7 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК: 681.3

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ АНАЛИЗА ДЕРЕВЬЕВ АТАК

С.А. Арустамов, Ю.А. Гатчин, А.Л. Липатов, А.С. Григорьева

Доказывается актуальность проблемы обеспечения безопасности ключевых систем (КС), проведен анализ основных угроз информационной безопасности (ИБ), разработана расширенная модель управления ИБ, развита методология деревьев атак как базис для разработки средств защиты КС. Разработаны расширенный параллельный автомат для моделирования и обнаружения фактов реализации атак на ключевые системы и расширенный параллельный автомат моделирования собственно деревьев атак. Проведен эксперимент с использованием программного обеспечения, моделирующего атаки и их элементы, результаты которого подтверждают эффективность предложенного подхода.

Ключевые слова: ключевые системы критически важной инфраструктуры, модели систем, угрозы информационной безопасности, деревья атак, параллельный автомат, моделирующий атаки.

Введение

Актуальность проблемы обеспечения информационной безопасности (ИБ) ключевых систем (КС), входящих в состав критически важной информационной инфраструктуры (КСИИ) органов государственной власти (ОГВ) Российской Федерации обусловливается современными условиями ведения деятельности на критически важных объектах информационной и телекоммуникационной инфраструктуры РФ: наличием растущей зависимости бизнес-процессов от информационно-коммуникационных технологий (ИКТ), сложностью используемых технологий, а также большим количеством потенциальных угроз ИБ как случайного, так и преднамеренного характера, включая терроризм, реализация которых может приводить к значительным негативным последствиям для безопасности государства в информационной сфере и препятствовать реализации Российской Федерацией своих целей во внутренней и внешней политике. В настоящей работе предлагается развитие методологии обеспечения безопасности информационных систем на основе деревьев атак, позволяющее внести значительный вклад в решение упомянутых задач.

Общесистемные решения по модели системы информационной безопасности ключевой системы

ИБ КСИИ должна обеспечиваться на комплексной и системной основе в масштабах всего критически важного объекта информационной и телекоммуникационной инфраструктуры РФ, в рамках системы информационной безопасности (СИБ) КСИИ. СИБ КСИИ образуется комплексом технических, программных и программно-технических средств обеспечения ИБ, процессов и персонала, объединенных на основе модели расширенной управления ИБ. Общая модель СИБ КСИИ приведена на рис. 1.

Расширенная модель управления ИБ (EPDCA-модель: Extended «Plan – Do – Check – Act»-модель; расширенная «Планирование–Реализация–Проверка–Улучшение»-модель), реализуемая в рамках СИБ КСИИ, должна базироваться на основе PDCA-цикла Шухарта–Деминга (рис. 2). При этом, в отличие от [1], при создании СИБ КСИИ целесообразно установить жесткие требования по реализации защитных мер эксплуатационного характера (отвечающих за обеспечение ИБ), таких как защитные меры, направленные на обеспечение

безопасности, связанной с персоналом, управление инцидентами ИБ, обеспечение непрерывности деятельности и др. Внедрение данных защитных мер не является обязательным и осуществляется по результатам оценки рисков ИБ, если эти риски ИБ являются неприемлемыми.

Кроме того, в отличие от [2], предлагается не устанавливать жесткие требования к реализации всех защитных мер эксплуатационного характера, описанных, в том числе, в [1], по результатам присвоения КСИИ в соответствии с положениями [3] определенного класса защищенности. В отличие от [1], на этапе «Планирование» («PLAN») PDCA-цикла предлагается осуществлять работы по специальным исследованиям (СИ) основных технических средств (ОТС) КСИИ на ПЭМИН (в случае обработки в КСИИ конфиденциальной информации), а также работы по специальным проверкам ОТС КСИИ на предмет выявления возможно внедренных в них закладных устройств («закладок»).

