А.В. Царегородцев, М.М. Тараскин, Е.А. Дербин

ОДИН ИЗ ПОДХОДОВ К ФОРМАЛИЗАЦИИ ОПИСАНИЯ УГРОЗ, УЯЗВИМОСТЕЙ И РИСКОВ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Аннотация: *Рассматривается один из подходов к оценке угроз, уязвимостей и рисков при защите информации в организациях, позволяющий полностью проанализировать и документально оформить требования, связанные с обеспечением безопасности информации в организации. Использование такого подхода даст возможность избежать расходов на избыточные меры безопасности, возникающие при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, а также обеспечить проведение работ в сжатые сроки. Предложены практические рекомендации по выбору мер противодействия и оценки эффективности контрмер, позволяющие сравнивать их различные варианты.*

Ключевые слова: *информация, безопасность, организация, риск, угроза, уязвимость, модель, методика, идентификация*

Введение

Ни одна сфера жизни цивилизованного государства в настоящее время не может эффективно функционировать без развитой информационной инфраструктуры. Безопасность информации выдвигается на первый план и становится элементом национальной безопасности. Защита информации, несомненно, должна рассматриваться как одна из приоритетных государственных задач.

Оценка состояния информационной безопасности и определение ключевых проблем в этой области должны базироваться на анализе источников угроз. При этом необходимо понимать, что эти угрозы в настоящее время носят не умозрительный характер, а каждой из них соответствуют целенаправленные действия конкретных носителей враждебных намерений (начиная с иностранных разведывательных служб и кончая криминальными группировками). В результате этих действий может быть нанесен серьезный ущерб жизненно важным интересам Российской Федерации в политической, экономической, оборонной и других сферах деятельности государства либо причинен существенный социально-экономический ущерб обществу в целом, различным организациям и отдельным гражданам [1].

Достижение требуемого уровня информационной безопасности в организации должно, прежде всего, базироваться на исследовании источников угроз информации, уязвимостей в ее защите, и, проистекающих из их соотношений, рисков. Для решения этих задач предлагается один из подходов к описания угроз, уязвимостей и рисков системы защиты информации, формализованный в виде соответствующей методики.

1. Основные этапы методики формализованного описания угроз, уязвимостей и рисков

Для определения источников угроз информации и уязвимостей на *первом этапе* следует сформулировать цели защиты информации в организации.

Необходимо попытаться – при помощи руководства и работников организации – понять, что же на самом деле нужно защищать и от кого. С этого момента начинается специфическая работа

на стыке информационных технологий и основной деятельностью организации, которая состоит в определении таких мероприятий и (если возможно) целевого состояния обеспечения безопасности информации, которое будет сформулировано одновременно и в терминах основной деятельности, и в терминах безопасности информации. Исследование рисков – это и есть инструмент, с помощью которого можно определить цели защиты информации, оценить основные критичные факторы, негативно влияющие на ключевые аспекты основной деятельности организации, и выработать эффективные решения для их контроля или минимизации.

На *втором этапе* осуществляется идентификация и оценка информационных активов организации.

Цель обеспечения безопасности информации состоит в сохранении ее конфиденциальности, целостности и доступности. Вопрос только в том, какую именно информацию необходимо охранять и какие усилия прилагать для обеспечения ее сохранности. С точки зрения исследования рисков безопасности информации к основным активам относятся непосредственно информация, инфраструктура, персонал, имидж и репутация компании. Без инвентаризации активов на уровне основной деятельности организации невозможно ответить на вопрос, что именно нужно защищать. Очень важно понять, какая информация обрабатывается в организации, где и как выполняется ее обработка.

В условиях крупной современной организации количество информационных активов может быть очень велико. Если деятельность организации автоматизирована при помощи тех или иных сервисных приложений, то можно говорить, что практически любому материальному объекту, использующемуся в этой деятельности, соответствует какой-либо информационный объект. Поэтому первоочередной задачей исследования рисков становится определение наиболее значимых активов.

