглашения о неразглашении конфиденциальной информации

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

Исполнение требований правоприменяющих органов

Необходимо обеспечить ясность в вопросах, связанных с возможностью того, что правоприменяющие органы на законном основании могут затребовать информацию от системы менеджмента инцидентов ИБ. В некоторых случаях может потребоваться ясность о минимальном уровне, определяемом законом, на котором инциденты необходимо документировать, и о сроке хранения этой документации.

Ясность в вопросах ответственности

Необходимо уточнить вопросы потенциальной ответственности и необходимые соответствующие защитные меры. Ниже приведены примеры событий, имеющих отношение к возложению ответственности:

- если инцидент ИБ может повлиять на деятельность другой организации (например раскрытие совместно используемой информации), которая вовремя не оповещается и в результате несет ущерб;

- если в продукции обнаружена новая уязвимость без уведомления об этом поставщика, что привело к возникновению серьезного связанного с этой уязвимостью инцидента, в результате которого значительно пострадали одна или несколько организаций;

- если в какой-либо стране, где от организаций требуется информирование или создание архивов для правоохранительных органов в отношении всех случаев, которые могут быть связаны с тяжким преступлением или проникновением в правительственную систему, содержащую информацию ограниченного доступа или элементы критически важной национальной инфраструктуры, соответствующие требования не выполнены;

- если информация раскрыта и появилось указание на причастность некоторого лица или организации к атаке на информационные ресурсы организации. Этот факт может нанести ущерб репутации и бизнесу конкретных лиц или организации;

- если раскрыта информация, что в определенном элементе программного обеспечения произошел сбой, но впоследствии эта информация оказалась ложной.

Специальные нормативные требования

Об инцидентах ИБ следует информировать соответствующий контрольный орган, если это предусмотрено специальными и нормативными требованиями, например, как это предусмотрено в атомной промышленности.

Судебные преследования или внутренние дисциплинарные разбирательства

Для успешного судебного преследования или проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников, независимо от того, были ли эти атаки техническими или физическими, необходимо применять соответствующие меры защиты ИБ, включая доказуемо защищенные от внесения изменений журналы аудита. Для обеспечения успешного судебного преследования или проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников, независимо от того, были ли эти атаки техническими или физическими, необходимо собрать свидетельства для федеральных судов или других административных органов. Необходимо показать, что:

- документация не подвергалась искажениям и является полной;
- копии электронного свидетельства доказуемо идентичны оригиналам;
- все системы ИТ, от которых были получены свидетельства, во время регистрации работали в штатном режиме.

Правовые аспекты, связанные с методами мониторинга

Последствия использования методов мониторинга должны быть рассмотрены в контексте национального законодательства. Законность различных методов может меняться в зависимости от страны. Например, в некоторых странах необходимо информировать людей о ведении мониторинга, в том числе методами наблюдения. Необходимо учесть несколько факторов, определяющих, кто (что) подвергается мониторингу, каким образом они (оно) подвергаются мониторингу и когда проводится мониторинг. Необходимо также отметить, что мониторинг/наблюдение в контексте систем обнаружения вторжений (СОВ) специально рассматривается в [3].

Подготовка правил пользования информационными ресурсами и ознакомление с ними

Порядок использования информационных систем и ресурсов в организации должен быть определен, документирован и доведен до сведения всего предполагаемого персонала (например, персонал необходимо проинформировать о допустимой политике использования и потребовать письменное подтверждение понимания и принятия ими этой политики при устройстве на работу в организацию или получении доступа к информационным системам).

5.2.4 Эффективность эксплуатации и качество

Эффективность эксплуатации и качество структурного подхода к менеджменту инцидентов ИБ зависит от ряда факторов, включающих в себя обязательность уведомления об инцидентах, качество уведомления, простоту использования, быстродействие и обучение. Некоторые из этих факторов связаны с обеспечением осведомленности пользователей о важности менеджмента инцидентов ИБ и их мотивированностью сообщать об инцидентах. Что касается быстродействия, то время, используемое на сообщение об инциденте ИБ, — не единственный фактор, важно также учитывать время, необходимое для обработки данных и распространения обработанной информации (особенно в случае с сигналами аварийности).

Для минимизации задержек соответствующие программы обеспечения осведомленности и обучения пользователей должны дополняться поддержкой по «горячей линии», которая обеспечивается персоналом, осуществляющим менеджмент инцидентов ИБ.

5.2.5 Анонимность

Вопрос обеспечения анонимности является основополагающим для успеха менеджмента инцидентов ИБ. Пользователи должны быть уверены, что информация об инцидентах ИБ, которую они сообщают, полностью защищена, а при необходимости обезличена, с тем чтобы ее невозможно было связать с их организацией или ее подразделением без их согласия.

Система менеджмента инцидентов ИБ должна учитывать ситуации, когда важно обеспечить анонимность лица или организации, сообщающих о потенциальных инцидентах ИБ при особых обстоятельствах. У каждой организации должны быть положения, в которых четко разъяснялись бы важность сохранения анонимности или ее отсутствия для лиц и организаций, сообщающих о потенциальном инциденте ИБ. ГРИИБ может потребоваться дополнительная информация, не сообщенная изначально информирующим об инциденте лицом или организацией. Более того, важная информация об инциденте ИБ может быть получена от первого обнаружившего его лица.

5.2.6 Конфиденциальность

В системе менеджмента инцидентов ИБ может содержаться конфиденциальная информация, и лицам, занимающимся инцидентами, может потребоваться доступ к ней. Поэтому во время обработки необходимо обеспечивать анонимность этой информации, или персонал должен подписать соглаше-

ние о конфиденциальности (неразглашении) при получении доступа к ней. Если события ИБ регистрируют через общую систему менеджмента проблем, то конфиденциальные подробности, возможно, придется опустить.

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

5.2.7 Независимость деятельности группы реагирования на инциденты информационной безопасности

Группа менеджмента инцидентов ИБ должна быть способна эффективно удовлетворять функциональные, финансовые, правовые и политические потребности конкретной организации и быть в состоянии соблюдать осторожность при управлении инцидентами ИБ. Деятельность группы менеджмента инцидентов ИБ должна также подвергаться независимому аудиту с целью проверки эффективности ее функционирования. Эффективным способом реализации независимости контроля является отделение цепочки сообщений о реагировании на инцидент ИБ от общего оперативного руководства и возложение на вышестоящего руководителя непосредственных обязанностей по управлению реагированием на инциденты. Финансирование работы группы, во избежание чрезмерного влияния на нее со стороны, также должно быть отдельным.

5.2.8 Типология

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

6 Примеры инцидентов информационной безопасности и их причин

Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. Инциденты ИБ, о которых не было сообщено, но которые были определены как инциденты, расследовать невозможно и защитных мер для предотвращения повторного появления этих инцидентов применить нельзя.

Ниже приведены некоторые примеры инцидентов ИБ и их причин, которые даются только с целью разъяснения. Важно заметить, что эти примеры не являются исчерпывающими.

6.1 Отказ в обслуживании

Отказ в обслуживании является обширной категорией инцидентов ИБ, имеющих одну общую черту. Подобные инциденты ИБ приводят к неспособности систем, сервисов или сетей продолжать функционирование с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

Существует два основных типа инцидентов ИБ, связанных с отказом в обслуживании, создаваемых техническими средствами: уничтожение ресурсов и истощение ресурсов.

Некоторыми типичными примерами таких преднамеренных технических инцидентов ИБ «отказ в обслуживании» являются:

- зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;
- передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;
- одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы (то есть замедление их работы, блокирование или разрушение).

[1)] Определение общей типологии не является целью настоящего стандарта. Рекомендуется обращение к другим источникам за этой информацией.

Одни технические инциденты ИБ «отказ в обслуживании» могут возникать случайно, например в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного программного обеспечения, а другие — преднамеренными. Одни технические инциденты ИБ «отказ в обслуживании» инициируются намеренно с целью разрушения системы, сервиса и снижения производительности сети, тогда как другие — всего лишь побочными продуктами иной 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 типа «отказ в обслуживании» часто инициируются анонимно (то есть источник атаки неизвестен), поскольку злоумышленник обычно не получает информации об атакуемой сети или системе.

Инциденты ИБ «отказ в обслуживании», создаваемые нетехническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться, например, следующими факторами:

- нарушениями систем физической защиты, приводящими к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;
- случайным нанесением ущерба аппаратуре и (или) ее местоположению от огня или воды/наводнения;
- экстремальными условиями окружающей среды, например высокой температурой (вследствие выхода из строя системы кондиционирования воздуха);
- неправильным функционированием или перегрузкой системы;
- неконтролируемыми изменениями в системе;
- неправильным функционированием программного или аппаратного обеспечения.

6.2 Сбор информации

В общих чертах инциденты ИБ «сбор информации» подразумевают действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки. Подобные инциденты ИБ предполагают проведение разведки с целью определения:

- наличия цели, получения представления об окружающей ее сетевой топологии и о том, с кем обычно эта цель связана обменом информации;
- потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

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

- 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, протокол FTP, сеть 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 и переходит в несанкционированный доступ, если, например, злоумышленник при поиске уязвимости пытается получить несанкционированный доступ. Обычно это осуществляется автоматизированными средствами взлома, которые не только производят поиск уязвимости, но и автоматически пытаются использовать уязвимые системы, сервисы и (или) сети.

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят к:

- 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).

Инциденты могут вызываться, например, следующими факторами:

- 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 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

Несанкционированный доступ как тип инцидента включает в себя инциденты, не вошедшие в первые два типа. Главным образом этот тип инцидентов состоит из несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети. Некоторые примеры несанкционированного доступа с помощью технических средств включают в себя:

- попытки извлечь файлы с паролями;

- 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 расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя или администратора.

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

- разрушением устройств физической защиты с последующим несанкционированным доступом к информации;

- неудачной и (или) неправильной конфигурацией операционной системы вследствие неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения, приводящих к результатам, подобным тем, которые описаны в последнем абзаце 6.2.

7 Этап «Планирование и подготовка»

Этап «Планирование и подготовка» менеджмента инцидентов ИБ включает в себя:

- документирование политики обработки сообщений о событиях и инцидентах ИБ и системе, соответствующей этой политике (включая родственные процедуры);

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

- создание программы обучения и проведения инструктажа с целью обеспечения осведомленности о менеджменте инцидентов.

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

7.1 Общее представление о менеджменте инцидентов информационной безопасности

Для результативного и эффективного ввода менеджмента инцидентов ИБ в эксплуатацию после необходимого планирования следует выполнить ряд подготовительных действий. Эти подготовительные действия включают в себя:

- формулирование и разработку политики менеджмента инцидентов ИБ, а также получение от высшего руководства утверждения этой политики (см. 7.2);

- разработку и документирование подробной системы менеджмента инцидентов ИБ (см. 7.3).

Документация системы менеджмента инцидентов ИБ должна содержать следующие элементы:

- шкалу серьезности для классификации инцидентов ИБ. Как указано в 4.2.1, такая шкала может состоять, например, из двух положений: «значительные» и «незначительные». В любом случае положение шкалы основано на фактическом или предполагаемом ущербе для бизнес-операций организации;

- формы докладов[1] о событиях[2] и инцидентах[3] ИБ (примеры форм приведены в приложении А), соответствующие документированные процедуры и действия, связанные со ссылками на нормальные процедуры использования данных и системы, сервисов и (или) сетевого резервирования, планами обеспечения непрерывности бизнеса;

- операционные процедуры для ГРИИБ с документированными обязанностями и распределением функций среди назначенных ответственных лиц[4] для осуществления различных видов деятельности, например таких, как:

- отключение атакованной системы, сервиса и (или) сети при определенных обстоятельствах по согласованию с соответствующим руководством ИТ и (или) бизнеса и в соответствии с предварительным соглашением;

- оставление атакованной системы, сервиса и (или) сети в работающем состоянии и подсоединенной к сети;

- ведение мониторинга потока входящих, выходящих или находящихся в атакованной системе, сервисе и (или) сети данных;

- активация нормальных дублирующих процедур и действий по планированию непрерывности бизнеса согласно политике безопасности системы, сервиса и (или) сети;

- ведение мониторинга и организация защищенного хранения свидетельств в электронном виде на случай их востребования для судебного разбирательства или дисциплинарного расследования внутри организации;

- передача подробностей об инциденте ИБ сотрудникам своей организации и сторонним лицам или организациям;

- тестирование функционирования системы менеджмента инцидентов ИБ, ее процессов и процедур (см. 7.3.5);

- обновление политик менеджмента и анализа рисков ИБ, корпоративной политики ИБ, специальных политик ИБ для систем, сервисов и (или) сетей для включения ссылок на менеджмент инцидентов ИБ и обеспечение регулярного пересмотра этих политик в контексте выходных данных системы менеджмента инцидентов ИБ (см. 7.4);

- создание ГРИИБ с соответствующей программой обучения ее персонала (см. 7.5);

- технические и другие средства поддержки системы менеджмента инцидентов безопасности ИБ (и деятельности ГРИИБ) (см. 7.6);

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

В следующих подразделах приведено описание каждого вида этой деятельности, включая содержание каждого требуемого документа.

