МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т E.409

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(05/2004)

СЕРИЯ E: ОБЩАЯ ЭКСПЛУАТАЦИЯ СЕТИ, ТЕЛЕФОННАЯ СЛУЖБА, ФУНКЦИОНИРОВАНИЕ СЛУЖБ И ЧЕЛОВЕЧЕСКИЕ ФАКТОРЫ

Управление сетью – Управление международной сетью

Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи

Рекомендация МСЭ-Т E.409

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ E

ОБЩАЯ ЭКСПЛУАТАЦИЯ СЕТИ, ТЕЛЕФОННАЯ СЛУЖБА, ФУНКЦИОНИРОВАНИЕ СЛУЖБ И ЧЕЛОВЕЧЕСКИЕ ФАКТОРЫ

МЕЖДУНАРОДНАЯ ЭКСПЛУАТАЦИЯ	
Определения	E.100–E.103
Общие положения, касающиеся администраций	E.104–E.119
Общие положения, касающиеся пользователей	E.120–E.139
Эксплуатация международных телефонных служб	E.140–E.159
План нумерации международной телефонной службы	E.160–E.169
Международный план маршрутизации	E.170–E.179
Тональные сигналы в национальных системах сигнализации	E.180–E.189
План нумерации международной телефонной службы	E.190–E.199
Морская подвижная служба и сухопутная подвижная служба общего пользования	E.200–E.229
ЭКСПЛУАТАЦИОННЫЕ ПОЛОЖЕНИЯ, ОТНОСЯЩИЕСЯ К НАЧИСЛЕНИЮ ПЛАТЫ И РАСЧЕТАМ В МЕЖДУНАРОДНОЙ ТЕЛЕФОННОЙ СЛУЖБЕ	
Начисление платы в международной телефонной службе	E.230–E.249
Измерение и регистрация продолжительности разговоров в целях расчетов	E.260–E.269
ИСПОЛЬЗОВАНИЕ МЕЖДУНАРОДНОЙ ТЕЛЕФОННОЙ СЕТИ ДЛЯ НЕТЕЛЕФОННЫХ СЛУЖБ	
Общие положения	E.300–E.319
Фототелеграфия	E.320–E.329
ВОЗМОЖНОСТИ СЕТИ ЦСИС, ОТНОСЯЩИЕСЯ К ПОЛЬЗОВАТЕЛЯМ	E.330–E.349
МЕЖДУНАРОДНЫЙ ПЛАН МАРШРУТИЗАЦИИ	E.350–E.399
УПРАВЛЕНИЕ СЕТЬЮ	
Статистические данные по международным службам	E.400–E.404
Управление международной сетью	**E.405–E.419**
Контроль качества международной телефонной службы	E.420–E.489
ТЕХНИЧЕСКИЕ АСПЕКТЫ ТРАФИКА	
Измерение и регистрация трафика	E.490–E.505
Прогнозирование трафика	E.506–E.509
Определение количества каналов при ручном обслуживании	E.510–E.519
Определение количества каналов при автоматическом и полуавтоматическом обслуживании	E.520–E.539
Категория обслуживания	E.540–E.599
Определения	E.600–E.649
Технические аспекты трафика для сетей с IP	E.650–E.699
Технические аспекты трафика в ЦСИС	E.700–E.749
Технические аспекты трафика в сети подвижной связи	E.750–E.799
КАЧЕСТВО УСЛУГ ЭЛЕКТРОСВЯЗИ: КОНЦЕПЦИИ, МОДЕЛИ, ЦЕЛИ И ПЛАНИРОВАНИЕ НАДЕЖНОСТИ РАБОТЫ	
Термины и определения, связанные с качеством услуг электросвязи	E.800–E.809
Модели для услуг электросвязи	E.810–E.844
Нормы на качество обслуживания и понятия, связанные с услугами электросвязи	E.845–E.859
Использование норм на качество обслуживания для планирования сетей электросвязи	E.860–E.879
Сбор эксплуатационных данных и оценка качества работы оборудования, сетей и служб	E.880–E.899

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т E.409

Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи

Резюме

Целью настоящей Рекомендации являются анализ, структурирование и предложение метода для создания некоторой организации по управлению обработкой инцидентов внутри организации электросвязи, участвующей в обеспечении международной электросвязи, в центре внимания которой находятся течение и структура инцидента. "Течение" и "обработка" будут полезны при определении необходимости классифицировать какое-либо событие как "событие", "инцидент" "инцидент безопасности" или "кризис". Течение охватывает также критические первые решения, которые должны быть приняты.

Компьютерная преступность следует, не отставая, за значительным ростом использования компьютеров в международной электросвязи. За последние годы число компьютерных преступлений резко увеличилось, что подтверждено несколькими международными и национальными обследованиями. В большинстве стран отсутствуют точные цифры относительно числа компьютерных "взломов" или инцидентов безопасности, особенно тех, которые связаны с международной электросвязью.

Большинство организаций или компаний электросвязи не имеют специализированной организации для обработки инцидентов безопасности в инфокоммуникационных сетях (ICN) (хотя они могут иметь общую кризисную группу для обработки кризисов любого типа). Когда возникает инцидент безопасности ICN, он обрабатывается в режиме, применимом к данному случаю, то есть человек, который обнаружил инцидент безопасности ICN, берет на себя ответственность за его обработку наилучшим для него образом. В некоторых организациях имеется тенденция забывать об инцидентах безопасности ICN и скрывать их, поскольку они могут повлиять на производительность, готовность и доходы.

Часто при обнаружении инцидента безопасности ICN, человек, который его обнаружил, не знает, кому сообщить об этом. Это может привести к использованию администратором системы или сети обходного действия или скороспелого решения просто для того, чтобы избавиться от проблемы. Они не имеют делегированных полномочий, времени или опыта для исправления системы таким образом, чтобы инцидент безопасности ICN не повторился. Это – главные доводы в пользу создания обученного подразделения или группы, которые смогут обрабатывать инциденты безопасности быстро и правильно. Кроме того, многие из этих вопросов могут относиться к различным областям, таким как связи со средствами массовой информации, право, обеспечение соблюдения законов, роль на рынке или финансовые вопросы.