Решить эту задачу невозможно без привлечения менеджеров основного направления деятельности организации, как среднего, так и высшего звена. Оптимальна ситуация, когда высший менеджмент организации лично задает наиболее критичные направления деятельности, для которых крайне важно обеспечить безопасность информации. При этом дальнейший анализ целесообразно проводить именно по обозначенным высшим менеджментом направлениям основной деятельности организации. Полученная информация обрабатывается, агрегируется и передается высшему менеджменту для комплексной оценки ситуации.

Идентифицировать и локализовать информацию можно на основании описания основной деятельности организации, в рамках которой информация рассматривается как один из типов ресурсов. Задача несколько упрощается, если в организации принят подход регламентации основной деятельности организации. Формализованные описания процессов основной деятельности организации обычно служат стартовой точкой для инвентаризации активов. После того как активы идентифицированы, необходимо определить их ценность.

Работа по определению ценности информационных активов в разрезе всей организации одновременно наиболее значима и сложна. Именно оценка информационных активов позволяет начальнику отдела информационной безопасности выбирать основные направления деятельности по обеспечению безопасности информации.

Ценность актива выражается величиной потерь, которые понесет организация в случае нарушения безопасности актива. Определение ценности достаточно сложный процесс. Но экономическая эффективность процесса обеспечения безопасности информации во многом зависит именно от осознания того, что нужно защищать и какие усилия для этого потребуются, так как в большинстве случаев объем прилагаемых усилий прямо пропорционален объему затрачиваемых финансовых средств и операционных расходов. Управление рисками позволяет ответить на вопрос, где можно рисковать, а где нельзя. В данном случае термин «рисковать» означает, что в определенной области можно не прилагать значительных усилий для защиты информационных активов и при этом в случае нарушения безопасности организация не понесет значимых потерь. Здесь можно провести аналогию с классами защиты автоматизированных систем: чем значительнее риски, тем более жесткими должны быть требования к защите.

Чтобы определить последствия нарушения безопасности, нужно либо иметь сведения о

зафиксированных инцидентах аналогичного характера, либо провести сценарный анализ (моделирование). В рамках сценарного анализа изучаются причинно-следственные связи между событиями нарушения безопасности активов и последствиями этих событий для основной деятельности организации. Последствия сценариев должны оцениваться несколькими экспертами. Критерии и шкалы определения ценности индивидуальны для каждой организации. По результатам сценарного анализа можно получить информацию о ценности активов.

Если активы идентифицированы и определена их ценность, можно говорить о том, что цели обеспечения безопасности информации частично установлены: определены объекты защиты и значимость поддержания их в состоянии информационной безопасности для организации.

На *третьем этапе* исследуются источники проблем для обеспечения безопасности информации в организации.

После определения целей обеспечения безопасности информации следует проанализировать проблемы, которые мешают приблизиться к требуемому целевому состоянию. На этом этапе исследование рисков переходит на уровень информационной инфраструктуры и традиционных понятий информационной безопасности – нарушителей, угроз и уязвимостей.

Модель нарушителя

Для оценки рисков недостаточно ввести стандартную модель нарушителя, разделяющую всех нарушителей по типу доступа к активу и знаниям о структуре активов. Такое разделение помогает определить, какие угрозы могут быть направлены на актив, но не дает ответа на вопрос, могут ли эти угрозы быть в принципе реализованы.

В процессе анализа рисков необходимо оценить мотивированность нарушителей при реализации угроз. При этом под нарушителем подразумевается не абстрактный внешний хакер или инсайдер, а сторона, заинтересованная в получении выгоды путем нарушения безопасности актива.

Первоначальную информацию о модели нарушителя целесообразно получить у высшего менеджмента, представляющего себе положение организации на рынке, имеющего сведения о конкурентах и о том, каких методов воздействия можно от них ожидать. Сведения, необходимые для разработки модели нарушителя, можно получить и из специализированных исследований по нарушениям в области компьютерной безопасности в той сфере деятельности, для которой проводится анализ рисков. Правильно проработанная модель нарушителя дополняет цели обеспечения безопасности информации, определенные при оценке активов организации. Вариант модели нарушителя (кибернарушителя) представлен на рис. 1.