7.2 Политика менеджмента инцидентов информационной безопасности

7.2.1 Назначение политики

Политика менеджмента инцидентов ИБ предназначена для всего персонала, имеющего авторизованный доступ к информационным системам организации и местам их расположения.

7.2.2 Лица, связанные с политикой менеджмента инцидентов информационной безопасности

Политика менеджмента инцидентов ИБ утверждается старшим должностным лицом организации с документально подтвержденными полномочиями, полученными от высшего руководства. Политика должна быть доступна для каждого сотрудника и подрядчика и доведена через инструктаж и обучение с целью обеспечения их осведомленности в области ИБ (см. 7.7).

---

[1] Если возможно, эти формы должны быть представлены в электронном виде (например, на защищенной веб-странице) и связаны с базой данных, хранящей электронную информацию о событиях/инцидентах ИБ. В настоящее время бумажная технология требовала бы слишком много времени и была бы неэффективной.

[2] Форму заполняет лицо, принимающее сообщение (то есть не член группы менеджмента инцидентов ИБ).

[3] Эта форма используется персоналом менеджмента инцидентов ИБ для пополнения первоначальной информацией о событии ИБ, текущего ведения записей оценок инцидента и пр. до полного разрешения инцидента. На каждой стадии в базу данных событий/инцидентов ИБ включаются обновления. Запись в базе данных, содержащая «заполненную» форму или сведения о событиях/инцидентах ИБ, далее используется в деятельности по разрешению инцидента.

[4] В небольших организациях одно и то же лицо может выполнять несколько функций.

7.2.3 Содержание политики менеджмента инцидентов информационной безопасности

Политика менеджмента инцидентов ИБ должна включать в себя следующие вопросы:

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

- общее представление об обнаружении событий ИБ, оповещении о них и сборе соответствующей информации, а также о путях использования этой информации для определения инцидентов ИБ. Это общее представление должно содержать перечень возможных событий ИБ, а также информацию о том, как сообщать о ней, что, где и кому сообщать, а также как обращаться с совершенно новыми событиями ИБ;

- общее представление об оценке инцидентов ИБ, включая перечень ответственных лиц, необходимые для выполнения действия, уведомления об инцидентах и дальнейшие действия ответственных лиц;

- краткое изложение действий после подтверждения того, что событие ИБ является инцидентом ИБ. Эти действия представляют:

- немедленное реагирование;

- правовую экспертизу;

- передачу информации соответствующему персоналу или сторонним организациям;

- проверку, находится ли инцидент ИБ под контролем;

- дальнейшее реагирование;

- объявление «кризисной ситуации»;

- определение критериев усиления реагирования на инциденты ИБ;

- определение ответственного за инцидент лица;

- ссылку на необходимость правильной регистрации всех действий для дальнейшего и непрерывного мониторинга с целью обеспечения защищенного хранения свидетельств в электронном виде на случай их востребования для судебного разбирательства или дисциплинарного расследования внутри организации;

- действия, следующие за разрешением инцидента ИБ, включая извлечение урока из инцидента и улучшение процесса, следующего за инцидентами ИБ;

- подробности места хранения документации о системе, включая процедуры хранения;

- общее представление о деятельности ГРИИБ, включающее в себя следующие вопросы:

- организационную структуру ГРИИБ и весь основной персонал группы, включая лиц, ответственных за:

- краткое информирование высшего руководства об инцидентах;

- проведение расследований и другие действия персонала группы после объявления «кризисной ситуации»;

- связь со сторонними организациями (при необходимости);

- положение о менеджменте ИБ, область деятельности ГРИИБ и полномочия, в рамках которых она будет ее осуществлять. Это положение должно включать в себя, как минимум, формулировку целевого назначения, определение области деятельности ГРИИБ и подробности об учредителе ГРИИБ и его полномочиях;

- формулировку целей ГРИИБ применительно к основной деятельности группы персонала. Для выполнения своих функций персонал должен участвовать в оценке инцидентов ИБ, реагировании на них и управлении ими, а также в их успешном разрешении. Для целей и назначения ГРИИБ требуется четкое и однозначное определение;

- определение сферы деятельности ГРИИБ. Обычно в сферу деятельности ГРИИБ организации входят все информационные системы, сервисы и сети организации. В некоторых случаях для организации может потребоваться сужение сферы действия ГРИИБ. При этом необходимо четко документировать, что входит и что не входит в сферу ее деятельности;

- личность учредителя ГРИИБ — старшего должностного лица (член правления, старший руководитель), который санкционирует действия ГРИИБ и устанавливает уровни полномочий, переданных ГРИИБ. Осведомленность об этом поможет всему персоналу организации понять предпосылки создания и структуру ГРИИБ, что является крайне важной информацией для формирования доверия к ГРИИБ. Следует отметить, что перед обнародованием подробностей о создании и структуре ГРИИБ необходимо проверить законность этого действия. В некоторых обстоятельствах раскрытие полномочий группы персонала может послужить причиной предъявления ей претензий по нарушению обязательств;

- общее представление о программе обеспечения осведомленности и обучения менеджменту инцидентов ИБ;

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

7.3 Программа менеджмента инцидентов информационной безопасности

7.3.1 Назначение системы

Программа менеджмента инцидентов ИБ предназначена для создания подробной документации, описывающей процессы и процедуры обработки инцидентов ИБ и оповещения (информирования) об инцидентах ИБ. Программа менеджмента ИБ приводится в действие при обнаружении события ИБ. Она используется в качестве руководства при:

- реагировании на события ИБ;

- определении того, становятся ли события ИБ инцидентами ИБ;

- менеджменте инцидентов ИБ до их разрешения;

- идентификации полученных уроков при обработке инцидентов, а также необходимых улучшений системы и (или) безопасности в целом;

- реализации идентифицированных улучшений.

7.3.2 Лица, связанные с программой менеджмента инцидентов информационной безопасности

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

- обнаружение и оповещение о событиях ИБ. Эти лица могут быть служащими, работающими на постоянной основе или по контракту;

- оценку и реагирование на события ИБ и инциденты ИБ, которые участвуют в извлечении уроков на этапе разрешения инцидентов ИБ и в улучшениях ИБ и самой программы менеджмента инцидентов ИБ. Этими лицами являются члены группы обеспечения эксплуатации (или подобной группы), ГРИИБ, руководство организации, персонал отделов по связям с общественностью и юристы.

Следует также учитывать пользователей третьей стороны, 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 программы менеджмента инцидентов информационной безопасности

В содержание программы менеджмента инцидентов ИБ должны быть включены:

- обзор политики менеджмента инцидентов ИБ;

- общее представление о программе менеджмента инцидентов ИБ в целом;

- детальные процессы и процедуры[1)], информация о соответствующих сервисных программах и шкалах, связанных:

для этапа «Планирование и подготовка»:

с обнаружением и оповещением о появлении событий ИБ (человеком или автоматическими средствами),

со сбором информации о событиях ИБ,

с проведением оценок событий ИБ (включая, если потребуется, их детализацию), используя принятую шкалу серьезности событий/инцидентов, и определением их способности к изменению своей категории на категорию инцидентов ИБ,

для этапа «Использование» (в случае подтверждения инцидентов ИБ):

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 в себя активизацию процедур восстановления и (или) передачу сообщений соответствующему персоналу согласно анализу и принятым степенями шкалы серьезности инцидентов,

с проведением правовой экспертизы (при необходимости) по степеням шкалы серьезности инцидентов ИБ и изменением этих степеней,

с определением наличия контроля над инцидентами ИБ,

с созданием дополнительных реагирований (если требуется), включая те, которые могут потребоваться гораздо позднее (например, при устранении последствий какого-либо бедствия),

---

[1)] Организация может принимать решения о включении всех процедур в программу или подробном изложении в дополнительных документах всех или некоторых процедур.

в случае отсутствия контроля над инцидентами ИБ с инициированием антикризисных действий (например, вызов пожарной команды или активизация плана обеспечения непрерывности бизнеса),

с детализацией дальнейшей оценки и (или), если потребуется, дальнейших решений,

с проверкой правильности регистрации всей деятельности для дальнейшего анализа,

с обновлением базы данных событий/инцидентов ИБ.

В программе менеджмента инцидентов ИБ предусматривается возможность как немедленного, так и более длительного реагирования на инциденты ИБ. Для всех инцидентов ИБ требуется своевременная оценка потенциальных негативных воздействий, как кратковременных, так и более длительных (например, крупномасштабное бедствие может произойти через некоторое время после первого инцидента ИБ). Более того, некоторые виды реагирования могут потребоваться для совершенно непредвиденных инцидентов ИБ, когда возникнет необходимость в специальных защитных мерах. Даже в такой ситуации в документации программы должны содержаться общие рекомендации по действиям, которые могут стать необходимыми:

- для этапа «Анализ»:

с проведением, если потребуется, дальнейшей правовой экспертизы,

с идентификацией и документированием опыта, извлеченного из инцидентов ИБ,

с определением и анализом улучшений ИБ на основе полученного опыта,

с анализом эффективности процессов и процедур реагирования на инциденты ИБ, оценкой инцидентов ИБ и восстановления после каждого из них, а также определением улучшений программы менеджмента инцидентов ИБ в целом (на основе полученного опыта),

с обновлением базы данных событий/инцидентов ИБ;

- для этапа «Улучшение» — уточнение на основе полученного опыта:

с результатами анализа и менеджмента рисков ИБ,

с программой менеджмента инцидентов ИБ (например, процессами и процедурами, формой оповещения и (или) структурой организации),

с общей безопасностью внедрения новых и (или) улучшенных защитных мер,

с градацией шкалы серьезности событий/инцидентов (например, значительный, незначительный; существенный, экстренный, незначительный, неэкстренный) и соответствующими руководствами,

с руководством для решения о необходимости интенсификации каждого процесса, для кого должна проводиться интенсификация и в соответствии с какими процедурами. Персонал, оценивающий событие или инцидент ИБ, должен знать, основываясь на руководствах из документации программы менеджмента инцидентов ИБ, когда при нормальных обстоятельствах необходимо переходить к интенсификации процессов и для кого. Кроме того, возможно возникновение непредвиденных обстоятельств, когда интенсификация процессов может стать необходимой. Например, незначительный инцидент ИБ может перейти в категорию «существенный» или в «кризисную ситуацию» в случае его неправильной обработки, или незначительный инцидент ИБ, не обработанный в течение недели, может стать «значительным» инцидентом ИБ. В руководстве должны определяться типы событий и инцидентов ИБ, типы интенсификации процессов и лица, которые могут ее проводить,

с необходимыми процедурами для надлежащей регистрации всех действий в соответствующей форме и проведением анализа журнала регистрации назначенным персоналом,

с процедурами и механизмами поддержания режима контроля изменений, который включает в себя прослеживание событий и инцидентов ИБ, обновление отчета об инцидентах ИБ и обновление самой программы,

с процедурами правовой экспертизы,

с процедурами и руководством по использованию систем обнаружения вторжений (СОВ), обеспечивающими соблюдение связанных с ними правовых и нормативных аспектов (см. 5.2.3). Руководство должно включать в себя рассмотрение преимуществ и недостатков действий по наблюдению за злоумышленником. Дополнительная информация по системам обнаружения вторжений (СОВ) содержится в ИСО/МЭК ТО 15947 [2] и ИСО/МЭК ТО 18043 [3],

со структурой организации программы,

с компетенцией и обязанностями членов ГРИИБ в целом и ее отдельных членов,

с важной информацией о контактах группы.