Использование разной систематики при сообщении об инциденте или при его обработке ведет к неправильному пониманию. Это, в свою очередь, может привести к тому, что инцидент безопасности ICN не получит ни должного внимания, ни быстрой обработки, которая нужна для остановки, ограничения и предотвращения повторения инцидента. Это может привести к серьезным последствиям для затронутой организации ("жертвы").

Чтобы иметь возможность достичь успеха в обработке инцидента и в сообщении о нем, необходимо понимать, как обнаруживать, обрабатывать и разрешать инциденты. Путем установления общей структуры инцидентов (то есть физических, административных или организационных и логических инцидентов) можно будет получить общую картину структуры и течения какого-либо инцидента. Единообразная терминология является базой для общего понимания слов и терминов.

Источник

Рекомендация МСЭ-Т E.409 утверждена 28 мая 2004 года 2-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) в соответствии с Резолюцией 1 ВАСЭ.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соответствие данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т E.409

Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи

1 Введение

1.1 Область применения

Целью настоящей Рекомендации являются анализ, структурирование и предложение метода для создания некоторой организации по управлению обработкой инцидентов внутри организации электросвязи, участвующей в обеспечении международной электросвязи, в центре внимания которой находятся течение и структура инцидента. "Течение" и "обработка" будут полезны при определении необходимости классифицировать какое-либо событие как "событие", "инцидент", "инцидент безопасности" или "кризис". Течение охватывает также критические первые решения, которые должны быть приняты.

Настоящая Рекомендация содержит обзор и рамочные положения, которые служат руководством для планирования организации по реагированию на инциденты и обработки инцидентов безопасности.

Настоящая Рекомендация носит общий характер, она не определяет требований для конкретных сетей и не ссылается на них.

Настоящая Рекомендация предназначена для содействия международным разработкам в части безопасности сети электросвязи. Таким разработкам было бы оказано содействие, если бы требования данной Рекомендации могли применяться также к национальным инфокоммуникационным сетям (ICN).

Чтобы иметь возможность достичь успеха в обработке инцидента и в сообщении о нем, необходимо понимать, как обнаруживать, обрабатывать и разрешать инциденты. Путем установления общей структуры инцидентов (то есть физических, административных или организационных и логических инцидентов) можно будет получить общую картину структуры и течения какого-либо инцидента. Единообразная терминология является базой для общего понимания слов и терминов.

Использование разной систематики при сообщении об инциденте или при его обработке ведет к неправильному пониманию. Это, в свою очередь, может привести к тому, что инцидент безопасности ICN не получит ни должного внимания, ни быстрой обработки, которая нужна для остановки, ограничения и предотвращения повторения инцидента. Это может привести к серьезным последствиям для затронутой организации ("жертвы").

В настоящей Рекомендации описываются течение и обработка инцидента.

Определение инцидента различно для разных профессий, организаций и лиц.

В соответствии с общим значением этого слова под инцидентом может пониматься какое-либо событие, начиная с ошибочного дублирования, нарушения работы служб, вирусной атаки и заканчивая проникновением в компьютерные системы.

1.2 Определения

В стандарте ISO 17799 упоминаются инцидент, инцидент безопасности и инцидент информационной безопасности.

Определен только термин "инцидент безопасности" как "взлом, угроза, слабое место и неисправность системы безопасности, которые могут повлиять на безопасность организационных ресурсов". Нигде не пояснены термины "инцидент" и "инцидент информационной безопасности". В настоящей Рекомендации предполагается, что инцидент менее серьезен, чем инцидент безопасности, а инцидент информационной безопасности является определенным типом инцидента безопасности.

Рисунок 1/E.409 – Пирамида событий

На рисунке 1 показана пирамида событий. Внизу находится событие, за которым следуют инцидент и инцидент безопасности, а на самом верху расположены кризис и катастрофа. Чем ближе к верху, тем серьезнее событие. Для того чтобы использовать общую и обоснованную терминологию по обработке инцидентов в области ICN, в настоящей Рекомендации определяются следующие термины:

1.2.1 **событие**: Событие – это наблюдаемое явление, которое невозможно предсказать (целиком) или которым невозможно управлять.

1.2.2 **инцидент**: Событие, которое может привести к явлению или эпизоду, не являющемуся серьезным.

1.2.3 **инцидент безопасности**: Инцидент безопасности – это любое неблагоприятное событие, в результате которого некий аспект безопасности может подвергнуться угрозе.

1.2.4 **инцидент безопасности инфокоммуникационных сетей (ICN)**: Любое фактическое или предполагаемое неблагоприятное событие в отношении безопасности ICN. Это охватывает:

- проникновение в компьютерные системы ICN через сеть;
- появление компьютерных вирусов;
- зондирование через сеть уязвимостей ряда компьютерных сетей;
- утечку вызовов учрежденческой АТС;
- любые другие нежелательные события, являющиеся результатом несанкционированных внутренних или внешних действий.

1.2.5 **кризис**: Кризис – это состояние, вызванное некоторым событием, или знание о приближающемся событии, которое может вызвать серьезные негативные последствия. Во время кризиса можно, в лучшем случае, иметь возможность принять меры для предотвращения перехода кризиса в катастрофу. Когда происходит **катастрофа**, обычно имеется План возобновления работы (BCP), а также группа кризисного управления для преодоления этой ситуации.

1.3 Обоснование

Рекомендуется, чтобы организации электросвязи, создающие группы реагирования на инциденты (компьютерной безопасности), в качестве первого шага объявляли используемую ими систематику во избежание ошибочного понимания. Осуществлять сотрудничество значительно легче, когда используется один и тот же "язык".

Рекомендуется, чтобы организации использовали термины "инцидент" и "инцидент безопасности ICN", а также определяли собственные производные термины с учетом серьезности инцидентов. По существу инцидент безопасности ICN является любым нежелательным несанкционированным событием. Это значит, что инцидент безопасности ICN охватывает проникновение в компьютер, атаку "отказ в обслуживании" или вирус в зависимости от мотивировки, опыта и доступных хорошо

осведомленных ресурсов в организации. В организациях, имеющих эффективную группу по борьбе с вирусами, вирусы могут рассматриваться не как инциденты безопасности ICN, а скорее как инциденты.