Модель угроз

Разработка модели угроз и идентификация уязвимостей неразрывно связаны с инвентаризацией окружения информационных активов организации. Важно понять, как информационная инфраструктура и информационные активы организации связаны между собой. С позиции безопасности информации значимость информационной инфраструктуры может быть установлена только после определения связи между информационными активами и инфраструктурой. В том случае, если процессы поддержания и эксплуатации информационной инфраструктуры в организации регламентированы, сбор информации, необходимый для идентификации угроз и оценки уязвимостей, значительно упрощается.

Рис. 1 Вариант модели нарушителя (кибернарушителя)

При разработке модели угроз можно также говорить о сценариях как о последовательных шагах, в соответствии с которыми могут быть реализованы угрозы. Очень редко случается, что угрозы реализуются в один шаг путем эксплуатации единственного уязвимого места системы.

В модель угроз следует включить все угрозы, выявленные по результатам исследования смежных процессов основной деятельности организации. Угрозы необходимо ранжировать друг относительно друга по уровню вероятности их реализации. Для этого при разработке модели угроз для каждой угрозы необходимо указать наиболее значимые факторы, существование которых оказывает влияние на ее реализацию [1].

Идентификация уязвимостей

После разработки модели угроз необходимо идентифицировать уязвимости в окружении активов. Идентификация и оценка уязвимостей может выполняться в рамках аудита. Для проведения аудита безопасности информации необходимо разработать критерии проверки. А критерии проверки могут быть разработаны как раз на основании модели угроз и модели нарушителя.

По результатам разработки модели угроз, модели нарушителя и идентификации уязвимостей можно говорить о том, что определены причины, влияющие на достижение целевого состояния безопасности информации организации.

На *четвертом этапе* исследуются риски для безопасности информации в организации.

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости – все это стандартные шаги, описание которых должно присутствовать в любой методике исследования рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации. Очень важно понять, что и как можно сделать с большим количеством накопленной информации и формализованными моделями. На наш взгляд, этот вопрос наиболее важен, и ответ на него должна давать используемая методика исследования рисков.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами безопасности информации, либо методом прогнозирования – на основании взвешивания факторов, соответствующих разработанной модели угроз.

Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов. Прогнозирование вероятности угроз проводится уже на основании свойств уязвимости и групп нарушителей, от которых исходят угрозы. В качестве примера системы классификации уязвимостей можно привести стандарт CVSS (Common Vulnerability Scoring System).

Величину (уровень) риска следует определить для всех идентифицированных и соответствующих друг другу наборов «актив – угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах.

На *пятом этапе* принимается решение по обеспечению безопасности информации в организации.

В первую очередь следует разработать простой и наглядный отчет об анализе рисков, основной целью которого будет презентация собранной информации о значимости и структуре рисков безопасности информации в организации. Отчет предоставляется высшему руководству организации.

Для наглядности отчета риски необходимо классифицировать в привычных для организации терминах, сходные риски – агрегировать. В целом классификация рисков может быть многогранной. С одной стороны, речь идет о рисках безопасности информации, с другой – о рисках ущерба для репутации или потери клиента. Классифицированные риски необходимо ранжировать по вероятности их возникновения и по значимости для организации.

Отчет об анализе рисков должен отражать следующие сведения:

– наиболее проблемные области обеспечения безопасности информации в организации;

– влияние угроз безопасности информации на общую структуру рисков организации;

– первоочередные направления деятельности отдела информационной безопасности по повышению эффективности обеспечения безопасности информации.

На основании отчета об анализе рисков руководитель отдела информационной безопасности может разработать план работы отдела на среднесрочный

период и заложить бюджет исходя из характера мероприятий, необходимых для снижения рисков.

Таким образом, методика формализованного описания угроз, уязвимостей и рисков системы защиты информации позволяет систематизировать порядок этапов ее проведения, определить их содержание, выработать рекомендации по обеспечению безопасности информации в организации для конкретной ситуации.