7.3.4 Процедуры

Перед тем как приступить к работе с программой менеджмента инцидентов ИБ, необходимо иметь в наличии документированные и проверенные процедуры. В документации по каждой процедуре дол-

жны указываться лица из группы эксплуатационной поддержки и (или) из ГРИИБ, ответственные за использование и менеджмент этой процедуры. Такие процедуры должны включать в себя процедуры сбора и защищенного хранения электронных свидетельств, которые должны непрерывно контролироваться на случай судебного разбирательства или дисциплинарного расследования внутри организации. Более того, должны существовать документированные процедуры, включающие в себя не только действия группы эксплуатационной поддержки и ГРИИБ, но и процедуры, задействованные в правовой экспертизе и «антикризисной» деятельности, если они не задействованы где-либо еще, например, в плане обеспечения непрерывности бизнеса. Очевидно, что эти документированные процедуры должны полностью соответствовать документированной политике менеджмента инцидентов ИБ и другой документации программы менеджмента инцидентов ИБ.

Необходимо иметь в виду, что не все процедуры являются общедоступными. Например, нежелательно, чтобы весь персонал организации знал подробности о работе ГРИИБ при взаимодействии с ней. ГРИИБ должна обеспечивать наличие «общедоступного» руководства, включая информацию, полученную из результатов анализа инцидентов ИБ, которая находится в легкодоступной форме, например в интранете организации. Более того, иногда нежелательно раскрывать некоторые детали программы менеджмента инцидентов ИБ, чтобы лицо, обладающее конфиденциальной информацией внутри организации (инсайдер), не могло помешать процессу расследования. Например, если банковский служащий, присваивающий денежные средства, осведомлен о некоторых деталях программы, то он может лучше скрывать свою деятельность от следствия или иным образом препятствовать обнаружению и расследованию инцидента ИБ и восстановлению после него.

Содержание рабочих процедур зависит от многих критериев, особенно связанных с характером уже известных потенциальных событий и инцидентов ИБ и типами задействованных 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 необходимо предпринять 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 уже известных типов событий и инцидентов ИБ должны существовать рабочие процедуры. Необходимы также рабочие процедуры, которым надо следовать, если тип обнаруженного инцидента ИБ или события неизвестен. В этом случае рассматривают следующие аспекты:

- процесс оповещения для обработки таких «исключительных случаев»;
- указания, определяющие время для получения одобрения реагирования на инцидент со стороны руководства с целью избежания задержки реагирования;
- предварительно одобренное делегирование принятия решения без обычного процесса одобрения.

7.3.5 Тестирование программы

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 реагирований на инциденты ИБ, должны подвергаться строгой проверке и тестированию.

7.4 Политики менеджмента рисков и информационной безопасности

7.4.1 Назначение

Целями включения содержания менеджмента инцидентов ИБ в корпоративные политики менеджмента рисков и ИБ и специальные политики ИБ систем, сервисов и сетей являются:

- описание значимости менеджмента инцидентов ИБ, особенно системы оповещения и обработки инцидентов ИБ;
- указание обязанностей высшего руководства относительно надлежащей подготовки к инцидентам ИБ и реагированию на них, то есть относительно системы менеджмента инцидентов ИБ;
- обеспечение согласованности различных политик;
- обеспечение планового и систематического реагирования на инцидент ИБ для минимизации негативного воздействия инцидентов.

7.4.2 Содержание

Корпоративная политика менеджмента рисков и ИБ, а также специальные политики ИБ для систем, сервисов или сетей должны обновляться с целью обеспечения точного соответствия общей по-

литике менеджмента инцидентов ИБ и соответствующей ей системе. В соответствующие разделы необходимо включать обязательства высшего руководства и описание:

- политики;
- процессов системы и соответствующей инфраструктуры;
- требований по обнаружению, оповещению, оценке и управлению инцидентами и
- четкого определения персонала, ответственного за авторизацию и (или) проведение определенных важных действий (например перевод информационной системы в режим off-line или даже отключение системы).

Кроме того, корпоративная политика должна содержать 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 стабильной результативности корпоративных 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 группы реагирования на инциденты информационной безопасности

Целью создания ГРИИБ является обеспечение организации соответствующим персоналом для оценки, реагирования на инциденты ИБ и извлечения уроков из них, а также необходимой координации, менеджмента, обратной связи и процесса передачи информации. Члены ГРИИБ могут участвовать в снижении физического и финансового ущерба, а также ущерба для репутации организации, связанного с инцидентами ИБ.

7.5.2 Члены группы реагирования на инциденты информационной безопасности и структура этой группы

Состав и количество персонала, а также структура ГРИИБ должны соответствовать масштабу и структуре организации. ГРИИБ может представлять собой изолированную команду или отдел, персонал этой группы может выполнять и другие обязанности, а также привлекать сотрудников из различных подразделений организации. В соответствии с 4.2.1 и 7.1 во многих случаях ГРИИБ может быть действующей группой, возглавляемой старшим руководителем. Вышестоящему руководителю оказывают помощь специалисты по конкретным вопросам, например, по отражению атак вредоносных программ, которые привлекаются в зависимости от типа инцидента ИБ. В зависимости от численного состава организации сотрудники ГРИИБ могут также выполнять несколько функций внутри ГРИИБ. В ГРИИБ могут также привлекаться служащие из различных подразделений организации (например бизнес-операций, ИТ/телекоммуникаций, аудита, отдела кадров и маркетинга).

Члены группы должны быть доступны для контакта так, чтобы их имена и имена лиц, их замещающих, а также подробности о контакте с ними были доступными внутри организации. Например, в документации системы менеджмента инцидентов ИБ должны быть четко указаны необходимые детали, включая любые документы по процедурам и формы отчетов, но не в положениях политики.

Руководитель ГРИИБ должен:

- иметь делегированные полномочия немедленного принятия решения о том, какие меры предпринять относительно инцидента;
- как правило, иметь отдельную линию для оповещения высшего руководства, которая должна быть изолирована от обычных бизнес-операций;
- обеспечивать необходимый уровень знаний и мастерства для всех членов ГРИИБ, а также поддержание этого уровня;
- поручать расследование каждого инцидента наиболее компетентному члену группы.

7.5.3 Взаимодействие с другими подразделениями организации

Уровень полномочий руководителя ГРИИБ и членов его группы должен позволять предпринимать необходимые действия, адекватные инциденту ИБ.

Однако действия, которые могут оказать неблагоприятное влияние на всю организацию в отношении финансов или репутации, должны согласовываться с высшим руководством. Поэтому важно уточнить, какой орган в системе обеспечения политики менеджмента инцидентов ИБ руководитель ГРИИБ оповещает о серьезных инцидентах ИБ.

Процедуры общения со СМИ и ответственность за это общение также должны быть согласованы со старшим руководством, документированы и определять:

- представителя организации по работе со средствами массовой информации;
- метод взаимодействия подразделения организации 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 КГБР;
- ГРИИБ сторонних организаций, а также КГБР;
- правоприменяющие организации;
- аварийные службы (например пожарная бригада/отделение);
- соответствующие государственные организации;
- юридический персонал;
- официальные лица по связям с общественностью и (или) представителями средств массовой информации;
- партнеры по бизнесу;
- потребители;
- общественность.

7.6 Техническая и другая поддержка реагирования на инциденты информационной безопасности

Быстрое и эффективное реагирование на инциденты ИБ осуществляется гораздо легче, когда все необходимые технические и другие средства поддержки получены, подготовлены и протестированы. Эти мероприятия включают в себя:

- доступ к деталям активов организации (предпочтительно иметь обновленный перечень активов) и информацию по их связям с бизнес-функциями;
- доступ к документированной стратегии обеспечения непрерывности бизнеса и соответствующим планам;
- документированные и опубликованные процессы передачи информации;
- использование электронной базы данных событий/инцидентов ИБ и технических средств для быстрого пополнения и обновления базы данных, анализа ее информации и упрощения процессов реагирования (хотя общепризнанно, что иногда сделанные вручную записи также оказываются востребованными и используются организацией);
- адекватные меры по обеспечению непрерывности бизнеса для базы данных событий/инцидентов ИБ.

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

- быстрому получению отчетов о событиях и инцидентах ИБ;
- уведомлению ранее отобранного персонала (соответствующих сторонних лиц) подходящими для этого средствами (например, через электронную почту, факс, телефон и т. д.), то есть запрашивая поддержку надежной контактной базы данных (которая должна быть всегда легкодоступной и должна включать в себя бумажные и другие копии) и средство передачи информации безопасным способом (при необходимости);
- соблюдению предосторожностей, соответствующих оцененным рискам, избежанию прослушивания электронной связи, реализуемой через Интернет или иным образом, во время атаки на систему, сервис и (или) сеть;
- соблюдению предосторожностей, соответствующих оцененным рискам, для сохранения доступности электронной связи, реализуемой через Интернет или иным образом, во время атаки на систему, сервис и (или) сеть;
- процессу сбора всех данных об информационной системе, сервисе и (или) сети и всех обрабатываемых данных;
- использованию криптографического контроля целостности, если это соответствует оцененным рискам, для содействия в определении наличия изменений и того, какие части системы, сервиса и(или) сети и данные подверглись изменениям;
- упрощению архивирования и защиты собранной информации (например, применяя цифровые подписи в записях в журнале регистрации или другие свидетельства перед хранением в автономном режиме на носителях, предназначенных только для чтения на устройствах CD или DVD ROM);

- подготовке распечаток (например, журналов регистрации), демонстрирующих развитие инцидента ИБ, процесс разрешения инцидента и обеспечивающих сохранность информации;

- восстановлению 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,

надежных и обновленных исправлений («патчей») для систем и приложений, согласованных с соответствующим планом обеспечения непрерывности бизнеса.

Атакованная информационная система, сервис и (или) сеть могут функционировать неверно. Поэтому работа технического средства (программного или аппаратного обеспечения), необходимого для реагирования на инцидент ИБ, не должна быть основана на системах, сервисах и (или) сетях, используемых в организации. По возможности, технические средства реагирования на инциденты должны быть полностью автономными.

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

Следует заметить, что технические средства, описанные в настоящем подразделе, не включают в себя технические средства, используемые непосредственно для обнаружения инцидентов ИБ и вторжений и автоматического оповещения соответствующих лиц. Данные технические средства описаны в [1], [2].

7.7 Обеспечение осведомленности и обучение

Менеджмент инцидентов ИБ — это процесс, включающий в себя не только технические средства, но также персонал, и, следовательно, этот процесс должен поддерживаться лицами, 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 менеджмента 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 подготовки, зависящие от типа, частоты и значимости их взаимодействия с системой менеджмента инцидентов ИБ.

Инструктажи по обеспечению осведомленности должны включать в себя:

- основы работы системы менеджмента инцидентов ИБ, включая сферу ее действия и технологию работ по менеджменту инцидентов и событий ИБ;
- способы оповещения о событиях и инцидентах ИБ;
- защитные меры по обеспечению конфиденциальности источников (по необходимости);
- соглашения об уровнях сервиса системы;
- уведомление о результатах — на каких условиях будут информированы источники;
- любые ограничения, налагаемые 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 включать 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 предоставить ценную информацию, связанную с определенными группами сотрудников, 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 специально ото-

бранный персонал должен быть хорошо осведомлен в отношении последующих процессов. Затем проводят регулярные инструктажи по обеспечению осведомленности и курсы подготовки. Подготовка должна сопровождаться специальными упражнениями и тестированием членов группы обеспечения эксплуатации и ГРИИБ, а также персонала, ответственного за ИБ, и специальных администраторов.