Примером, или шаблоном, такого образования производных терминов может быть следующее:

–	Инциденты	• Нарушение сетевого этикета Интернет (рассылка спама, вредоносный контент и т. д.) • Нарушение стратегии обеспечения безопасности • Отдельные вирусы
–	Инциденты безопасности ICN	• Сканирование и зондирование • Проникновение в компьютер • Компьютерные диверсия и повреждение (атаки на готовность, такие как "бомбардировка", атаки на DoS) • Злонамеренное программное обеспечение (вирусы, программы "троянский конь", черви и т. д.) • Кража информации и шпионаж • Маскировка под законного пользователя.

Использование одной и той же степени детализации и точности в терминологии дает возможность приобретать опыт по:

– руководящим указаниям о строгости и области применения;

– указанию необходимости быстродействия;

– влиянию возможных контрмер;

– возможным затратам.

2 Описание системы

2.1 Структура и течение

Путем установления общей структуры инцидентов (то есть физических, административных или организационных и логических инцидентов) получают общую картину структуры и течения инцидентов.

2.1.1 Принципы защиты

Механизмы защиты, которые реализует какая-либо организация, должны отражать требования ее стратегии обеспечения безопасности ICN или определенного эквивалента, включая правовые аспекты. Организация по обработке инцидентов и ее задачи должны поддерживать эти требования.

Рисунок 2/E.409 – Принципы защиты

На рисунке 2 показано, что начинать необходимо с "нулевой точки". Чтобы обеспечить согласованную защиту, организация должна реализовать все ступени, связанные с механизмами защиты.

Первыми идут механизмы превентивной защиты. Когда имеются достаточные механизмы превентивной защиты, реализованные с помощью физической или логической защиты, тогда можно определить и запустить механизмы защиты с обнаружением.

Механизмы защиты с обнаружением в простейшей форме могут представлять собой проверку регистрируемых файлов, сигналы о логической или физической аварии, то есть тревожную сигнализацию, пожарную сигнализацию и другие контрольные функции. Одной из форм механизма обнаружения является система обнаружения проникновения (IDS).

После обнаружения инцидента должно выполняться действие. Такое действие обычно охватывает следующие задачи:

- остановить текущий инцидент;
- определить область действия/масштаб инцидента;
- ограничить ущерб;
- принять меры по анализу хода событий;
- предотвратить повторение этого инцидента.

Действия, необходимые для остановки и ограничения инцидента (его удержания), а также для предотвращения его повторного появления, выполняются постоянной организацией, то есть службой помощи или группой поддержки. Если инцидент развивается в кризис, то действия выполняет специально обученная кризисная группа. Что касается изучения и анализа инцидента, рекомендуется, чтобы это делала группа реагирования на инциденты.

Когда имеются и функционируют все три механизма защиты, возникает отпугивающий эффект, то есть преступник знает, что имеются механизмы защиты и что обнаружение инцидента и реагирование на него будут быстрыми. Отпугивающий эффект можно усилить путем реагирования на все инциденты и уведомления правоохранительных органов о любых противозаконных инцидентах.

2.1.2 Структура обработки инцидента

Чтобы понять роль обработки инцидента и организации по реагированию на инциденты внутри определенной организации, рекомендуется использовать структуру обработки инцидента. Эта структура дает обзор течения инцидента, описывая возникновение инцидента, действия/меры с целью ограничения инцидента, восстановление и проверку выполнения.

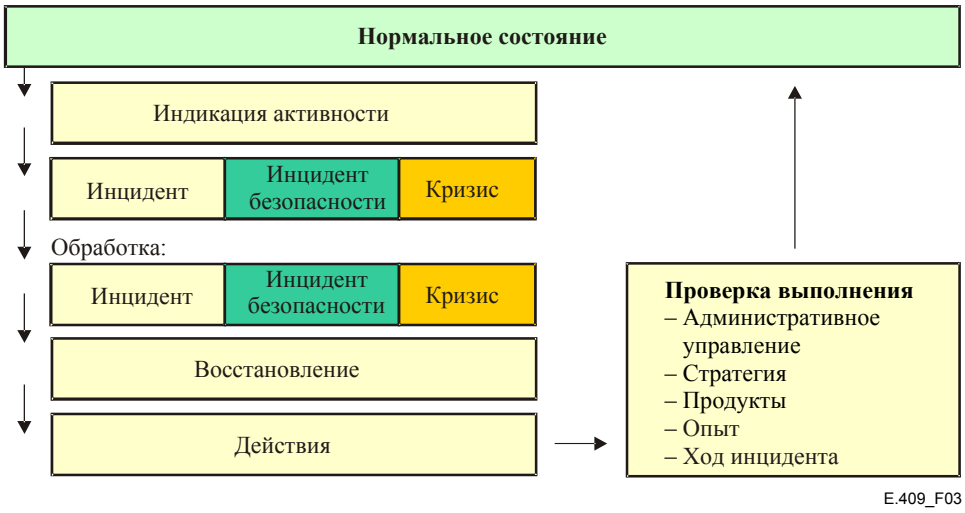

Рисунок 3/E.409 – Структура обработки инцидента

Структура (см. рисунок 3) показывает, что все события, инциденты, инциденты безопасности и кризисы возникают из нормального состояния, то есть из нормально функционирующего дела.

Когда обнаружена индикация активности, которая может привести к инциденту или инциденту безопасности, она обрабатывается постоянной организацией, как описывается ниже. Время между индикацией и появлением инцидента или инцидента безопасности может быть очень коротким. Типом индикации отдельного инцидента может быть вирус на одном рабочем месте, ошибка в сети и т. д. Что касается инцидентов безопасности, их индикаторы можно найти в регистрируемых файлах, фильтрах брандмауэра и т. д. Индикациями могут быть также срабатывающие аварийные сигналы, индикации от камер наблюдения и др.