2. Критериально-математический аппарат методики формализованного описания угроз, уязвимостей и рисков

Существующие в настоящее время подходы к количественной оценке рисков (ущерба) от нарушения безопасности информации в организации чаще всего основываются либо на вероятностных вычислениях, либо на экспертных оценках [3].

Использование вероятностных вычислений представляется адекватным только для случаев, где существует устойчивая выборка событий, что для исследуемого случая (оценка рисков) характерно крайне редко. Экспертные заключения требуют определенной квалификации специалистов и специфических знаний у них конкретной оперативной обстановки.

Поэтому для формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними предлагается применить математический аппарат алгебры логики, исключающий отмеченные недостатки.

Первый шаг методики.

Определяются потенциальные угрозы безопасности информации в организации. В качестве угроз для защищаемой информации будем рассматривать средства технической разведки. Техническую разведку по функциональному предназначению классифицируем следующим образом:

– *радиоэлектронная,* включающая в себя: радио; радиотехническую; радиолокационную; радиотепловую; разведку побочных электромагнитных излучений и наводок (ПЭМИН);

– *оптико-электронная,* включающая в себя телевизионную; инфракрасную (тепловизионную и теплопеленгационную); визуальную оптико-электронную; разведку лазерных излучений;

– *компьютерная;*

– *фотографическая;*

– *визуальная оптическая;*

– *акустическая,* подразделяющаяся на акустическую речевую и сигнальную;

– *гидроакустическая,* включающую в себя разведку гидроакустических шумовых полей; гидролокационную; разведку гидроакустических сигналов; разведку звукоподводной связи;

– *магнитометрическая;*

– *химическая;*

– *радиационная;*

– *сейсмическая.*

Из перечисленного перечня угроз выбираются конкретные, характерные для складывающейся оперативной обстановки в сфере безопасности информации в организации.

Второй шаг методики.

Предположим, что угрозу для безопасности информации в организации представляет радиомониторинг (радиоразведка), которая ведется конкурентами.

Исследуются в организации уязвимости, которые могут привести к утечке защищаемой информации.

Допустим, что в организации информация может передаваться по телефону ($Q_{\text{тлф}}$), факсу ($Q_{\text{факс}}$) и видео ($Q_{\text{видео}}$).

Введем обозначения: ($Q_{\text{тлф}}$) – передача информации по телефону в организации; $Q_{\text{тлф}} = 1$ – передача информации в организации по телефону осуществляется, $Q_{\text{тлф}} = 0$ – передача информации в организации по телефону не осуществляется. Аналогично для ($Q_{\text{факс}}$) и ($Q_{\text{видео}}$).

В организации информация может быть использована либо для внутренних целей ($Q_{\text{пер.}} = 0$), либо передана по каналам радиосвязи другим потребителям ($Q_{\text{пер.}} = 1$).

С учетом введенных обозначений для получения вида логической функции, описывающей процедуру передачи информации в организации, составим таблицу истинности (табл. 1) [2].

Поскольку определяющей для передачи информации по каналам радиосвязи другим потребителям является переменная $Q_{\text{пер.}}$, то выходную переменную (логическую функцию) обозначим $Q_{\text{пер. вых.}}$.

Таблица 1

Таблица истинности, описывающая процедуру передачи информации в организации

Входы				**Выход**
$Q_{\text{тлф}}$	$Q_{\text{факс}}$	$Q_{\text{видео}}$	$Q_{\text{пер.}}$	$Q_{\text{пер. вых.}}$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1

По данным таблицы истинности (см. табл. 1) синтезируем логическое выражение для функции $Q_{\text{пер. вых.}}$

1) $Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} \vee Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge \overline{Q}_{\text{видео}} \wedge Q_{\text{пер.}} = Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}}$;

2) $Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} \vee Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge \overline{Q}_{\text{видео}} \wedge Q_{\text{пер.}} = Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{пер.}}$;

3) $\overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} \vee \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge \overline{Q}_{\text{видео}} \wedge Q_{\text{пер.}} = \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}}$;

4) $Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}} \vee Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{пер.}} = Q_{\text{тлф}} \wedge Q_{\text{пер.}}$;

5) $Q_{\text{тлф}} \wedge Q_{\text{пер.}} \vee \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}} = Q_{\text{пер.}}(Q_{\text{тлф}} \vee \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}}) =$

$= Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}})$ (по теореме отражения);

6) $Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}}) \vee \overline{Q}_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} = Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee \overline{Q}_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{видео}}) = Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee Q_{\text{видео}})$ (по теореме отражения).