8 Этап «Использование»

8.1 Введение

Менеджмент инцидентов ИБ в процессе эксплуатации состоит из двух главных этапов: «Использование» и «Анализ», за которыми следует этап «Улучшение», на котором проводят любые усовершенствования, идентифицированные в результате извлечения уроков из инцидентов ИБ. Эти этапы и связанные с ними процессы представлены в подразделе 4.2. В настоящем разделе рассматривается этап «Использование», в разделе 9 — этап «Анализ», а в разделе 10 — этап «Улучшение». Эти три этапа и соответствующие им процессы представлены на рисунке 2.

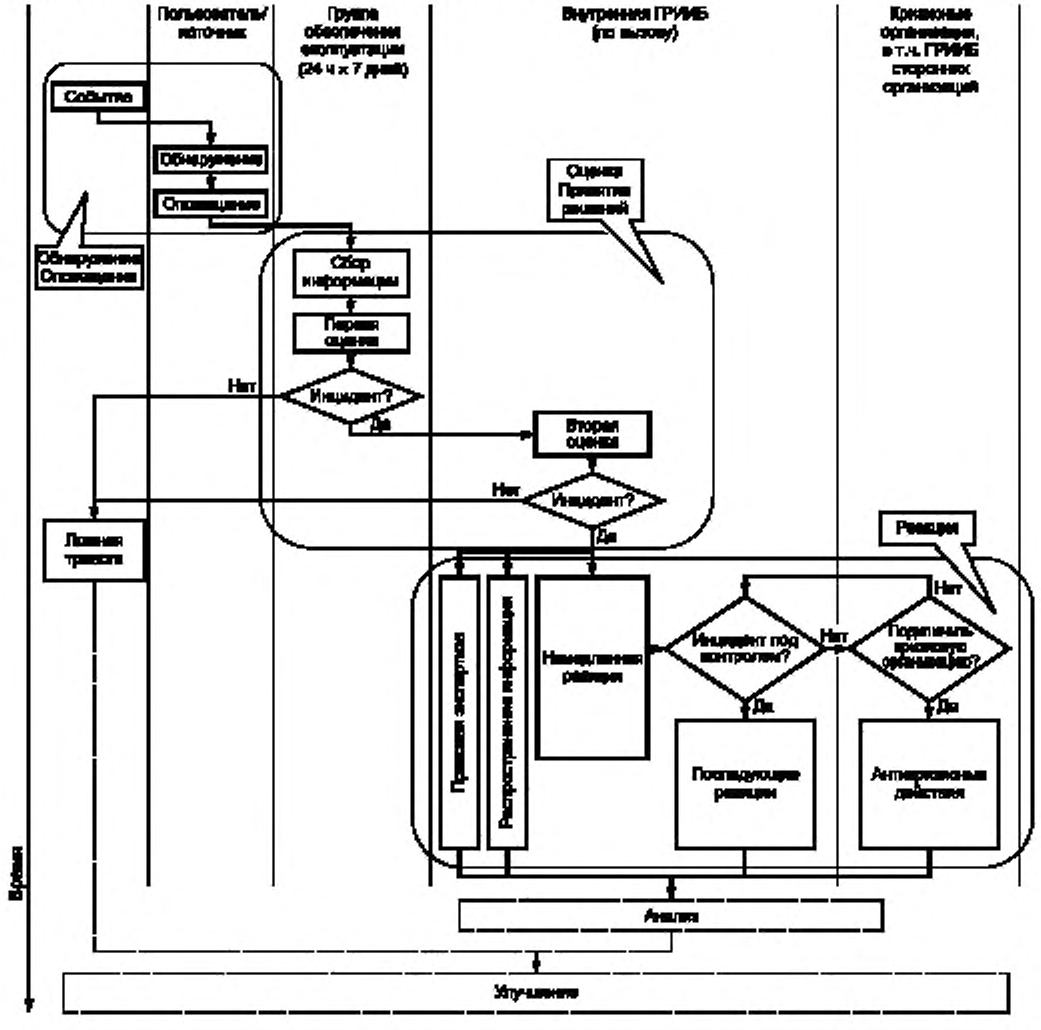


Рисунок 2 — Блок-схема последовательности операций обработки событий и инцидентов ИБ (этап «Использование»)

8.2 Обзор ключевых процессов

В этапе «Использование» ключевыми процессами являются:

- обнаружение события ИБ и оповещение о нем одним из сотрудников персонала/клиентом 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;

- проведение второй оценки ГРИИБ с целью подтвердить, что событие является инцидентом ИБ и, в положительном случае, инициировать немедленное реагирование, а также необходимость правовой экспертизы и действий по передаче информации;

- анализ, проводимый ГРИИБ с целью определить, находится ли инцидент под контролем:

в положительном случае инициируется дальнейшее необходимое реагирование и обеспечивается готовность всей информации для использования в процессе анализа последствий инцидента,

при отрицательном ответе инициируются антикризисные действия с привлечением соответствующего персонала, например руководителя и группы обеспечения непрерывности бизнеса организации;

- расширение области действия 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 дальнейшего анализа;

- обеспечение сбора и защищенного хранения свидетельств в электронном виде и постоянного мониторинга защищенного хранения этих свидетельств на случай их востребованности для судебного преследования или внутреннего дисциплинарного разбирательства;

- поддержка режима контроля изменений, включая отслеживание инцидентов ИБ и обновления отчетов по инцидентам с тем, чтобы база данных событий/инцидентов ИБ постоянно соответствовала действительности.

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 быть как можно более полной в любое время, чтобы обеспечить наиболее прочную основу для оценок и принятия решений, а также для предпринимаемых действий.

После обнаружения события ИБ и сообщения о нем целями последующих процессов являются:

- распределение ответственности за деятельность, связанную с менеджментом инцидентов, через соответствующую иерархию персонала вместе с оценкой и принятием решений, а также за действия с привлечением персонала как связанного, так и не связанного с обеспечением безопасности;

- обеспечение формальных процедур для каждого оповещенного лица, включая анализ и корректировку сделанного сообщения, оценку ущерба и уведомление 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 инциденту ИБ, то и для последующих действий в отношении инцидента ИБ и обновления базы данных событий/инцидентов ИБ.

Рекомендации приведены:

по обнаружению и оповещению о событиях ИБ — в 8.3, оценке и принятию решений (является ли событие инцидентом ИБ) — в 8.4, реагированию на инциденты ИБ — в 8.5 и включают в себя:

- немедленное реагирование,
- анализ с целью определения, находится ли инцидент ИБ под контролем,
- последующие реагирования,
- антикризисные действия,
- правовую экспертизу,
- передачу информации,
- комментарий по вопросам расширения сферы менеджмента инцидентов ИБ,
- регистрацию деятельности.

8.3 Обнаружение и оповещение о событиях информационной безопасности

События ИБ могут быть обнаружены непосредственно лицом или лицами, заметившими что-либо, вызывающее беспокойство и имеющее технический, физический или процедурный характер. Обнаруже-

---

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

ние 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, это могут быть сигналы тревоги, производимые устройствами анализа записей аудита, межсетевыми экранами, системами обнаружения вторжений, антивирусными программами, в каждом случае стимулируемые заранее установленными параметрами этих устройств.

Независимо от причины обнаружения события ИБ, лицо, непосредственно обратившее внимание на нечто необычное или оповещенное автоматическими средствами, несет ответственность за инициирование процесса обнаружения и оповещения. Этим лицом может быть любой представитель персонала организации, работающий постоянно или по контракту. Этот представитель должен следовать процедурам и использовать форму отчета о событиях ИБ, определенную системой менеджмента инцидентов ИБ, с целью привлечения внимания, прежде всего, группы обеспечения эксплуатации и менеджмента. Следовательно, важно, чтобы весь персонал был ознакомлен с рекомендациями, относящимися к вопросу оповещения о возможных событиях ИБ, включая формы отчета, имел доступ к ним и знал сотрудников, которых необходимо оповещать о каждом случае появления события ИБ. Необходимо, чтобы весь персонал организации был, по крайней мере, осведомлен о форме отчета, что способствовало бы его пониманию системы менеджмента инцидентов ИБ.

Обработка конкретного события ИБ зависит от того, что оно собой представляет, а также от последствий и воздействий, к которым это событие может привести. Для многих людей принятие решения о способе обработки события выходит за пределы их компетентности. Поэтому сотрудник, информирующий о событии ИБ, должен заполнить форму отчета так, чтобы в ней было как можно больше информации, доступной ему на тот момент. При необходимости он связывается со своим руководителем. Желательно, чтобы эта форма была в электронном виде (например, послана по электронной почте или представлена на веб-сайте), чтобы ее можно было передать безопасным способом в надлежащую группу обеспечения эксплуатации (работающую, по возможности, 24 ч в сутки по семь дней в неделю), а копию сообщения — руководителю ГРИИБ. Образец формы отчета сообщения о событии ИБ приведен в приложении А.

Следует подчеркнуть, что при заполнении формы отчета важна не только точность содержания, но и своевременность заполнения. Не следует задерживать представление формы отчета о событии ИБ по причине уточнения ее содержания. Если сообщающий сотрудник не уверен в данных какого-либо поля в форме отчета, то это поле должно быть помечено, а уточнение — послано позже. Также следует признать, что некоторые механизмы электронного оповещения (например электронная почта) сами являются очевидными целями атаки.

При наличии проблем или при существовании мнения о наличии проблем с установленными по умолчанию механизмами электронного оповещения (например электронной почтой), включая случаи атаки на систему и считывание формы отчета несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть нарочные, телефон, текстовые сообщения. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться значительным.

Следует заметить, что, хотя в большинстве случаев группа обеспечения эксплуатации должна сообщать о событии ИБ с целью его дальнейшей обработки, могут быть случаи, когда событие ИБ может быть обработано на месте с помощью местного руководства. Событие ИБ можно быстро распознать как ложную тревогу или успешно разрешить. В этих случаях форму отчетов необходимо заполнить и отправить местному руководству, а также группе обеспечения эксплуатации и ГРИИБ с целью ее регистрации в базе данных событий/инцидентов ИБ. В этом случае лицо, сообщающее о закрытии события ИБ, может предоставить информацию, требуемую для заполнения формы отчета об инцидентах ИБ. В этом случае такая форма отчета об инциденте ИБ должна быть заполнена и отправлена по инстанции.

8.4 Оценка и принятие решений по событиям/инцидентам

8.4.1 Первая оценка и предварительное решение

В группе обеспечения эксплуатации системы менеджмента инцидентов ИБ принимающее лицо должно подтвердить получение заполненной формы отчета, ввести ее в базу данных событий/инцидентов ИБ и проанализировать данную форму отчета. Далее должностное лицо должно попытаться получить любые уточнения от сообщившего лица о событии ИБ и собрать требуемую дополнительную информацию, считающуюся доступной, как от сообщившего о событии лица, так и из любого другого места. Затем представитель группы обеспечения эксплуатации должен провести оценку для определения, подходит ли это событие под категорию инцидента ИБ или является ложным. Если событие ИБ

определяется как ложное, необходимо заполнить форму отчета и передать в ГРИИБ для записи в базу данных и дальнейшего анализа, а также создать копии для сообщившего о событии 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 хорошо знать требования по сбору и сохранению свидетельств.

Дополнительно к дате (датам) и времени выполнения действий необходимо полностью документировать:

- проведенные мероприятия (включая использованные средства) и их цели;
- место хранения свидетельства наличия события;
- способ архивирования свидетельства (если оно уместно);
- способ верификации свидетельства (если оно уместно);
- 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 проводится дальнейшая оценка. В результате могут потребоваться корректирующие действия, например идентификация дополнительных «аварийных» защитных мер и обращение за помощью в их реализации к соответствующему лицу. Событие ИБ может быть определено как инцидент ИБ, причем значительный (по шкале серьезности, принятой в организации), в этом случае необходимо проинформировать непосредственно руководителя ГРИИБ. Может потребоваться объявление «кризисной ситуации» и, как следствие, уведомление руководителя обеспечения непрерывности бизнеса о возможной активизации плана обеспечения непрерывности бизнеса с одновременным информированием руководителя ГРИИБ и вышестоящего руководства. Однако наиболее вероятна ситуация передачи инцидента ИБ непосредственно в ГРИИБ для дальнейшей оценки и выполнения соответствующих действий.