Когда *происходит инцидент или инцидент безопасности*, он оценивается по его области действия и последствиям. Инцидент может развиться в инцидент безопасности или кризис. Постоянная организация обрабатывает инциденты, а инциденты безопасности обрабатывает специальная группа реагирования на инциденты (CSIRT, Группа реагирования на компьютерные инциденты). Кризисы обрабатывает специально создаваемая группа кризисного управления.

CSIRT может входить в состав группы безопасности в организации электросвязи либо быть полностью отделенной от такой группы безопасности в организации. Как вариант, хотя организация электросвязи может не иметь отдельной CSIRT, эту роль может фактически исполнять неявно группа безопасности данной организации.

Предпринимаемые *действия*/*меры* соответствуют установленной методике или стандартной процедуре. В случае серьезных инцидентов безопасности или кризисов меры будут зависеть от области действия и последствий такого инцидента. Меры осуществляются группой безопасности или группой реагирования на инциденты.

Во время *восстановления* принимаются меры для возвращения к нормальной деятельности. В зависимости от возникшего события это может означать перезапуск компьютерных или сетевых систем, повторную установку программ, восстановление резервных ресурсов. Такие меры могут охватывать установку аварийных сигналов в исходное положение, восстановление поврежденного свойства и т. д.

Во время этой работы также производится оценка того, должно ли это событие иметь правовое последствие. Это может потребовать более тщательного анализа, надежных данных и т. д.

Важна *проверка выполнения* той работы, которая производилась во время обработки инцидента и инцидента безопасности, а также при кризисе. Целью проверки выполнения является улучшение стандартных операций и процедур, чтобы предотвратить повторное появление инцидента и минимизировать любые последствия и затраты.

Отчет о проверке выполнения может привести к изменению процессов обработки инцидента, изменению продуктов и стратегии. Руководителям предоставляются краткие сведения о происшедших инцидентах и инцидентах безопасности, их области действия, последствиях и затратах. Этих сведения должны также включать эффективность работы организации по обработке инцидентов. Следует создать файл извлеченных уроков/опыта, чтобы иметь возможность сравнивать разные инциденты с целью нахождения более эффективных методов и практики обнаружения и обработки инцидентов и инцидентов безопасности.

2.2 Течение инцидента

Ниже описывается течение инцидента или инцидента безопасности. Этот подход основан на опыте и должен быть применим ко всем организациям электросвязи и всем типам инцидентов, так как это течение является простым и общим. Обработку инцидента (течения инцидента) можно сравнить с действиями, которые выполняются при несчастном случае, пожаре и т. д. Начальной точкой, или параметром, является возникновение события, которое имеет последствия для определенной организации.

2.2.1 Фазы обработки при кризисе

При кризисном управлении кризис, как говорят, проходит через три фазы:

- **Предфаза** возникает, когда имеются признаки того, что что-то может пойти неправильно. В этой фазе организация должна находиться в состоянии "предупреждение" и повысить свой уровень готовности.
- **Аварийная фаза** возникает при наступлении кризиса. Аварийное состояние всегда бывает неожиданным и несвоевременным, часто возникает в нерабочие часы или в выходные дни. Так как каждый кризис своеобразен, важно, чтобы обработка выполнялась не по какой-то стандартной методике, которая определяет каждое выполняемое действие применительно к

определенной угрозе. Важно знать, что кризисное управление зависит от осуществления руководства в данной ситуации и что необходимо иметь возможность импровизировать.

- **Постфаза**, или последствия, является решающей фазой, если организация собирается преодолеть кризис и уцелеть. Эта фаза состоит из нескольких других подфаз, таких как психологическая первая помощь, действия по возвращению к нормальной работе, извлеченные уроки и т. д.

2.2.2 Фазы обработки инцидента

Обработка инцидента основана на аварийной фазе кризисного управления. Эта фаза дополняется двумя добавочными фазами – *фазой обработки* и *фазой проверки выполнения* (см. рисунок 4). Они описываются ниже.

Причиной, по которой не используются те же фазы, что и для кризисного управления, является то, что предфаза в кризисном управлении охватывает фазы обработки инцидента в виде единого целого. При нормальных обстоятельствах обработка инцидента не достигает уровня кризисного управления. Если какой-либо инцидент следует перевести на уровень кризисного управления, это означает, что такой инцидент перерос в кризис.