Рис. 1. Общая модель СИБ КСИИ

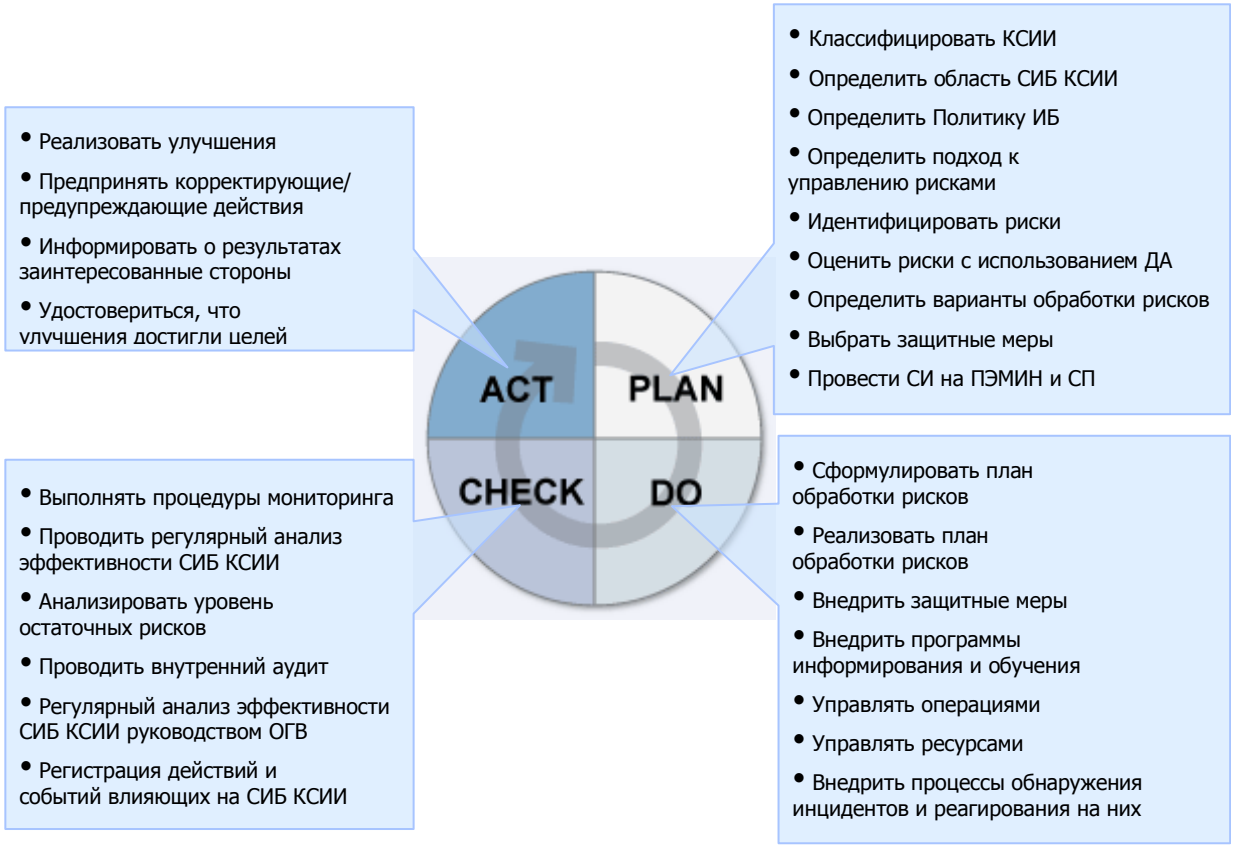

Рис. 2 Расширенная модель управления ИБ (EPDCA-модель) СИБ КСИИ

Организация СИБ КСИИ должна быть основана на следующих принципах:

- комплексность – использование комплексного подхода, предусматривающего применение организационных, процедурных, правовых и технических мер;
- системность – использование системного подхода, предусматривающего объединение всех используемых мер на основе заданной модели управления ИБ;
- управление рисками – оценка рисков возможных инцидентов ИБ и принятие решений по их обработке на основании установленных критериев риска;
- мониторинг – оперативное обнаружение инцидентов ИБ и реагирование на них;
- совершенствование – оценка эффективности функционирования СИБ КСИИ с целью принятия корректирующих и предупреждающих действий и определения возможных улучшений;
- адекватность защитных мер – эффективность защитных мер и их стоимость должна быть адекватной имеющимся рискам.

Разработка перечня угроз информационной безопасности применительно к активам ключевых систем

Для осуществления эффективного управления ИБ КСИИ в рамках расширенной модели управления необходимо осуществить разработку перечня угроз ИБ с указанием типов активов КСИИ, на которые данные угрозы ИБ могут воздействовать. Данная информация приведена в таблице и позволяет при оценке рисков ИБ КСИИ в процессе управления ИБ КСИИ учитывать тот факт, что в целом каждая конкретная угроза ИБ воздействует только на определенные типы активов КСИИ. В таблице приведен перечень угроз с указанием типов активов, на которые они могут воздействовать.