Каким бы ни был следующий шаг, сотрудник группы обеспечения эксплуатации должен заполнить форму отчета по возможности наиболее подробно. Образец формы отчета по инциденту ИБ приведен в приложении А. Отчет должен содержать информацию в описательном виде и, насколько это возможно, характеризовать:

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

При рассмотрении потенциального или фактического негативного воздействия инцидента на бизнес организации в результате несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и(или) сервиса, уничтожения информации и(или) сервиса в первую очередь необходимо определить, какое из перечисленных ниже последствий будет иметь инцидент ИБ.

Примерами последствий ИБ являются:

- финансовые убытки/прерывание бизнес-операций;
- ущерб коммерческим и экономическим интересам;
- ущерб информации, содержащей персональные данные;
- нарушение правовых и нормативных обязательств;
- сбои операций по менеджменту и бизнес-операций;
- утрата престижа организации.

Для категорий, отнесенных к инциденту ИБ, должны использоваться соответствующие рекомендации по категорированию потенциальных или фактических воздействий для внесения их в отчет по инцидентам ИБ. Примеры рекомендаций приведены в приложении В.

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

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

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

Важно, чтобы сотрудник группы обеспечения эксплуатации, оценивающий инцидент ИБ, основываясь на руководстве, содержащемся в документации системы менеджмента инцидентов ИБ, был осведомлен о том:

- когда и кому необходимо направлять материалы об инциденте;
- что при осуществлении всех действий, выполняемых группой обеспечения эксплуатации, необходимо выполнять документированные процедуры контроля изменений.

При наличии проблем или мнения о том, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например электронной почтой), включая случаи атаки на информационную систему и считывание несанкционированными лицами формы отчета об инцидентах ИБ, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть: телефон, текстовые сообщения, а также курьеры. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться «значительным».

8.4.2 Вторая оценка и подтверждение инцидента информационной безопасности

Вторая оценка и подтверждение инцидента ИБ или какое-либо другое решение относительно того, надо ли отнести событие ИБ к инциденту ИБ, должны входить в обязанности ГРИИБ. Принимающий отчеты сотрудник ГРИИБ должен:

- подтвердить получение 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 дополнительную необходимую информацию о событии ИБ (если существует) от группы обеспечения эксплуатации, лица, заполнившего отчетную форму, или из какого-либо иного источника.

Если все еще остается какая-либо неопределенность относительно аутентичности инцидента ИБ или полноты полученной информации, то сотрудник ГРИИБ должен провести вторую оценку для определения реальности или ложности инцидента ИБ. Если инцидент ИБ определен как «ложный», необходимо заполнить отчет о событии ИБ, добавить его в базу данных событий/инцидентов ИБ и передать руководителю ГРИИБ. Копии отчета необходимо передать 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:

- того, что представляет собой инцидент ИБ, что явилось его причиной, чем или кем был вызван, на что повлиял или мог повлиять, воздействие или потенциальное воздействие инцидента ИБ на бизнес организации, указание на вероятную значительность/незначительность инцидента (по шкале серьезности инцидентов, принятой в организации);
- предумышленной технической атаки нарушителя на некоторую информационную систему, сервис и (или) сеть, например:

глубины проникновения нарушителя в систему, сервис и (или) сеть и степень контроля, которой он обладает,

данных об информации, к которой получил доступ нарушитель, были ли они скопированы, изменены или удалены,

о том, какое программное обеспечение было скопировано, изменено или разрушено нарушителем;

в отношении предумышленной физической атаки нарушителя на любую информационную систему аппаратной части, сервиса и (или) на сеть, и (или) на физическое месторасположение, например:

масштаба прямых и косвенных последствий нанесенного физического ущерба (при отсутствии физической защиты доступа),

прямых и косвенных последствий в отношении инцидентов ИБ, косвенно созданных действиями нарушителя (например, стал ли физический доступ возможным по причине пожара, является ли уязвимость информационной системы следствием неправильного функционирования программного обеспечения, линии связи или ошибки оператора),

- используемого до настоящего времени способа обработки инцидента ИБ.

При анализе потенциального или реального негативного воздействия инцидента ИБ на бизнес организации вследствие несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и (или) сервиса, разрушения информации и (или) сервиса необходимо подтвердить, какие последствия имели место вследствие данного инцидента. Примерами категорий последствий являются:

- финансовые убытки/разрушение бизнес-операций;
- ущерб коммерческим и экономическим интересам;
- ущерб для информации, содержащей персональные данные;
- нарушение правовых и нормативных обязательств;
- ущерб для менеджмента и бизнес-операций;
- утрата престижа организации.

Для отнесения потенциальных или фактических воздействий к той или иной категории необходимо использовать соответствующие рекомендации, которые относили бы их к инциденту ИБ и вносились в отчет по инцидентам ИБ. Примеры рекомендаций приведены в приложении В.

8.5 Реагирование на инциденты

8.5.1 Немедленное реагирование

8.5.1.1 Обзор

В большинстве случаев после подтверждения инцидента член ГРИИБ выполняет действия по немедленному реагированию относительно инцидента ИБ, регистрации подробностей в форме отчета об инциденте ИБ, введению в базу данных событий/инцидентов ИБ и уведомлению сотрудников организации о требуемых действиях на инцидент ИБ. Результатом данных действий может быть принятие аварийных защитных мер (например отключение атакованной информационной системы, сервиса и (или) сети по предварительному соглашению с соответствующим руководством ИТ-подразделения и (или) бизнес-руководством) и (или) определение дополнительных постоянных защитных мер и уведомление сотрудников организации о принятии этих мер. Если аварийные защитные меры не применены, то нужно определить значительность инцидента ИБ по оценочной шкале, принятой в организации, и если инцидент ИБ достаточно «значителен», то об этом необходимо непосредственно уведомить соответствующее вышестоящее руководство. Если очевидна необходимость объявления «кризисной ситуации», руководитель, отвечающий за обеспечение непрерывности бизнеса, должен быть оповещен о возможной активизации плана обеспечения непрерывности бизнеса, причем необходимо проинформировать руководителя ГРИИБ и вышестоящее руководство.

8.5.1.2 Примерные действия по реагированию

Примером действий по немедленному реагированию в случае преднамеренной атаки на информационную систему, сервис и (или) сеть может быть то, что они остаются подключенными к Интернету и другим сетям с целью:

- обеспечения правильного функционирования критически важных бизнес-приложений;
- сбора наиболее полной информации о нарушителе при условии, если он не знает, что находится под наблюдением.

Однако при принятии решения по реагированию нужно учитывать следующие факторы:

- нарушитель может почувствовать, что находится под наблюдением, и предпринять действия, наносящие дальнейший ущерб атакованной системе, сервису и (или) сети и данным;
- нарушитель может разрушить информацию, которая способствует его отслеживанию.

Важно, чтобы при принятии соответствующего решения была техническая возможность быстро и надежно отключить атакованную информационную систему, сервис и (или) сеть. Однако для предотвращения такого отключения не имеющим на это право персоналом необходимо применять соответствующие средства аутентификации.

Предотвращение повторного проявления инцидента обычно является более приоритетной задачей. В некоторых случаях необходимо учитывать то, что нарушитель выявил слабое место, которое должно быть устранено, а выгоды от выявления нарушителя не оправдывают затраченных на это усилий. Это особенно справедливо, если нарушитель на самом деле не является злоумышленником и не нанес большого или вообще не причинил никакого ущерба.

Что касается других инцидентов ИБ, кроме преднамеренной атаки, то их источник должен быть идентифицирован. Может потребоваться отключение информационной системы, сервиса и (или) сети или изоляция соответствующих их частей после получения предварительного согласия соответствующего руководства ИТ и (или) бизнес-руководителя на время внедрения защитных мер. Для этого может

потребоваться больше времени, если уязвимое место для информационной системы, сервиса и (или) для сети окажется существенным или критически важным.

Другим действием по реагированию может быть активизация методов наблюдения [4]. Это действие должно осуществляться на основе процедур, документированных для системы менеджмента инцидентов ИБ.

Информация, которая могла быть повреждена в результате инцидента ИБ, должна быть проверена членом ГРИИБ по резервным записям на предмет изменения, стирания или модификации информации. Может возникнуть необходимость проверки целостности журналов регистрации, поскольку злонамеренный нарушитель может подделать их с целью сокрытия следов проникновения.

8.5.1.3 Обновление информации об инцидентах

Независимо от последующих действий, сотрудник ГРИИБ должен обновить отчет об инциденте ИБ с максимальной детализацией, добавить его в базу данных событий/инцидентов ИБ, оповестив об этом руководителя ГРИИБ и (при необходимости) других лиц. Обновляют следующую информацию:

- о том, что представляет собой инцидент ИБ;
- о том, что явилось причиной, чем или кем он был вызван;
- на что воздействует или мог воздействовать;
- о фактическом или потенциальном воздействии инцидента ИБ на бизнес организации;
- об изменениях в указании на вероятную значительность или незначительность инцидента ИБ (по шкале серьезности, принятой в организации);
- о том, как он обрабатывался до этого времени.

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

ГРИИБ отвечает за обеспечение безопасного хранения информации, относящейся к данному инциденту ИБ, с целью возможного проведения дальнейшей экспертизы и возможного использования судом в качестве доказательства. Например, для инцидента ИБ, ориентированного на ИТ, после первоначального обнаружения инцидента ИБ все непостоянные данные должны быть собраны до отключения пораженной системы ИТ, сервиса и (или) сети до проведения судебного расследования. Предназначенная для сбора информация содержит сведения о любых функционирующих процессах и хранится в памяти, кэше и регистрах. При этом необходимо:

- в зависимости от характера инцидента ИБ провести полное дублирование пораженной системы, сервиса и (или) сети на случай судебного разбирательства или резервное копирование журналов и важных файлов;
- собрать и проанализировать журналы соседних систем, сервисов и (или) сетей, например, маршрутизаторов и межсетевых экранов;
- всю собранную информацию хранить на носителях только для чтения;
- при выполнении дублирования на случай судебного разбирательства обеспечить присутствие не менее двух лиц для утверждения и подтверждения того, что все действия были выполнены согласно действующему нормативному законодательству;
- документировать и хранить вместе с исходными носителями спецификации и описания сервисных команд, которые используются для дублирования на случай судебного разбирательства.

Член ГРИИБ также является ответственным, если это возможно, во время обновления информации об инцидентах ИБ за возвращение в безопасное рабочее состояние пораженных устройств (имеющих или не имеющих отношение к ИТ) в интересах исключения атак на эти устройства.

8.5.1.4 Дополнительные действия

При определении членом ГРИИБ реальности инцидента ИБ его дополнительными действиями должны быть:

- проведение правовой экспертизы;
- информирование лиц, ответственных за передачу информации внутри организации и за ее пределами, о фактах и предложениях по информации, которую надо передать, в какой форме и кому.

После возможно наиболее подробного заполнения отчета об инциденте ИБ отчет вводится в базу данных событий/инцидентов ИБ и передается руководителю ГРИИБ.

Если время расследования превышает время, ранее согласованное внутри организации, то 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;

- что при осуществлении любой деятельности ГРИИБ необходимо следовать документированным процедурам контроля за внесением изменений.

При наличии проблем или если считается, что существуют проблемы в отношении обычных средств связи (например, с электронной почтой), включая случаи, когда система, возможно, подвергается атаке и целесообразно сделать вывод, что инцидент ИБ является значительным и (или) была определена «кризисная ситуация», то следует, в первую очередь, сообщить об инциденте ИБ ответственным лицам лично, по телефону или текстовым сообщением.

При необходимости руководитель ГРИИБ совместно с руководителем обеспечения безопасности ИБ организации и соответствующим руководителем организации (членом совета директоров) правления должны связаться со всеми отделами, которые вовлечены в инцидент ИБ как внутри организации, так и за ее пределами (см. 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. Такие меры предосторожности могут включать в себя назначение резервных консультантов или представителей организации на случай отсутствия кого-либо из ее основных руководителей.

8.5.2 Контролируемость инцидента

После инициирования членом ГРИИБ немедленного реагирования соответствующей правовой экспертизы и действий по передаче информации необходимо срочно убедиться, находится ли инцидент ИБ под контролем. При необходимости член ГРИИБ может проконсультироваться с коллегами, руководителем ГРИИБ и (или) другими сотрудниками организации.

