Это проявляется в низкой скорости выполнения анализа событий, его качестве и невыявлении взаимосвязей между событиями, являющихся симптомами инцидента.

Проблемы мониторинга событий негативно влияют на выявление инцидентов.

Инцидент – появление одного или нескольких нежелательных или неожиданных событий, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ [1].

Инцидент – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [2].

Инцидент – событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

• нарушение или возможное нарушение работы средств защиты информации в составе СОИБ организации БС РФ;

• нарушение или возможное нарушение требований законодательства РФ, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение или возможное нарушение в выполнении процессов СОИБ организации БС РФ;

• нарушение или возможное нарушение в выполнении банковских технологических процессов организации БС РФ;

• нанесение или возможное нанесение ущерба организации БС РФ и (или) ее клиентам [3].

Определения выше различаются, но все они, так или иначе, указывают на причинение негативных последствий процессу, информационной системе, организации в результате возникновения инцидента. Таким образом, своевременное выявление инцидента минимизирует потери организации.

В условиях децентрализации информации о событиях из многих источников обнаружение инцидента становится сложной и не всегда решаемой задачей. После выявления инцидента необходимо идентифицировать пострадавшие активы, понять причины инцидента, оценить его степень тяжести, приоритет, предпринять меры по реагированию. При выполнении этих операций исполнители зачастую сталкиваются с той же проблемой разрозненности источников информации. Это проявляется в ненадлежащем реагировании или его отсутствии, что влечёт за собой убытки организации.

SIEM-система позволяет избежать указанных выше проблем. Она решает задачи по сбору и хранению информации из различных источников, анализу поступающих событий, их корреляции и обработке по правилам, обнаружению инцидентов, их приоритезации и автоматическому оповещению. Кроме того, SIEM-системы часто имеют возможность проведения проверки на соответствие стандартам.

Типовая структура SIEM-систем:

• агенты – устанавливаются на информационную систему и передают данные с нее на сервер, в состав агентов могут включаться модули для преобразования данных;

• сервер-коллектор – собирает события от множества источников;

• сервер-коррелятор – собирает и обрабатывает информацию от коллекторов и агентов;

• сервер баз данных – хранит журналы событий.

SIEM-система собирает информацию из различных источников с помощью агентов и серверов-коллекторов в централизованное хранилище данных, что позволяет впоследствии анализировать события в целом. Также это позволяет избежать разрозненной и, в подавляющем числе случаев, неконтролируемой конфигурации средств анализа событий. Негативным моментом такого построения системы является возрастание нагрузки на сеть организации.

После сбора информации SIEM-система начинает анализ событий ИБ, требующийся для обнаружения инцидента. Для этого применяются 2 основных метода корреляции: сигнатурный (т.е. на основе правил) и бессигнатурный, определяющий аномальное поведение информационной системы. По результатам анализа SIEM-система показывает выявленные инциденты ИБ.

Для того чтобы SIEM-система эффективно выполняла свои задачи в конкретной организации, требуется правильная конфигурация корреляционных механизмов и постоянная их модификация. Вследствие этого SIEM-системы начинают окупать себя значительно позже ее внедрения, особенно при применении бессигнатурных методов корреляции, которые требуют накопления статистических данных. Настройкой SIEM-системы организации, как правило, занимается эксперт, прошедший специальные курсы и имеющий определённый опыт в этой области.

Кроме основной задачи по мониторингу событий и обнаружению инцидентов на основе данных о критичности активов организации и опасности угрозы SIEM-системы могут приоритезировать инциденты, автоматически оповещать об инциденте, выдавать заранее подготовленные рекомендации по немедленному реагированию на инцидент, хранить данные об инциденте для последующего расследования.

На данный момент на рынке SIEM-систем можно выделить следующие продукты:

• HP ArcSight;
• McAfee Nitro;
• IBM QRadar;
• Splunk SIEM;
• RSA Security Analytic;
• LogRhythm.