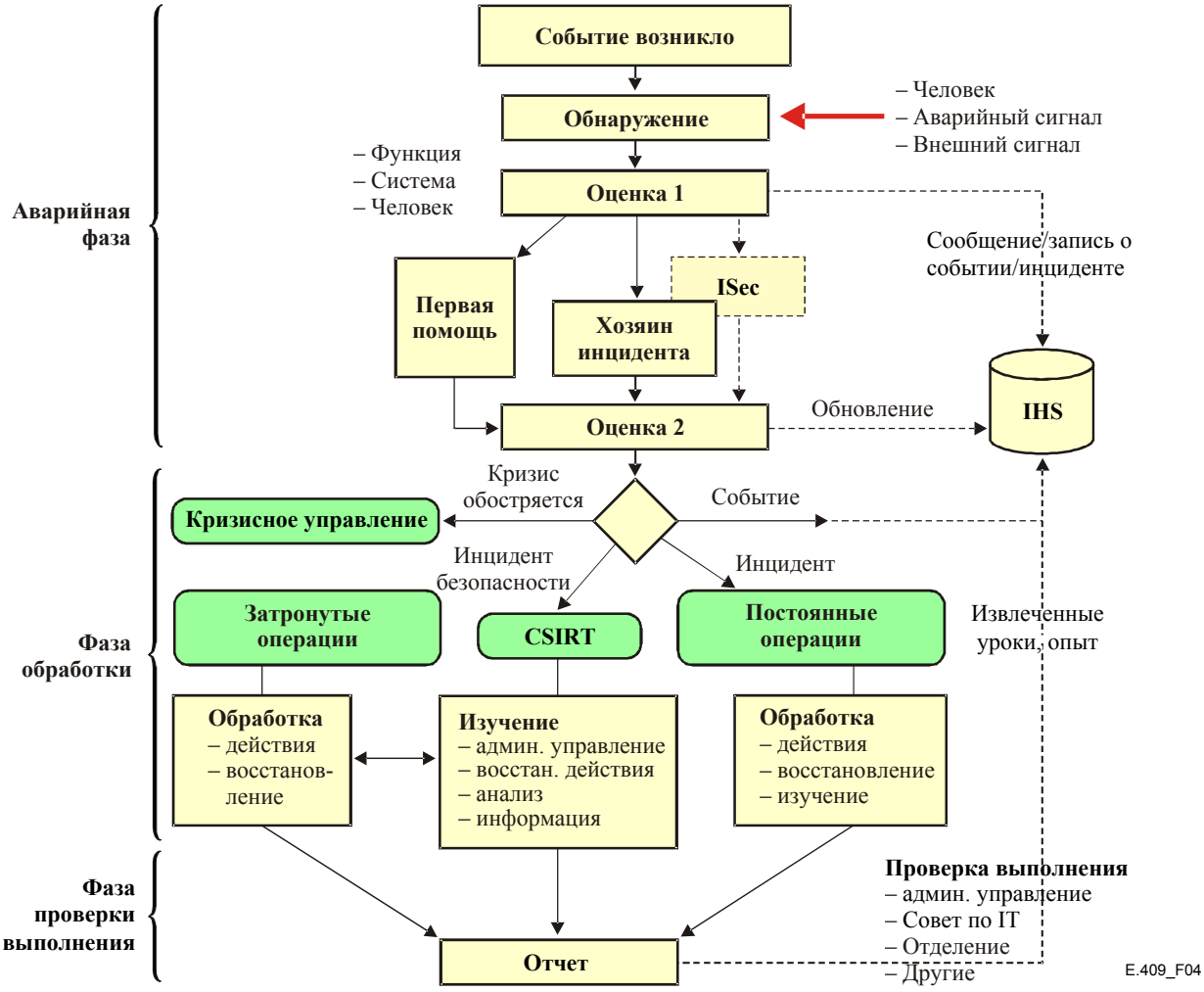

Рисунок 4/E.409 – Течение инцидента

Течение инцидента представлено ниже в разных фазах.

2.2.2.1 Аварийная фаза

Как показано на рисунке 4, аварийная фаза является первой фазой. Эту фазу можно сравнивать с ситуацией при несчастном случае, то есть во время дорожно-транспортного происшествия первые предпринимаемые действия часто являются определяющими для конечного результата. Эти действия имеют наиболее важные последствия для результата. Стадии в аварийной фазе описываются по порядку (см. рисунок 5).

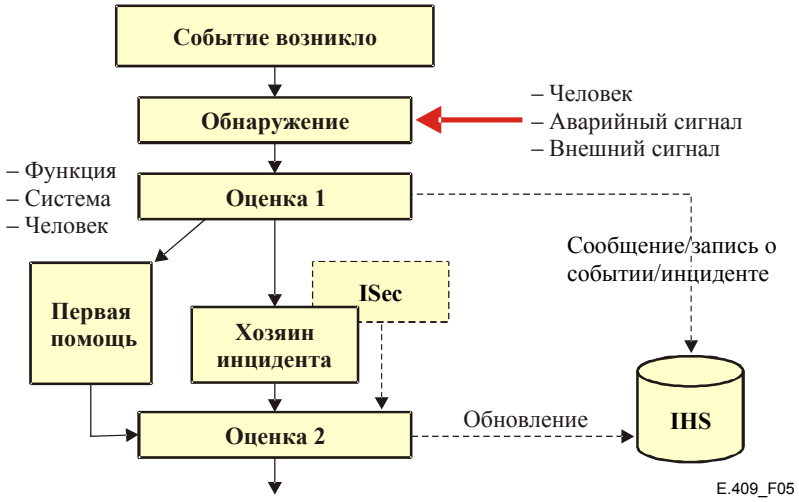

Рисунок 5/E.409 – Аварийная фаза

2.2.2.2 Обнаружение

Событие может быть обнаружено человеком визуально, то есть путем отслеживания сообщения об ошибке, чтения результирующего файла или аудиторского контроля. Визуальное обнаружение может иметь место в случае, когда оператор видит, что некто совершает проникновение, либо когда кто-то обнаруживает пожар. Событие может также обнаруживаться человеком, который почувствовал неправильность и необычность происходящего.

Логическими авариями являются ситуации, которые требуют внимания конечного пользователя, эксплуатационного персонала, функций безопасности и т. д. Логической аварией может быть аварийный сигнал, запускаемый антивирусной программой, аудиторской подсистемой, брандмауэром или системой обнаружения проникновения. Событие может также запустить физические аварийные сигналы, такие как пожарная сигнализация, охранная сигнализация и т. д.

Внешнее обнаружение происходит в случае, когда кто-то, не работающий в организации, обнаруживает событие. Это может быть, в худшем случае, объявлено в новостях либо репортером, который изучает источники или обратился в организацию, чтобы получить комментарии о событии, которое организация еще не обнаружила. Это также могут быть правоохранительные органы, которые уведомляют отделение безопасности во время расследования преступления, либо добропорядочный гражданин, обнаруживший нежелательные характеристики на Web-сайте этой организации электросвязи.

Когда событие обнаружено, должна производиться начальная оценка ситуации для подтверждения категории и серьезности. Это делается путем категоризации событий по типам, то есть является ли оно инцидентом, инцидентом безопасности, кризисом или просто событием. После этого должны быть рассмотрены область действия и последствия. Ниже дается простая классификация, применимая только к инцидентам безопасности ICN, для определения серьезности инцидента или инцидента безопасности.

Эта оценка может производиться человеком, который обнаружил событие и который мог бы также предпочесть уведомить об обнаруженном событии некоторую функцию, то есть службу помощи, группу поддержки или Отделение информационной безопасности. Когда о событии уведомлена какая-либо функция, она становится ответственной за этой событие. Функции, которые могут получать уведомления об обнаружении, называются также точкой контакта (POC); они ответственны за обработку ситуации. Аварийный сигнал обычно автоматически передается к ответственному лицу, функции или системе. Все уведомления о событиях должны регистрироваться в системе обработки инцидентов (IHS).