Таким образом,

$$Q_{\text{пер. вых.}} = Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee Q_{\text{видео}}). \quad (1)$$

Следовательно, уязвимости, которые могут привести к утечке защищаемой информации в организации, при условии ее передачи по каналам радиосвязи другим потребителям в условиях ведения конкурентами радиоразведки, включают: передачу информации из организации другим потребителям по каналам радиосвязи по телефону, факсу и видео (1).

Третий шаг методики.

Рассмотрим угрозы для защищаемой информации в организации с учетом введенных ограничений. Синтезируем логическое выражение для функции $Q_{рр}$ (условие выполнения радиоразведкой возложенных на нее функций).

Введем обозначения: ($Q_{поиск}$) – поиск информации в каналах радиосвязи; $Q_{поиск} = 1$ – поиск информации в каналах радиосвязи осуществляется, $Q_{поиск} = 0$ – поиск информации в каналах радиосвязи не осуществляется. Аналогично для ($Q_{обн.}$) и ($Q_{расп.}$), где ($Q_{обн.}$) – обнаружение информации в каналах радиосвязи; ($Q_{расп.}$) – распознавание информации, полученной из каналов радиосвязи.

Условие выполнения радиоразведкой возложенных на нее функций (риски для безопасности информации в организации) может быть записано

$$Q_{поиск\ вых.} \wedge Q_{обн.\ вых.} \wedge Q_{расп.\ вых.} = Q_{рр} \qquad (2)$$

Детализируем выражение (2).

По аналогии составим таблицу истинности, описывающую процедуру поиска информации в каналах радиосвязи радиоразведкой. По данным таблицы истинности синтезируем логическое выражение для функции поиска

$$Q_{поиск\ вых.} = Q_{пер.\ вых.} \wedge Q_{поиск} (Q_{тлф} \vee Q_{факс} \vee Q_{видео}). \qquad (3)$$

Выражение (3) предполагает, что процесс поиска информации может осуществляться для случаев передачи ее по телефону, факсу и видео.

Перепишем выражение (3) с учетом выражения (1).

$$Q_{поиск\ вых.} = Q_{пер.} \wedge Q_{поиск} (Q_{тлф} \vee Q_{факс} \vee Q_{видео}). \qquad (4)$$

Для $Q_{обн.\ вых.}$ также запишем логическое выражение с предположением того, что радиоразведка может обнаруживать информацию, передаваемую только по телефону и факсу.

$$Q_{обн.\ вых.} = Q_{пер.} \wedge Q_{поиск} \wedge Q_{обн.} (Q_{тлф} \vee Q_{факс} \vee Q_{видео}) \wedge (Q_{тлф} \vee Q_{факс}) = Q_{пер.} \wedge Q_{поиск} \wedge Q_{обн.} (Q_{тлф} \vee Q_{факс})$$

(по теоремам идемпотентности и характер стической). (5)

Для $Q_{расп.\ вых.}$ запишем логическое выражение (с учетом, что может быть распознана информация, передаваемая только по телефону и факсу).

$$Q_{расп.\ вых.} = Q_{пер.} \wedge Q_{поиск} \wedge Q_{обн.} (Q_{тлф} \vee Q_{факс}) \wedge Q_{расп.} (Q_{тлф} \vee Q_{факс}) = Q_{пер.} \wedge Q_{поиск} \wedge Q_{обн.} \wedge Q_{расп.} (Q_{тлф} \vee Q_{факс}). \qquad (6)$$

Следовательно, угрозы, которые могут привести к утечке защищаемой информации в организации, при условии ее передачи по каналам радиосвязи другим потребителям в условиях ведения конкурентами радиоразведки, включают: передачу информации из организации другим потребителям по телефону и факсу.