Если подтверждается, что инцидент ИБ находится под контролем, то член ГРИИБ должен перейти к другим дальнейшим необходимым действиям по реагированию, проведению правовой экспертизы и передаче информации (см. 8.5.3, 8.5.5 и 8.5.6) с целью ликвидации инцидента ИБ и восстановления нормальной работы пораженной информационной системы.

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

8.5.3 Последующее реагирование

Определив, что инцидент ИБ находится под контролем и не является объектом «антикризисной ситуации», член ГРИИБ должен определить необходимость и вероятные способы дальнейшего реагирования в отношении данного инцидента. Реагирование может включать в себя восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Затем член ГРИИБ должен занести детали в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а также проинформировать об этом лиц, ответственных за завершение соответствующих действий. Подробности успешного завершения этих действий необходимо внести в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а затем инцидент ИБ должен быть закрыт и соответствующий персонал должен быть проинформирован об этом.

Некоторые реагирования должны быть направлены на предотвращение повторения подобного ему инцидента ИБ. Например, если определено, что причиной инцидента ИБ является отказ аппаратурной части или программного обеспечения ИТ из-за отсутствия вставок в программу («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 защиты ИБ. Необходимо также решить любые проблемы, связанные с конфигурацией ИТ и выявленным инцидентом ИБ. Другими мерами уменьшения возможности повторения или появления такого инцидента ИБ или подобного ему инцидента могут быть изменение системных паролей и отключение неиспользуемых сервисов.

Другая область деятельности по реагированию на инцидент ИБ может включать в себя мониторинг системы, сервиса и (или) сети ИТ. Следом за оценкой инцидента ИБ может оказаться целесообразным ввести дополнительные защитные меры мониторинга для содействия в обнаружении необычных или подозрительных событий, которые могут оказаться признаками инцидентов ИБ. Такой мониторинг

поможет также глубже раскрыть инцидент ИБ и идентифицировать другие системы ИТ, которые подверглись компрометации.

Может возникнуть необходимость в активизации специальных реагирований, документированных в соответствующем плане обеспечения непрерывности бизнес-процесса, которые можно применить к инцидентам ИБ как связанным, так и не связанным с ИТ. Специальные реагирования должны быть предусмотрены для всех аспектов бизнеса, связанных не только непосредственно с ИТ, но также с поддержкой ключевых функций бизнеса и последующего восстановления с помощью речевой сети связи и физических устройств.

Еще одной областью реагирования 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 осуществлено применением «патчей» для известных уязвимостей или отключением скомпрометированных элементов. Если вследствие уничтожения журналов регистрации во время действия инцидента ИБ исчезает весь объем информации об инциденте ИБ, может потребоваться полная перестройка системы, сервиса и (или) сети. Также может потребоваться активизация части соответствующего плана непрерывности бизнеса.

Если инцидент ИБ, не связанный с ИТ, например, спровоцирован пожаром, наводнением или взрывом, то выполняются действия по восстановлению, документированные в соответствующем плане обеспечения непрерывности бизнеса.

8.5.4 «Антикризисные» действия

Может случиться так (см. 8.5.2), что при определении ГРИИБ контролируется ли инцидент ИБ, группа придет к выводу, что инцидент ИБ не находится под контролем и должен обрабатываться в режиме «антикризисных действий». В этом случае используется предварительно разработанный план (планы).

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

- предупреждающие, поддерживающие меры обеспечения непрерывности бизнеса и устойчивости к внешним изменениям;
- организационную структуру и обязанности, связанные с управлением планирования непрерывности бизнеса;
- структуру и основные положения плана (планов) обеспечения непрерывности бизнеса.

План (планы) обеспечения непрерывности бизнеса и защитные меры для поддержки активизации этого (этих) плана (планов), протестированных и признанных удовлетворительными, должны создать основу для ведения наиболее «антикризисных» действий, для которых они предназначены.

Другие типы возможных «антикризисных действий» включают в себя (но не ограничиваются) активизацией:

- средств пожаротушения и процедур эвакуации;
- средств предотвращения наводнения и процедур эвакуации;
- средств предотвращения взрыва бомбы и соответствующих процедур эвакуации;
- работы специалистов по расследованию фактов мошенничества в информационных системах;
- работы специалистов по расследованию технических атак.

8.5.5 Правовая экспертиза

Если в ходе предыдущей оценки была определена необходимость правовой экспертизы в целях доказательства значительного инцидента ИБ, правовую экспертизу проводит ГРИИБ. В целях проведения более подробной экспертизы конкретного инцидента ИБ необходимо применять следственные методы и средства, основанные на ИТ и поддерживаемые документированными процедурами, не используемые ранее в процессе менеджмента инцидентов ИБ. Такую экспертизу проводят структурным методом и определяют, что может использоваться в качестве доказательства при внутренних дисциплинарных разбирательствах или в ходе судебных процессов.

Для проведения правовой экспертизы могут использоваться технические (например средства и методы аудита, средства восстановления свидетельств) и программные средства, защищенные слу-

жебные помещения, а также соответствующий персонал. Каждое действие правовой экспертизы должно быть полностью документировано, включая представление соответствующих фотографий, составление отчетов об анализе результатов аудита, проверку журналов восстановления данных. Квалификация лица или лиц, проводившего(их) правовую экспертизу, должна быть документирована так же, как результаты квалификационного тестирования. Необходимо также документировать любую другую информацию, способную продемонстрировать объективность и логический характер правовой экспертизы. Все записи о самих инцидентах ИБ, деятельности, связанной с правовой экспертизой этих инцидентов, и т. д., а также соответствующие носители информации должны храниться в физически защищенной среде и контролироваться соответствующими процедурами для предотвращения доступа к ним неавторизованных лиц с целью модификации записей. Средства правовой экспертизы, основанные на применении ИТ, должны точно соответствовать правовым нормам с целью исключения возможности оспаривания этого соответствия в судебном порядке и, в то же время, в них должны учитываться все текущие изменения в технологиях. В физической среде ГРИИБ необходимо создавать необходимые условия, гарантирующие неоспоримость обработки свидетельств. В любое время для обеспечения реагирования на инцидент ИБ число персонала должно быть достаточным.

Со временем, несомненно, возникнет необходимость разработки требований к анализу свидетельств в контексте многообразия инцидентов ИБ, включая мошенничество, кражу и акты вандализма. Следовательно, для содействия ГРИИБ потребуется большее число средств, основанных на ИТ, и вспомогательных процедур для раскрытия информации, скрытой в информационной системе, сервисе и(или) сети, включая информацию, которая, на первый взгляд, кажется стертой, зашифрованной или поврежденной. Эти средства должны учитывать все аспекты, связанные с известными типами инцидентов ИБ (разумеется, они должны быть документированы в процедурах ГРИИБ).

В современных условиях в правовую экспертизу часто включают сложные среды с сетевой структурой, в которых расследование распространяется на всю операционную среду, включая множество серверов (файловый сервер, серверы печати, связи, электронной почты и т. д.), а также средства удаленного доступа. Существует много инструментальных средств, включая средства поиска текстов, программное обеспечение формирования изображений и пакеты программ для правовой экспертизы. Главной целью процедур правовой экспертизы является сохранение свидетельств в неприкосновенности, их проверка на предмет противостояния любым оспариваниям в суде и проведение правовой экспертизы на точной копии исходных данных с тем, чтобы избежать сомнений в целостности исходных носителей в ходе аналитической работы.

Общий процесс правовой экспертизы должен охватывать следующие виды деятельности:

- обеспечение защиты целевой системы, сервиса и (или) сети в процессе проведения правовой экспертизы от превращения их в недоступные, изменения или от иной компрометации, включая введение вирусов, и обеспечение защиты от воздействий или минимальных воздействий на их нормальную работу;

- назначение приоритетов сбора доказательств, то есть рассмотрение их от наиболее до наименее изменчивых (что в значительной степени зависит от характера инцидента ИБ);

- идентификация всех необходимых файлов в предметной 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 стертых файлов и других данных;

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

- извлечение содержимого скрытых, временных файлов и файлов подкачки, используемых как программное обеспечение операционной системы, так и как прикладное программное обеспечение;

- доступ к содержимому программного обеспечения защищенных или зашифрованных файлов (если это не запрещено законодательством);

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

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

- 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;

- проведение проверок целостности файлов с целью обнаружения файлов, содержащих «Троянского коня», и файлов, изначально отсутствовавших в системе;

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

- обработка и хранение добытых потенциальных свидетельств так, чтобы избежать их повреждения, приведения в негодность и предотвращения просмотра конфиденциального материала несанкционированными лицами. Следует подчеркнуть, что сбор доказательств всегда должен проводиться в соответствии с правилами судопроизводства или слушания дела, для которых возможно представление данного доказательства;

- получение выводов о причинах инцидента ИБ, необходимых действиях и времени их выполнения с приведением свидетельств, включая список соответствующих файлов, включенных в приложение к главному отчету;

- обеспечение экспертной поддержки для любого дисциплинарного или правового действия (при необходимости).

Метод(ы) выполнения вышеуказанных действий должен(ны) документироваться в работе процедуры ГРИИБ.

ГРИИБ должна обладать разнообразными навыками в обширной области технических знаний (включая знание средств и методов, которые, возможно, будут использоваться нарушителем), опытом проведения анализа/расследования (с учетом защиты используемых свидетельств), знанием правовых и нормативных положений и постоянной осведомленностью о тенденциях, связанных с инцидентами ИБ.

8.5.6 Передача информации

Во многих случаях, когда ГРИИБ подтвердила реальность инцидента ИБ, возникает необходимость информирования конкретных 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: подтверждение реальности инцидента ИБ и его подконтрольности, определение инцидента ИБ как объекта «антикризисной деятельности», закрытие и завершение анализа инцидента ИБ и формирование вывода об инциденте ИБ.

Для оказания содействия такой деятельности целесообразно заранее подготовить конкретную информацию с целью быстрой адаптации ее к обстоятельствам возникновения конкретного инцидента ИБ и предоставления этой информации прессе и (или) другим средствам массовой информации. Если прессе предоставляется неполная информация, относящаяся к инцидентам ИБ, то она должна быть предоставлена в соответствии с политикой распространения информации организации. Информация, подлежащая распространению среди общественности, должна быть проанализирована соответствующими лицами, например высшим руководством, координаторами по связям с общественностью и персоналом ИБ.

8.5.7 Расширение области принятия решений

Могут возникнуть обстоятельства, когда в решение об инциденте ИБ придется вовлекать высшее руководство, другую группу внутри организации или лицо/группу сторонней организации. Речь может идти о принятии решения относительно рекомендуемых действий, относящихся к инциденту ИБ, или дальнейшей оценке с целью определения требуемых действий. Расширение области принятия решений может потребоваться вслед за процессами оценки в соответствии с 8.4 или происходить в ходе процессов оценки, если проблема становится очевидной на ранней стадии ее обнаружения. Для тех, кому когда-либо придется принимать решение о расширении области принятия решений, то есть для группы обеспечения эксплуатации и членов ГРИИБ, необходимо иметь соответствующее описание в документации системы менеджмента инцидентов ИБ.

8.5.8 Регистрация деятельности и контроль за внесением изменений

Следует подчеркнуть, что все, кто причастен к оповещению (информированию) и менеджменту инцидентов ИБ, должны надлежащим образом регистрировать все свои действия на случай их дальнейшего анализа. Информацию об этих действиях вносят в форму отчета об инцидентах ИБ и в базу данных событий/инцидентов ИБ, непрерывно обновляемую в течение всего времени действия инцидента ИБ, от первой формы отчета до завершения анализа инцидента ИБ. Эта информация должна храниться по возможности с применением средств защиты и обеспечением соответствующего режима резервирования. Кроме того, изменения, вносимые в процессе отслеживания инцидента ИБ, обновления форм отчета и баз данных событий/инцидентов ИБ, должны вноситься в соответствии с формально принятой системой контроля за внесением изменений.