Применение SIEM-системы не является обязательным при построении комплексной системы защиты информации и во многих случаях нецелесообразно. Основным заказчиком таких систем являются крупные организации, в которых требуется непрерывный контроль за обеспечением ИБ и журналирование связанных с этим событий.

В заключение хотелось бы отметить, что SIEM-системы – это развивающийся продукт, функциональные возможности которого со временем расширяются.

Список литературы

1. ГОСТ Р ИСО/МЭК ТО 18044–2007 »Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», 2 стр.

2. ГОСТ Р ИСО/МЭК 27001–2006 »Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности – Требования». – 2 с.

3. СТО БР ИББС-1.0-2014 »Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». – 9 с.

ОБЗОР МЕТОДИК ПРОВЕДЕНИЯ ПРОВЕРОК НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРЕДСТАВЛЕННЫХ В РОССИЙСКИХ И ЗАРУБЕЖНЫХ НОРМАТИВНЫХ ДОКУМЕНТАХ

Никифорова К.А.

Университет ИТМО, Санкт-Петербург,
e-mail: nikiforova.k.a@yandex.ru

Управление соответствием системе требований нормативных документов в области информационной безопасности (далее ИБ) – процесс, направленный на

обеспечение выполнения и демонстрации соответствия набору требований, предъявляемых к системе обеспечения информационной безопасности (далее – СОИБ).

В целом процесс управления соответствием требованиям ИБ состоит из выявления, учета требований ИБ, проведения проверок их выполнения и принятия корректирующих воздействий по результатам выявленных несоответствий.

В данной работе приведен обзор существующих методик проведения оценки соответствия СОИБ, как части процесса управления требованиями ИБ, представленных в действующих российских и зарубежных нормативно-методических документов по ИБ.

СТО БР ИББС-1.2-2014

Для оценки используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ организации, менеджмента и уровня осознания ИБ.

Оценки групповых показателей используются для получения оценки по направлениям. Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки, которые затем формируют оценки групповых показателей.

Частные показатели разделены на два типа: ЧП, выполнение которых обязательно в организации и ЧП, выполнение которых рекомендуется в организации. Способ оценивания частного показателя зависит от его принадлежности к одному из типов.

В процессе проведения устного опроса сотрудников проверяемой организации и наблюдений за деятельностью указанных сотрудников члены проверяющей группы должны сделать вывод о степени соответствия оцениваемой деятельности требованиям внутренних документов проверяемой организации.

Полученные свидетельства оценки соответствия ИБ и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств оценки соответствия ИБ.

В качестве источников свидетельств используются:

• внутренние документы проверяемой организации и при необходимости документы третьих лиц, относящиеся к обеспечению ИБ организации;

• устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;

• результаты наблюдений членов проверяющей группы за деятельностью сотрудников проверяемой организации.

Отдельно вычисляются итоговые оценки по каждому из направлений:

– текущий уровень ИБ организации

– менеджмент ИБ организации

– уровень осознания ИБ организации.

Каждому направлению присваивается уровень соответствия ИБ требованиям СТО БР ИББС-1.0. Значение итоговой оценки определяется по наименьшему значению из трех оценок по направлениям оценки.

Значения, соответствующие уровням с нулевого по третий (Оценка принимает значения от 0 до 0,85), не являются рекомендуемыми Банком России. Для отображения результатов оценивания используется круговая диаграмма.

Положение Банка России N 382-П

Оценка соответствия осуществляется на основе:

• информации на бумажном носителе и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации;

• анализа соответствия порядка применения организационных мер защиты информации и использования технических средств защиты информации требованиям настоящего Положения;

• результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств.

Степень выполнения требований оценивается по заданной шкале оценки.