Точка контакта (POC) – это подразделение или человек, которому сообщается о событии. Иногда это – подразделение или функция, такие как служба помощи, отдел управления производством, Отделение безопасности или информационной безопасности (ISec). О событии не может уведомляться CSIRT, так как она является виртуальной группой, которая формируется во время инцидента безопасности. Об инциденте безопасности можно уведомить Отделение информационной безопасности (ISec), которое несет ответственность за CSIRT или какую-либо другую POC, в которой будет выполняться правильная оценка и инициироваться контакт с ответственными подразделениями.

• Класс 4	Очень серьезно	Инцидент безопасности, который имеет значительные последствия для организации, например скоординированные атаки, проникновение в компьютер, кража уязвимой и конфиденциальной информации и т. д. Инцидент безопасности, который подпадает под этот класс, требует значительных контрмер и приводит к значительному ущербу.
• Класс 3	Серьезно	Инцидент безопасности, который имеет последствия для организации, например компьютерная диверсия, компьютерное мошенничество, взлом целостности, злоупотребление корпоративной или пользовательской информацией или раскрытие информации.
• Класс 2	Менее серьезно	Инцидент безопасности, такой как попытки проникновения, неправильное использование компьютерных ресурсов и т. д. Инцидент безопасности, который подпадает под этот класс, имеет меньшие последствия, требует незначительных контрмер и приводит к небольшому ущербу.
• Класс 1	Без последствий	Инцидент, который обрабатывается постоянной организацией, но может перерасти в инцидент безопасности, например просмотр, одиночные вирусы, события неправильного использования, атаки, обнаруженные почтовыми системами, и т. д. Этот класс обычно охватывает инциденты, которые влияют на нормальное производство. Инцидент безопасности, который подпадает под этот класс, требует незначительных контрмер или не требует их вообще, приводит к небольшому ущербу или не приводит к ущербу.

Обычно о событии сообщается в службу помощи, особенно в случаях, когда событие обнаружил конечный пользователь. Конечные пользователи, как правило, сообщают о всех событиях и ошибках в службу помощи. В других случаях событие может обнаружить системный администратор или оператор. События могут также обнаруживать эксплуатационные управляющие центры электросвязи, отдел системной безопасности и физическая охрана, так как они получают аварийные сигналы от логических или физических датчиков либо от внешних источников.

Все функции и подразделения, которые могут получать аварийные сигналы или индикации о событии, должны быть снабжены инструкциями о порядке действий. Это должно быть сделано во избежание игнорирования или неправильной обработки событий и аварийных сигналов.

2.2.2.2.1 Оценка 1

Эта оценка выполняется человеком или функцией (POC), или системой (IDS). В большинстве случаев она выполняется человеком, получившим аварийный сигнал или другую информацию о событии.

Событие должно быть определено по принадлежности к одной из пяти разных категорий:

- кризис;
- инцидент безопасности;
- инцидент;
- событие;
- ложный аварийный сигнал.

Если какое-либо событие не может быть отнесено к одной из категорий, указанных выше, то оно должно классифицироваться как инцидент и обрабатываться постоянной организацией, то есть службой помощи и группой поддержки. Некоторые события не требуют действий, так как они рассматриваются как "ошибки пользователя" или ошибочные интерпретации.

Кроме того, событие должно также оцениваться по влиянию, которое оно оказывает на организацию или дело. Этот "уровень серьезности" оценивается по следующим четырем уровням:

- очень серьезные последствия для организации электросвязи;
- серьезные последствия для организации электросвязи;
- некоторые последствия для организации электросвязи;
- без последствий для организации электросвязи.

Эти оценки следует зарегистрировать в системе обработки инцидентов (IHS).

В случае инцидентов, инцидентов безопасности и кризисов должна немедленно оказываться первая помощь. Она охватывает начальное уведомление об ущербе, оценку последствий и оценку наличия каких-либо быстрых решений, которые можно применить для ограничения ущерба. Эта оценка часто выполняется человеком или функцией, которые получили аварийный сигнал или извещение о событии.

При инцидентах человек или POC информирует затронутые отделения и начинает принимать меры. С учетом области действия и последствий это может также означать, что немедленно привлекаются эксперты. Если действует компьютерный вирус, который распространился только в одном отделении, то он обрабатывается функцией обеспечения с помощью стандартных операций.

В то же время о событии *информируется* служба помощи: какое событие произошло, какие приняты меры и когда компьютерная и сетевая системы вернутся к норме. Это делается для информирования персонала службы помощи, так как именно они будут получать запросы от конечных пользователей, затронутых инцидентом. Они смогут сообщать конечным пользователям, что помощь оказывается. Другая, еще более важная, причина состоит в том, что если кто-то еще сообщит о том же или похожем инциденте, то служба помощи будет знать, кого информировать о новом случае.

Однако если появился компьютерный вирус и распространился на несколько отделений, то следует предпринять скоординированные усилия, чтобы эффективно ограничить ущерб и устранить вирус.

Все *внешние запросы* должны направляться в Отделение информационной безопасности.

Перед принятием решения о следующих шагах или действиях необходимо передать информацию об инциденте хозяину инцидента или в Отделение информационной безопасности (ISec). Хозяин инцидента – это лицо, которое ответственно за затронутое отделение, либо владелец затронутой системы. Хозяин инцидента является лицом, которое должно взять на себя ответственность за потери и затраты.

Если затронуты несколько отделений, то хозяином инцидента является отделение с наибольшими потерями или затратами. Если инцидент влияет на инфраструктуру организации электросвязи, то ответственным будет соответствующее отделение. Если хозяин инцидента не может быть определен, то хозяином инцидента считается Отделение информационной безопасности (ISec).

Хозяин инцидента имеет полномочия для обработки этого инцидента и несет за него ответственность.

2.2.2.2.2 Оценка 2

Эта оценка выполняется хозяином инцидента или Отделением информационной безопасности (ISec). Отделение информационной безопасности и CSIRT владеют экспертными знаниями в вопросах безопасности и безопасности ICN. К ним можно обращаться за консультацией для оценки области действия и последствий.