9 Этап «Анализ»

9.1 Введение

После принятия решения о закрытии инцидента ИБ необходимо провести дальнейшую правовую экспертизу и анализ с целью определения извлеченных уроков и потенциальных улучшений общей безопасности и системы менеджмента инцидентов ИБ.

9.2 Дальнейшая правовая экспертиза

Иногда после закрытия инцидента ИБ может по-прежнему сохраняться необходимость проведения правовой экспертизы с целью определения свидетельств. Она должна проводиться ГРИИБ с использованием совокупности средств и процедур в соответствии с 8.5.5.

9.3 Извлеченные уроки

После завершения инцидента ИБ важно быстро идентифицировать уроки, извлеченные из его обработки, и предпринять соответствующие действия, которые могут рассматриваться с точки зрения:

- новых или изменившихся требований к мерам защиты ИБ. Это могут быть технические или нетехнические (включая физические) меры защиты. В зависимости от извлеченных уроков требования могут включать в себя необходимость быстрого обновления материалов и проведения инструктажа с целью обеспечения осведомленности в вопросах безопасности (для пользователей, а также для другого персонала) и выпуска руководств и (или) стандартов по безопасности;
- изменений в системе менеджмента инцидентов ИБ и ее процессах, формах отчета и базе данных событий/инцидентов ИБ.

Кроме того при изучении урока по инциденту ИБ необходимо рассматривать полученный опыт не только в рамках отдельного инцидента ИБ, но и проводить проверку наличия тенденций (закономерностей) появления предпосылок к инцидентам ИБ, которые могут быть использованы в интересах определения потребности в защитных мерах или изменениях подходов к устранению инцидента ИБ. Целесообразно также проведение тестирования ИБ, в особенности оценки уязвимостей, после ориентированного на ИТ инцидента ИБ.

Поэтому необходимо регулярно анализировать базы данных событий/инцидентов ИБ для определения:

- тенденций/образцов;
- проблемных областей;
- областей деятельности, где можно предпринять предупредительные меры для снижения вероятности появления инцидентов в будущем.

Существенная информация, получаемая в процессе обработки инцидента ИБ, должна направляться для анализа тенденций (закономерностей), что может в значительной мере способствовать ранней идентификации инцидентов ИБ и обеспечивать предупреждение о том, какие следующие инциденты ИБ могут возникнуть на основе предшествующего опыта и документов.

Необходимо также использовать информацию об инцидентах ИБ и соответствующих им уязвимостях, полученную от государственных и коммерческих КГБР и 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, пораженных этим инцидентом ИБ. Тестирование безопасности и оценку уязвимостей необходимо распространить на любые связанные с ними информационные системы, сервисы и (или) сети. Детальная оценка уязвимостей используется для того, чтобы в ходе инцидента ИБ выявить существование уязвимостей на других информационных системах, сервисах и (или) сетях, и исключить вероятность появления новых уязвимостей.

Важно подчеркнуть, что оценка уязвимостей должна проводиться регулярно и повторная оценка уязвимостей, проводимая после инцидента ИБ, должна быть частью, а не заменой непрерывного процесса оценки.

Необходимо опубликовывать итоговый анализ инцидентов ИБ для обсуждения его на каждом совещании руководства организации по вопросам обеспечения ИБ и (или) на других совещаниях, касающихся вопросов по общей организационной политике ИБ.

9.4 Определение улучшений безопасности

В процессе анализа, проведенного после разрешения инцидента ИБ, новые или измененные защитные меры могут быть определены как необходимые. Рекомендации и соответствующие им требова-

ния к защитным мерам могут оказаться такими, что их немедленное внедрение будет невозможно по финансовым или эксплуатационным причинам; в этом случае они должны быть предусмотрены в более долгосрочных целях организации. Например, по финансовым соображениям невозможно за короткое время осуществить переход к более совершенным межсетевым экранам, тем не менее, решение этого вопроса необходимо внести в долговременные цели ИБ организации (см. 10.3).

9.5 Определение улучшений системы

После разрешения инцидента руководитель ГРИИБ или назначенное вместо него лицо должны проанализировать все произошедшее с целью оценки и определения степени результативности реагирования на инцидент ИБ. Подобный анализ предназначен для выявления успешно задействованных элементов системы менеджмента инцидентов ИБ и определения потребности в любых улучшениях.

Важным аспектом анализа, проводимого после реагирования на инцидент, является возвращение информации и полученных знаний в систему менеджмента инцидентов ИБ. Если инцидент ИБ достаточно серьезен, то вскоре после разрешения инцидента необходимо провести совещание всех заинтересованных сторон, владеющих информацией о нем. На этом совещании должны рассматриваться следующие вопросы:

- 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 по этим результатам осуществлены конкретные согласованные действия (см. 10.4).

10 Этап «Улучшение»

10.1 Введение

Этап «Улучшение» включает в себя внедрение рекомендаций этапа «Анализ», то есть рекомендаций по улучшению результатов менеджмента и анализа рисков ИБ, безопасности и системы менеджмента инцидентов ИБ. Каждая из тем рекомендаций рассматривается ниже.

10.2 Улучшение анализа рисков и менеджмента безопасности

В зависимости от серьезности инцидента ИБ и степени его воздействия при оценке результатов анализа рисков ИБ и менеджмента ИБ, возможно, придется учитывать новые угрозы и уязвимости. В результате завершения обновленного анализа рисков ИБ и анализа менеджмента ИБ может возникнуть необходимость внесения изменений в существующие или применения новых защитных мер.

10.3 Осуществление улучшений безопасности

Следуя рекомендациям, сделанным в процессе этапа «Анализ» (см. 9.4), и анализу нескольких инцидентов, ИБ инициируют процесс внедрения обновленных и (или) новых защитных мер. В соответствии с 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 выпуска рекомендаций и (или) нормативных документов по безопасности. Информационные системы, сервисы и сети организации должны также регулярно подвергаться анализу с целью определения уязвимостей и обеспечения процесса непрерывного повышения надежности систем/сервисов/сетей.

Анализ связанных с безопасностью процедур и документации может проводиться сразу после инцидента, но более вероятно, что это потребуется позднее. После инцидента ИБ необходимо обновить политики и процедуры обеспечения ИБ с учетом собранной информации и любых проблем, выявленных в процессе менеджмента инцидента ИБ. Долговременной целью ГРИИБ вместе с руководителем ИБ организации является распространение в организации этих обновленных вариантов политики и процедур обеспечения ИБ.

10.4 Осуществление улучшений системы

Области системы менеджмента инцидентов ИБ, предназначенные для улучшения (см. 9.5), должны быть проанализированы, а обоснованные изменения внесены в обновленный вариант документации системы. Изменения в процессах, процедурах и формах отчета системы менеджмента инцидентов ИБ должны быть тщательно проверены и протестированы перед применением на практике.

10.5 Другие улучшения

На этапе «Анализ» могли быть установлены другие улучшения, например изменения в политиках, стандартах и процедурах ИБ, а также изменения в конфигурациях аппаратного и программного обеспечения.

Приложение А
(справочное)

Образец формы отчета о событиях и инцидентах информационной безопасности

Отчеты о событиях и инцидентах информационной безопасности

Рекомендации по заполнению

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

Если подозревается, что событие ИБ развивается или уже свершилось, особенно событие, которое может привести к существенным потерям или ущербу собственности или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная информация будет использована для инициирования соответствующего процесса оценки, которая определит, должно ли это событие категорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения или ограничения потерь или ущерба, следует предпринять. Поскольку процесс оценки по своему характеру является краткосрочным, то в данный момент необязательно заполнять все поля формы отчета.

Если сотрудник является членом группы обеспечения эксплуатации, анализирующим полностью/частично заполненные формы отчета, то он должен принять решение, надо ли отнести данное событие к категории инцидента ИБ. При положительном решении сотрудник должен внести в форму отчета об инциденте ИБ как можно больше информации и передать формы отчетов о событии и инциденте ИБ в ГРИИБ. Независимо от того, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена.

Если сотрудник является сотрудником ГРИИБ, анализирующим формы отчетов о событиях и инцидентах ИБ, переданные членом группы обеспечения эксплуатации, то форма отчета об инциденте ИБ должна обновляться по ходу расследования и, соответственно, должна обновляться база данных событий/инцидентов ИБ.

При заполнении форм следует соблюдать следующие рекомендации:

- по возможности формы отчета должны заполняться и передаваться в электронном виде[1)]. В случае, если существуют проблемы или считается, что существуют проблемы с принятыми по умолчанию механизмами электронного оповещения (например электронная почта), включая случаи, когда система может подвергаться атаке и формы отчета могут быть прочитаны несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть телефон или текстовые сообщения, а также использование курьеров;

- следует представить информацию, основанную на фактах, в которой сотрудник уверен, не следует что-либо придумывать для того, чтобы заполнить все формы. Если сотрудник считает уместным включить иную информацию, которую не может подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее недостоверности;

- следует подробно указать, как можно связаться с сотрудником. Немедленно или спустя некоторое время может возникнуть необходимость контакта с ним для получения дальнейшей информации, касающейся Вашего отчета.

Если позднее сотрудник обнаружит, что какая-либо представленная им информация неточна, неполна или ошибочна, то следует внести поправки в отчет и представить его повторно.

[1)] Если возможно, то формы отчетов должны быть, например, на безопасной web-странице с привязкой к электронной базе данных событий инцидентов ИБ. В настоящее время основанная на бумажной технологии система является слишком медленно действующей и далеко не самой эффективной в эксплуатации.

Отчет о событии информационной безопасности

Дата события
Номер события[1]:

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия _____
Организация _____
Телефон _____

Адрес _____
_____
Электронная почта _____

_____

Описание события ИБ

Описание события:

Что произошло

Как произошло

Почему произошло

Пораженные компоненты

Негативное воздействие на бизнес

Любые идентифицированные уязвимости

Подробности о событии ИБ

Дата и время наступления события

Дата и время обнаружения события

Дата и время сообщения о событии

Закончилось ли событие? (отметить в квадрате) Да ☐ Нет ☐

Если «да», то уточнить длительность события в днях/часах/минутах

[1] Номера событий назначаются руководителем ГРИИБ организации.

Отчет об инциденте информационной безопасности

Дата инцидента
Номер инцидента[1]:

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сотруднике группы обеспечения эксплуатации

Фамилия	_____	Адрес	_____
Телефон	_____	Электронная почта	_____

Информация о сотруднике ГРИИБ

Фамилия	_____	Адрес	_____
Телефон	_____	Электронная почта	_____

Описание инцидента ИБ

Дополнительное описание инцидента:

Что произошло

Как произошло

Почему произошло

Пораженные компоненты

Негативное воздействие на бизнес

Любые идентифицированные уязвимости

Подробности об инциденте ИБ

Дата и время возникновения инцидента

Дата и время обнаружения инцидента

Дата и время сообщения об инциденте

Закончился ли инцидент? (отметить в квадрате) Да ☐ Нет ☐

Если «Да», то уточнить длительность инцидента в днях/часах/минутах. Если «Нет», то уточнить, как долго он уже длится

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

Отчет об инциденте информационной безопасности

Тип инцидента ИБ

(Сделать отметку в одном из квадратов, затем заполнить ниже соответствующие поля)	Действительный	☐	Попытка ☐	Предполагаемый	☐

(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 системы связи (CF)	☐		потеря значимых 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 в эксплуатации аппаратных средств (HE)	☐		Ошибка проектирования (DE)	☐
	Ошибка в эксплуатации ПО (SE)	☐		Другие случаи (включая ненамеренные ошибки) (OA)	☐
			Определить:		
	Неизвестно	☐	(Если еще не установлен тип инцидента ИБ (намеренный, случайный, ошибка), то следует сделать отметку в квадрате «неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)		
			Определить:		

Отчет об инциденте информационной безопасности

Пораженные активы

Пораженные активы (при наличии)

(Дать описания активов, пораженных инцидентами ИБ или связанных с ним, включая (где требуются), серийные, лицензионные номера и номера версий)

Информация/данные _____

Аппаратные средства _____

Программное обеспечение _____

Средства связи _____

Документация _____

Негативное воздействие/влияние инцидента на бизнес

Сделать отметку в соответствующих квадратах для указанных ниже нарушений, затем в колонке «значимость» указать степень негативного воздействия на бизнес по шкале 1 ÷ 10, используя следующие сокращения (указатели «категорий»): (FD) — финансовые убытки/разрушение бизнес-операций, (CE) — коммерческие и экономические интересы, (PI) — информация, содержащая персональные данные, (LR) — правовые и нормативные обязательства (это необходимо сравнить с английским оригиналом), (MO) — менеджмент и бизнес-операции, (LG) — потеря престижа (см. примеры в приложении В). Записать кодовые буквы в колонке «указатели», а если известны действительные издержки, — указать их в колонке «стоимость».