Проверка соответствия проводится по трем категориям:

• требования к обеспечению защиты информации при осуществлении переводов денежных средств, реализуемых применением организационных мер защиты информации или использованием технических средств защиты информации (Требования категории 1);

• требования к обеспечению защиты информации при осуществлении переводов денежных средств, устанавливающих необходимость обеспечения наличия определенного документа (Требования категории 2);

• требований к обеспечению защиты информации при осуществлении переводов денежных средств, устанавливающих необходимость выполнения определенной деятельности (Требования категории 3).

Система оценки соответствия зависит от категории требований.

Для оценки соответствия требованиям категории 1 используется следующая система оценки:

– требование не выполняется – 0;

– требование выполняется частично – 0.25(меры защиты определены во внутренних документах, но не применяются), 0.5(меры защиты определены во внутренних документах, но осуществляются не в полном соответствии с данными документами) или 0.75(меры защиты определены во внутренних документах, и осуществляются почти в полном соответствии с данными документами);

– требование выполняется полностью – 1.

Для оценки соответствия требованиям категории 2 используется следующая система оценки:

– оценка 0 выставляется, в случае если документ отсутствует;

– оценка 1 выставляется, в случае если документ имеется в наличии.

Для оценки соответствия требованиям категории 3 используется следующая система оценки:

– оценка 0 выставляется, в случае если деятельность не выполняется;

– оценка 0.5 выставляется, в случае если деятельность выполняется частично;

– оценка 1 выставляется, в случае если деятельность выполняется полностью.

С использованием оценки выполнения требований вычисляются три обобщающих показателя (по одному для каждой категории). Обобщающий показатель вычисляется как среднее арифметическое оценок выполнения указанных требований, умноженное на корректирующий коэффициент.

Итоговый принимается равным наименьшему из значений обобщающих показателей.

В зависимости от значения итогового показателя проставляется качественная оценка соответствия требованиям:

<0.5 – «неудовлетворительная»

0.5-0.7 – «сомнительная»

0.7-0.85 – «удовлетворительная»

>0.85 – «хорошая»

NIST 800-53

NIST 800-53 определяет следующие этапы проведения оценки защитных мер:

• Подготовка к оценке

• Разработка планов оценки
• Проведение оценки и анализ результатов
• Анализ итогового отчета и последующие действия.

Оценка осуществляется экспертом или экспертной группой.

На подготовительном этапе рассматривается ряд вопросов, касающихся стоимости, расписания и выполнения оценки, проводится определение целей и области оценки, выбор эксперта или экспертной группы, а также сбор необходимых для оценки данных.

План оценки безопасности содержит цели оценки и детальное описание ее проведения. В ходе разработки планов эксперт определяет включаемые в план защитные меры, а также выбирает, адаптирует и оптимизирует надлежащие процедуры оценки.

После утверждения плана оценки безопасности эксперт или экспертная группа приступает к его выполнению. Оценка мер безопасности производится путем применения к объектам оценки методов оценки. Процедура оценки зависит от оцениваемой меры безопасности (NIST 800-53 разделяет все меры на 17 семейств. Описание методов оценки приводится в приложении к стандарту). При использовании мер безопасности, не описанных в NIST 800-53 эксперты указывают это в плане безопасности и разрабатывают свои процедуры оценки. В качестве методов оценки NIST 800-53 выделяет исследование, интервью и тестирование. На основе собранных свидетельств делается вывод о соответствии или несоответствии мер безопасности предъявляемым требованиям. По результатам оценки безопасности составляется отчет и описание мероприятий по устранению несоответствий.

MEHARI 2010

Методология MEHARI позволяет осуществить полный процесс управления информационными рисками в соответствии со стандартом ISO/IEC 27000. В базу знаний методологии включена оценка оценка комплектации средствами защиты по стандарту ISO/IEC 27002:2005, что позволяет организации подготовиться к прохождению аудита на соответствие стандарту.

Согласно предложенной в MEHARI методике, домены безопасности декомпозируются на сервисы безопасности, состоящие из подсервисов, в которые, в свою очередь, сгруппированы меры безопасности.