Эта оценка заключается в проверке предыдущей оценки, касающейся классификации инцидента (то есть является ли это событием, инцидентом, инцидентом безопасности или кризисом). Хозяин инцидента решает, правильно ли оценен инцидент или необходимо сделать поправки. Он также принимает решения о дальнейшей его обработке. В их число входит решение о том, кто будет

обрабатывать и изучать инцидент – группа кризисного управления, CSIRT или постоянная организация.

Хозяин инцидента принимает решение об информировании группы поддержки и службы помощи. В некоторых случаях будет лучше отсрочить это решение до появления руководителя по инциденту или группы реагирования на инцидент.

В случаях наличия каких-либо сомнений относительно того, может ли инцидент быть обработан внутри постоянной организации, следует обратиться к лицу для контактов по CSIRT. В случае инцидента безопасности контакт с CSIRT обязателен. Если целесообразно, можно связаться с Отделением информационной безопасности. За время этой работы будет выяснена область действия инцидента безопасности и проведена совместная оценка необходимости вызова группы кризисного управления.

Запись о фактическом инциденте, зарегистрированная в системе обработки инцидентов (IHS), обновляется. События, по которым не выполнялись действия, также регистрируются. Необходимость регистрации всех событий объясняется тем, что некоторое отдельное событие или несколько событий могут быть связаны с другими событиями, инцидентами или инцидентами безопасности, хотя эта связь не очевидна в тот момент времени. Если инцидент безопасности возник, то связь между этими событиями и инцидентом безопасности может стать ясной.

После этой фазы инцидент безопасности переходит в фазу обработки.

2.2.2.2.3 Фаза обработки

Во время фазы обработки производится фактическая обработка события. Этим событием может быть инцидент, инцидент безопасности или кризис. При переходе в эту фазу событие приобретает "официальный" статус и должно быть обработано, как описывается ниже.

Во время **кризиса** или **обострения** вводится кризисное управление, которое принимает на себя обработку согласно установленным методикам. Меры, которые принимаются, также соответствуют установленным кризисным методикам и ведут к формированию группы кризисного управления. Кризисное управление и обработка кризиса не входят в предмет рассмотрения настоящей Рекомендации.

Инцидент обрабатывается постоянной организацией электросвязи, то есть группой управления производством, группой поддержки, службой безопасности и наблюдения и т. д. Инцидент может заключаться в ошибках и нарушениях производства, наличии посетителей, действующих бесконтрольно, и т. д. Постоянная организация обрабатывает инциденты путем:

- принятия мер для противодействия причине и следствиям инцидента и для предотвращения его повторения;
- восстановления с целью возобновления деятельности;
- изучения причин возникновения инцидента и его последствий и документирования выполненных действий.

Предлагается, чтобы производственные инциденты обрабатывались подразделением поддержки производства и организацией, созданной для таких событий.

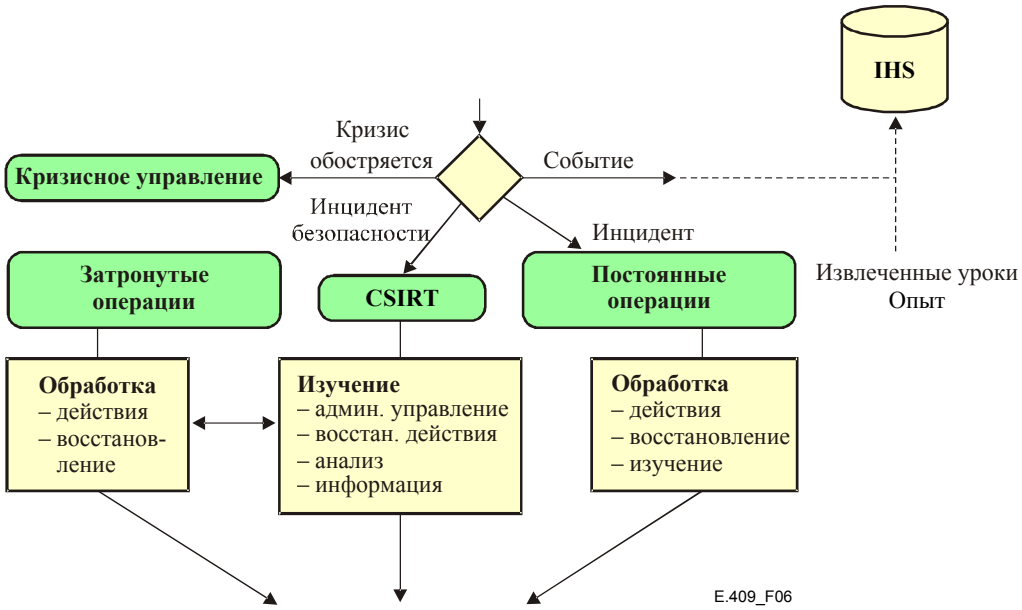

Рисунок 6/E.409 – Фаза обработки

Когда **инцидент безопасности** входит в фазу обработки, обработка выполняется согласно установленным методикам.

Хозяин инцидента в консультации с Отделением информационной безопасности (ISec) инициирует и создает виртуальную и временную группу реагирования на инцидент (CSIRT). Выбирается также руководитель по инциденту. Это может быть любое лицо из затронутых подразделений поддержки, группы наблюдения или Отделения информационной безопасности (ISec). Группа реагирования на инцидент (CSIRT) формируется с учетом соответствующих лиц и их умений и навыков.

CSIRT изучает инцидент безопасности, что означает:

- административное управление работой по изучению и ее выполнение;
- принятие мер для остановки и ограничения последствий инцидента безопасности (его локализации). Это делается совместно с затронутым отделением. Обычно CSIRT действует как подразделение поддержки;
- восстановление с целью возврата к работе предприятия электросвязи. Это делается совместно с затронутыми отделениями. Обычно CSIRT является подразделением поддержки;
- анализ обстоятельств и причин инцидента, его последствий и документации о выполненных действиях и затратах;
- информацию для участвующих сторон, то есть для Отделения информационной безопасности, службы помощи, группы поддержки и т. д.