		Значимость	Указатели	Издержки
Нарушение конфиденциальности (то есть несанкционированное раскрытие)	☐			
Нарушение целостности (то есть несанкционированная модификация)	☐			
Нарушение доступности (то есть недоступность)	☐			
Нарушение неотказуемости	☐			
Уничтожение	☐			

Общие расходы на восстановление после инцидента ИБ

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

Отчет об инциденте информационной безопасности

Разрешение инцидента

Дата начала расследования инцидента ИБ _____

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

Дата завершения инцидента ИБ _____

Дата окончания воздействия _____

Дата завершения расследования инцидента ИБ _____

Место хранения отчета о расследовании _____

Причастные к инциденту лица/нарушители

(Один из)

Лицо (PE) ☐

Организованная группа (GR) ☐

Легально учрежденная организация/учреждение (OI) ☐

Случайность (AC) ☐

Отсутствие нарушителя (NP)
Например, природные факторы, отказ оборудования, человеческий фактор ☐

Описание нарушителя
Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода(CG) ☐

Политика/терроризм (PT) ☐

Развлечение/хакерство (PH) ☐

Месть (RE) ☐

Другие мотивы (OM)

Определить:

Действия, используемые для разрешения инцидента ИБ

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

Действия, запланированные для разрешения инцидента

(включая возможные приведенные выше действия)

Прочие действия

(например, по-прежнему требуется проведение расследования, но другим персоналом)

Отчет об инциденте ИБ

Заключение

(Сделать отметку в одном из квадратов, является ли инцидент значительным или нет, и приложить краткое изложение обоснования этого заключения)

Значительный ☐ Незначительный ☐

(Указать любые другие заключения) _____

Оповещенные 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 службы ИБ ☐

Руководитель ГРИИБ ☐

Местный руководитель (уточнить, какого подразделения) ☐

Руководитель информационных систем ☐

Автор отчета ☐

Руководитель автора отчета ☐

Полиция ☐

Другие лица ☐

(например, справочная служба, отдел кадров, руководство, служба внутреннего аудита, регулятивный орган, сторонняя КСБР)

Определить:

Привлеченные лица

Инициатор	Аналитик	Аналитик
Подпись _____	Подпись _____	Подпись _____
Фамилия _____	Фамилия _____	Фамилия _____
Должность _____	Должность _____	Должность _____
Дата _____	Дата _____	Дата _____

Аналитик	Аналитик	Аналитик
Подпись _____	Подпись _____	Подпись _____
Фамилия _____	Фамилия _____	Фамилия _____
Должность _____	Должность _____	Должность _____
Дата _____	Дата _____	Дата _____

Приложение В
(справочное)

Примеры общих рекомендаций по оценке инцидентов информационной безопасности

В.1 Введение

В настоящем приложении представлены примерные рекомендации по оценке и категорированию негативных последствий инцидентов ИБ, где каждая рекомендация имеет шкалу от 1 до 10 (1 — низкий, 10 — высокий). (На практике могут использоваться другие шкалы, например, с градацией от 1 до 5. Каждая организация должна использовать шкалу, наиболее подходящую для ее условий).

Перед изучением рекомендаций необходимо ознакомиться со следующими пояснениями:

- в некоторых из рекомендаций, представленных ниже, содержится примечание «Нет записи», для негативных последствий, приведенных для каждой градации инцидента ИБ (от 1 до 10) и идентичных для других шкал (например, с градацией от 1 до 5). Однако на некоторых градациях (по шкале от 1 до 10) для конкретных инцидентов ИБ считается, что из-за отсутствия больших различий в записях о последствиях инцидента ИБ на более низких градациях делать запись нецелесообразно и в этом случае делается примечание «Нет записи». Аналогично вышеизложенному, при более высоких градациях инцидента ИБ считается, что негативные последствия для них не могут быть серьезнее негативных последствий, показанных для самой высокой градации, и, следовательно, для этих градаций действует примечание «Нет записи». (Таким образом, было бы неправильно исключить указания с пометкой «Нет записи» и тем самым градацию шкалы);

- для приведенных рекомендаций, в которых применяются финансовые показатели, приведенные пределы колебаний кажутся несколько необычными. Перед использованием эти рекомендации должны быть дополнены нормированием колебаний курса валюты, наиболее подходящей для организации.

Таким образом, при использовании перечисляемых рекомендаций для расследования негативных последствий инцидента ИБ для бизнеса организации, являющихся следствием несанкционированного раскрытия информации, несанкционированного изменения информации, отказа от использованной информации, недоступности информации и (или) сервиса, уничтожения информации и (или) сервиса, в первую очередь необходимо определить, какая из нижеследующих категорий является соответствующей. Необходимо применять рекомендации по категорированию для определения реального негативного воздействия на бизнес-процессы («значимость») с целью занесения в форму отчета об инциденте ИБ.

В.2 Финансовые убытки/нарушение хода бизнес-операций

Последствия несанкционированного раскрытия, модификации и искажения смысла переданной информации, а также недоступности и уничтожения такой информации могут привести к финансовым убыткам, например, в результате снижения цен на акции, мошенничества или разрыва контракта по причине бездействия или запоздалых действии в отношении этих последствий. Последствиями недоступности или уничтожения любой информации может быть также нарушение бизнес-процесса. На исправление ситуации и (или) восстановление бизнес-процесса после таких инцидентов ИБ потребуются время и усилия. Эти последствия в некоторых случаях могут быть значительными и должны обязательно приниматься во внимание. Для расчетов последствий необходимо, чтобы время восстановления вычислялось в единицах рабочего времени персонала и пересчитывалось в стоимость рабочего времени (финансовые затраты). Эти финансовые затраты должны быть вычислены, исходя из средней стоимости 1 чел.-мес по соответствующей градации/уровню, принятой/принятого внутри организации. Предлагается руководствоваться следующими рекомендациями:

1) результат в финансовых убытках/затратах x_1 или менее;
2) результат в финансовых убытках/затратах между x_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.

В.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. Следует руководствоваться следующими рекомендациями по обеспечению защиты информации, представляющей интерес:

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

2) для конкурента при значении параметра ценности информации, равном y_1 или менее (коммерческий оборот);

3) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_1 + 1$ 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) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_2 + 1$ и y_3 (товарооборот);

5) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_3 + 1$ и y_4 (товарооборот);

6) для конкурента при значении параметра ценности информации более $y_4 + 1$ (оборот);

а также в случаях, когда:

7) нет записи[1)];

8) нет записи;

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

10) нет записи.

В.4 Информация, содержащая персональные данные

В местах хранения и обработки информации, содержащей персональные данные физических лиц, считают моральной и этически корректной, а при некоторых обстоятельствах юридически необходимой защиту этой информации от несанкционированного раскрытия, которое может привести в лучшем случае к созданию дискомфорта у юридического лица, а в худшем — к судебному преследованию лица, раскрывшего информацию, в соответствии с требованием законодательства в части защиты персональных данных. В равной степени необходимо, чтобы информация, содержащая персональные данные, была всегда правильной, поскольку ее несанкционированное изменение, приводящее к появлению некорректных данных, может иметь такое же последствие, что и ее несанкционированное раскрытие. Важно, чтобы информацию, содержащую персональные данные, нельзя было сделать доступной или уничтожить, поскольку это может привести к принятию неправильных решений юридическими лицами или их бездействию во время инцидента ИБ, что может иметь такое же воздействие, что и несанкционированное раскрытие или модификация информации. Следует руководствоваться следующим рекомендациями по градации нанесения ущерба информации, содержащей персональные данные:

1) нанесение (причинение) незначительного ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

2) нанесение (причинение) ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

3) нарушение правовых, нормативных или этических требований, а также опубликование намерения относительно нарушения защиты информации, приводящее к незначительному дискомфорту конкретного лица или группы лиц;

4) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к чувству значительного дискомфорта для конкретного лица или к незначительному дискомфорту — группы лиц;

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

6) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к серьезному дискомфорту для группы лиц;

7) нет записи;

8) нет записи;

9) нет записи;

10) нет записи.

В.5 Правовые и нормативные обязательства

Данные, хранимые и обрабатываемые организацией, могут подчиняться правовым и нормативным обязательствам или храниться и обрабатываться с целью обеспечения соответствия организации данным обязательствам. Несоблюдение таких обязательств, намеренное или ненамеренное, может привести к принятию правовых или административных мер к лицам, работающим в данной организации. Результатом принятия данных мер могут быть штрафы и (или) тюремное заключение. Предлагается руководствоваться следующими рекомендациями:

1) нет записи;

[1)] Термин «Нет записи» означает, что для этой градации последствий инцидента ИБ соответствующая запись отсутствует.

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 10 лет;

7) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу или тюремному заключению сроком более 10 лет;

8) нет записи;

9) нет записи,

10) нет записи.

В.6 Менеджмент и бизнес-операции

Информация может быть такой, что ее компрометация способна нанести ущерб эффективности работы организации. Например, будучи раскрытой, относящаяся к внесению изменений в политике информация может спровоцировать такую общественную реакцию, что реализация данной 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 по обеспечению ИБ может иметь негативные последствия для бизнеса. Предлагается руководствоваться следующими рекомендациями по оценке последствий:

1) неэффективная работа одного подразделения организации;

2) нет записи;

3) нарушение функций (деятельности) по эффективному руководству организацией и ее работы;

4) нет записи;

5) создание препятствий для эффективной разработки или функционирования политик организации;

6) причинение ущерба организации при коммерческих или политических переговорах с другими организациями;

7) создание препятствий для разработки или функционирования главных политик организации, отключение или значительное прерывание важных операций каким-либо другим способом;

8) нет записи;

9) нет записи;

10) нет записи.

В.7 Утрата престижа

Несанкционированное раскрытие информации, отказ от обязательств по обеспечению ИБ или модификация информации, а также недоступность информации могут привести к потере престижа организации с последующим возможным нанесением ущерба ее репутации, к потере доверия и другим негативным последствиям. Предлагается руководствоваться следующими рекомендациями по оценке престижа организации:

1) нет записи,

2) создание атмосферы недовольства внутри организации;

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

4) нет записи;

5) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям национального масштаба;

6) нет записи;

7) значительное негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям;

8) нет записи,

9) нет записи;

10) нет записи.

Приложение С
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица С.1

Обозначение ссылочного международного стандарта	Обозначение и наименование 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 17799:2000	ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью

Библиография

[1] ИСО/МЭК 13335-2:1998 Информационная технология. Методы и средства обеспечения безопасности. Часть 2. Методы менеджмента рисков безопасности информационных и телекоммуникационных технологий

[2] ИСО/МЭК ТО 15947:2002 Информационная технология. Методы и средства обеспечения безопасности. Структура обнаружения вторжения в информационные технологии

[3] ИСО/МЭК ТО 18043:2002 Информационная технология. Методы и средства обеспечения безопасности. Рекомендации по выбору, развертыванию и эксплуатации систем обнаружения вторжения

[4] ИСО 9000 Комплекс стандартов систем менеджмента качества

[5] ИСО 14000 Комплекс стандартов по экологической безопасности

УДК 004.056:006.354 ОКС 01.040.01
35.040 Т00

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

Редактор *В.Н. Копысов*
Технический редактор *Н.С. Гришанова*
Корректор *М.В. Бучная*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 02.12.2008. Подписано в печать 27.01.2009. Формат 60x84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 5,58. Уч.-изд. л. 5,40 Тираж 278 экз. Зак. 27.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер , 4.
www.gostinfo.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6

gost.e-ecolog.ru