Процесс оценки сервиса безопасности осуществляется путем распространения среди подразделений специальных вопросников позволяющих оценить качество решений, направленных на снижение риска. Опросники заполняются аудитором в процессе интервьюирования персонала подразделения.

Выделяется три показателя производительности сервиса безопасности:
• эффективность;
• надежность;
• постоянство.

Качество сервиса безопасности оценивается по шкале от 0 до 4, отражающей сложность нарушения работоспособности сервиса. Описание каждого из уровней приведено в документе MEHARI 2010: Evaluation Guide for security services.

Выводы

Выполненный анализ существующих подходов к проведению проверок на соответствие системе требований ИБ позволяет сделать следующие выводы:

• каждая методика содержит свой перечень требований ИБ, сгруппированных по направлениям оценки, являющихся наиболее важными с точки зрения авторов;

• в качестве демонстрации соответствия требованиям ИБ используются метрики, числовое выражение которых позволяет судить о степени выполнения конкретных требований ИБ и направлений в целом;

• методики отличаются в алгоритме расчета итоговых метрик, но в целом являются общими применение функций свертки с использованием весовых коэффициентов требований.

Таким образом, следует отметить, что при внедрении процесса управления требованиями необходимо определить наиболее важные направления требований ИБ, инвентаризировать их, классифицировать по степени важности и утвердить формулу свертки для определения итогового уровня соответствия СОИБ требованиям ИБ.

Список литературы

1. СТО БР ИББС-1.2-2014 Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014, 2014.
2. Положение Банка России N 382-П О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств, 2012.
3. NIST SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems and Organizations, 2010.
4. MEHARI 2010 knowledge base, 2010.
5. MEHARI 2010: Risk analysis and treatment Guide, 2010
6. MEHARI 2010: Security Stakes Analysis and Classification Guide, 2010.
7. MEHARI 2010: Processing guide for risk analysis and management, 2010.
8. MEHARI 2010: Fundamental concepts and functional specifications, 2010.
9. MEHARI 2010: Evaluation Guide for security services, 2010
10. Управление информационными рисками на основе методологии MEHARI / М.К. Янчин, 2011.

АЛГОРИТМ РАЗРЕШЕНИЯ ПРОТИВОРЕЧИЙ В ПРАВИЛАХ ФИЛЬТРАЦИИ

Семакин А.И., Мордвин Д.В.
Южный федеральный университет, Таганрог, e-mail: neverminden@gmail.com

Обеспечение безопасности компьютерных сетей является важной задачей при построении систем защиты информации. Межсетевые экраны (МЭ) играют большую роль для сетевой безопасности. Межсетевое экранирование – широко распространенный механизм для усиления защищенности сетей организаций. Однако конфигурирование МЭ является сложной задачей, подверженной возникновению ошибок, даже для опытных администраторов. В результате, ошибки конфигурирования МЭ, в частности, противоречия в правилах фильтрации трафика в сети являются достаточно распространенными и серьезными.

Обычно правила фильтрации состоят из полей адреса источника, адреса назначения, порта источника, порта назначения, протокола и действия фильтрации (разрешить или запретить).

Основными видами аномалий для конфигураций МЭ являются несогласованность и неэффективность правил фильтрации трафика.

Конфигурации МЭ отображает намерения администратора, которые должны быть согласованы между собой. Поэтому несогласованность правил в конфигурации часто является хорошим индикатором ошибок конфигурации.

Таблица 1

Пример конфигурационного файла 1

1.	deny tcp 10.1.1.0/25 any
2.	accept udp any 192.168.1.0/24
3.	deny tcp 10.1.1.128/25 any
4.	deny udp 172.16.1.0/24 192.168.1.0/24
5.	accept tcp 10.1.1.0/24 any
6.	deny udp 10.1.1.0/24 192.168.0.0/16
7.	accept udp 172.16.1.0/24 any