Эти процедуры могут быть еще более детализированы по сравнению с приведенными здесь процедурами, которые могут использоваться в качестве руководящих указаний.

Методика состоит из пяти разных шагов:

1) определение типа инцидента, области его действия и последствий;

2) локализация, то есть остановка явления и ограничение последствий инцидента безопасности;

3) ликвидация причины и предотвращение повторения;

4) восстановление нормальной работы;

5) проверка выполнения.

Когда CSIRT сформирована, "определение" является стандартной процедурой при инструктаже членов CSIRT. Они также информируются об инциденте безопасности, фактическом состоянии, принятых мерах, мерах предосторожности и т. д.

2.2.2.2.4 Фаза проверки выполнения

В фазе проверки выполнения кризис, инцидент безопасности или инцидент уже разрешен, а его последствия минимизированы. Осталось оценить событие и его обработку, направить отчет руководству, в Отделение информационной безопасности, отделение управления производством и т. д.

Отчет о проверке выполнения должен описывать обнаружение инцидента, время запаздывания между обнаружением и реакцией/действием, принятые меры, их эффективность и результаты. Отчет должен также показать изъяны, обнаруженные в исходной среде (ICN), недостатки в обработке и процедурах. Все это следует зарегистрировать в файле извлеченных уроков или опыта работы, который может использоваться во избежание повторения тех же ошибок. Следует оценить как прямые, так и косвенные затраты.

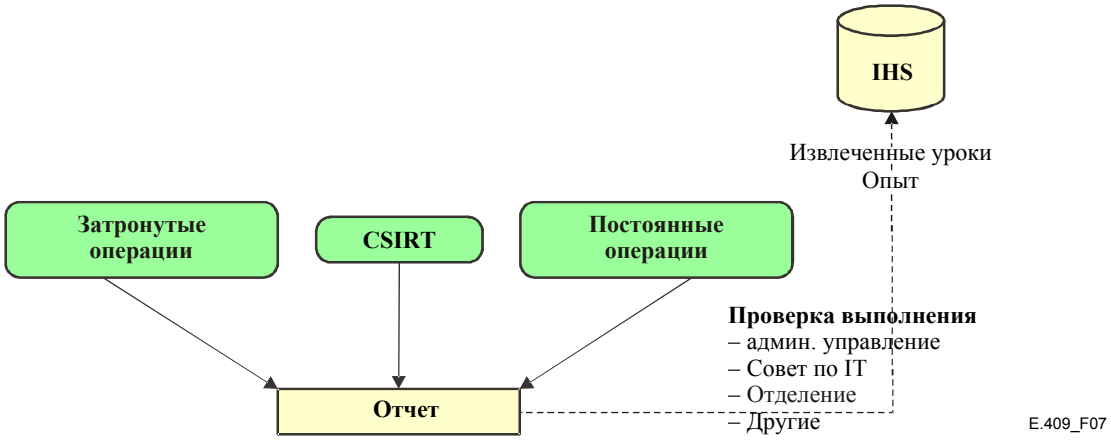

Рисунок 7/E.409 – Фаза учета

Во время этой фазы в HIS осуществляется завершение записи о фактическом инциденте. Должен быть сформирован файл извлеченных уроков/опыта работы с целью обзора и повторного обращения к опыту, приобретенному во время аварийной фазы, фазы обработки и фазы проверки выполнения.

3 Система обработки инцидентов

Весьма важным является реализация системы обработки инцидентов, которая отслеживает каждое обнаруженное событие, о котором было сообщено, инцидент, инцидент безопасности и кризис. Путем анализа этих файлов можно изучить, какие типы событий чаще встречаются, по каким причинам они возникают, как они обнаруживаются, их область действия, последствия и затраты. Важным аспектом является регистрация событий, которые не являются инцидентами, инцидентами безопасности или кризисами. Хотя такие события могут не представлять угрозы, когда они рассматриваются в виде изолированных событий, вместе они могут дать информацию о том, как возникают инциденты. Такие события могут показывать сходство с инцидентами безопасности, направленными против организации. Незначительные события, если их рассматривать индивидуально, могут выглядеть как неправильный запрос в сети, но если рассматривать их в целом, то они могут показать частое сканирование сети организации электросвязи, в частности компьютерной сети и систем.

БИБЛИОГРАФИЯ

- Excerpts from Master's Thesis in Incident Organization and Security Incident Handling, Jimmy Arvidsson, FIINA, 2001.
- CERT/CC (URL: http://www.cert.org) 2000-09-26.
- Federal Incident Response Capability (URL: http://www.fedcirc.llnl.gov) 2000-05-20.
- Internet Security Glossary; R. Shirey, GTE/BBN Technologies, May 2000.
- Informationssäkerhetshandbok, del 5 – Katastrofskydd för IT-verksamhet, v.2, Jan-Olof Andersson, JOA InfoSäk, 1999.
- Handbook for Computer Security Incident Response Teams (CSIRTs); Moira J. West-Brown, Dan Stikvoort, Klaus-Peter Kossakowski; Carnegie Mellons, Software Engineering Institute, 1998.
- Computer Security Incident Handling – Step by step, SANS Institute, NSWC, 1998.
- Intrusion Detection, Edward Amoroso, Intrusion.Net Books, 1998.
- Best Current Practice; Expectations for Computer Security Incident Response; N. Brownlee, The University of Auckland, E. Guttman, Sun Microsystems, June 1998.
- Computer Security Incident Handling Procedure, NSWC Dahlgren, October 1996.
- Computer Crime: A Crimefighter's Handbook, David Icove, Karl Seger and William –VonStorch, O'Reilly & Associates, 1995.
- An Analysis of Security Incidents On The Internet, 1989-1995, John Howard, CERT/CC (URL: http://www.cert.org/research/JHThesis/Start.html) 2000-05-20.
- Establishing a Computer Security Incident Response Capability (CSIRC), NIST, November 1991.
- "The Oxford Reference Dictionary"; Oxford University Press, 1986.
- A Common Language for Computer Security Incidents; John D. Howard and Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667].
- Intrusion Detection – Network Security Beyond The Firewall, Terry Escamilla.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	**Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы**
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола (IP) и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2005 г.