Четвертый шаг методики.

Проведенные выше расчеты создают условия для получения логического выражения, характеризующего риск для безопасности информации в организации.

С учетом полученных выражений (4, 5, 6) перепишем выражение (2)

$$Q_{рр} = \{Q_{пер.} \wedge Q_{поиск}(Q_{тлф} \vee Q_{факс} \vee Q_{видео})\} \wedge \{Q_{пер.} \wedge Q_{поиск} \wedge Q_{обн.}$$

$$(Q_{тлф} \vee Q_{факс})\} \wedge \{Q_{пер.} \wedge Q_{поиск} \wedge Q_{обн.} \wedge Q_{расп.}(Q_{тлф} \vee Q_{факс})\}$$ (по теоремам характеристическим, идемпотентности, поглощения и отражения)

$$= Q_{пер.} \wedge Q_{поиск} \wedge Q_{обн.} \wedge Q_{расп.}(Q_{тлф} \vee Q_{факс}). \quad (7)$$

Следовательно, риски, которые могут привести к утечке защищаемой информации в организации, при условии ее передачи по каналам радиосвязи другим потребителям в условиях ведения конкурентами радиоразведки (при условии реализации поиска, обнаружения и распознавания), включают: передачу информации из организации другим потребителям по телефону и факсу.

Анализ и оценка ущерба при реализации угроз через уязвимости (риски) от утечки информации в организации обычно осуществляются с учетом конкретной оперативной обстановки и существенных для нее свойств (параметров и характеристик) в данный период времени.

Заключение

На первый взгляд, может показаться, что ряд полученных выводов и рекомендаций в той или иной степени априорно очевиден. Однако, если количество реальных угроз и уязвимостей возрастает в разы (что имеет место в реальных системах), их совместное исследование в силу конкретной оперативной обстановки требует перехода на следующий уровень (например, для рассмотренного выше случая необходимо учитывать скорость передачи сигнала, вид модуляции сигнала, протоколы кодирования информации, особенности ведения радиообмена между потребителями информации и т.п.), и становится невозможным априорно выработать необходимые рекомендации либо по демпфированию рисков, либо по минимизации ущерба от них.

Таким образом, использование предложенной методики формализованного описания угроз, уязвимостей и рисков системы защиты информации для реальной оперативной обстановки с любым количеством угроз и уязвимостей, а также глубиной их исследования, позволит получать обоснованные выводы о наличии рисков и тем самым обуславливать выработку эффективных решений по их демпфированию или минимизации ущерба от них.

Библиография:

1. Царегородцев А.В. Защита информационных ресурсов предприятия. – М.: Изд-во ВГНА Минфина России, 2008.
2. Боридько С.И., Забелинский А.А., Коваленко Ю.И., Тараскин М.М. Защита информации в организациях: методика исследования угроз, уязвимостей и рисков. – М.: МИНИТ, 2011 г.
3. Царегородцев А.В., Лукьянчук А.В. Принципы централизованного управления в системах обнаружения сетевых атак, основанных на многоагентной технологии // Национальная безопасность. – М.: Изд-во «НБ Медиа», 2011. – № 4. – С. 90-95.

References (transliteration):

1. Tsaregorodtsev A.V. Zashchita informatsionnykh resursov predpriyatiya. – M.: Izd-vo VGNA Minfina Rossii, 2008.
2. Borid'ko S.I., Zabelinskiy A.A., Kovalenko Yu.I., Taraskin M.M. Zashchita informatsii v organizatsiyakh: metodika issledovaniya ugroz, uyazvimostey i riskov. – M.: MINIT, 2011 g.
3. Tsaregorodtsev A.V., Luk'yanchuk A.V. Printsipy tsentralizovannogo upravleniya v sistemakh obnaruzheniya setevykh atak, osnovannykh na mnogoagentnoy tekhnologii // Natsional'naya bezopasnost'. – M.: Izd-vo «NB Media», 2011. – № 4. – S. 90-95.