Название угрозы ИБ КСИИ	Активы КСИИ										
	Информационные активы КСИИ	Сервисы КСИИ	Рабочие станции КСИИ	Серверы КСИИ	Активное сетевое оборудование КСИИ	Структурированные кабельные сети КСИИ	Внешние каналы связи КСИИ	Помещения КСИИ	Площадки КСИИ	Внешние сервисы КСИИ	Носители информации КСИИ
1	2	3	4	5	6	7	8	9	10	11	12
1. Фальсификация полномочий (FGR)	•	•									
2.Злоупотребление полномочиями (ABR)	•	•									
3. Применение вредоносного программного обеспечения (IDS)			•	•	•						
4.Недопустимое использование оборудования (MEQ)			•	•	•						
5. Угрозы уровня сетевых интерфейсов (NI)			•	•	•	•	•				
6. Угрозы уровня межсетевых взаимодействий (NE)			•	•	•		•				

7. Угрозы уровня приложений (APP)			•	•	•						
8. Отказ от действий (DEN)		•									
9. Сбой в работе внешнего сервиса (FS)										•	
10. Внедрение вредоносного мобильного кода (MC)	•	•									
11. Технический сбой в работе оборудования (FEQ)			•	•	•						
12. Сбои в сети электропитания (FEL)								•	•		
13. Сбои в работе систем вентиляции и кондиционирования (FCN)								•	•		
14. Сбои в работе программного обеспечения (FSF)			•	•							
15. Ошибки персонала (HE)	•	•	•	•	•						
16. Пожар (FIRE)								•	•	•	
17. Затопление (WTR)								•	•	•	
18. Катастрофы (MA)									•	•	
19. Нехватка персонала (HUN)			•	•	•						
20. Кража (THF)								•	•	•	•
21. Вандализм (VAN)								•	•	•	
22. Использование нелицензионного ПО (NLS)			•	•							
23. Несанкционированное визуальное ознакомление с информацией (VIS)	•										
24. Утечка при утилизации оборудования и носителей (DIS)	•										
25. Разглашение информации (DSCL)	•										
26. Недостаточность функциональных характеристик (IEF)			•	•	•						
27. Утечка / воздействие на информацию по техническим каналам (DTC)	•		•	•	•	•	•				

Таблица. Перечень угроз ИБ с указанием типов активов КСИИ, на которые данные угрозы могут воздействовать

Применение методологии деревьев атак

Рассмотрим использование методологии деревьев атак для моделирования и обнаружения инцидентов информационной безопасности в расширенной модели управления информационной безопасности ключевых систем.

Деревья атак являются формальным методом моделирования реализации угроз ИБ в отношении КСИИ (атак). Атаки представляются в виде деревьев, где корнем является цель атаки, ближайшие узлы – подцелями, а листья – способами достижения подцелей и реализации атаки на основную цель. Дочерние узлы в дереве могут быть двух типов: И (операция «логическое И») и ИЛИ (операция «логическое ИЛИ»). Для реализации атаки необходимо обойти все дочерние узлы типа И или хотя бы один узел типа ИЛИ. Дерево атак при этом формируется следующим образом. Определяются потенциальные

цели атаки. Каждая цель атаки является корнем собственного дерева атак, при этом рассматриваются все возможные атаки на заданные цели. Эти атаки формируют дочерние узлы И и ИЛИ, и каждая из атак рассматривается как цель и формирует ее дочерние узлы. Данный процесс продолжается рекурсивно.

При такой структуре дерева сценарий атаки является поддеревом, которое включает узел – цель, а также все его дочерние узлы И и хотя бы один узел ИЛИ. Подобным образом определяются все поддеревья для дочерних подцелей. Дерево атак является законченным, если оно содержит поддеревья для всех возможных атак, ведущих к достижению главной цели. Для каждого узла можно назначить атрибут (например, время жизни (ВЖ) и др.). Используя такие атрибуты, можно выявить атаки с определенными параметрами, что может быть полезно для определения угроз и требуемых защитных мер.

Автомат деревьев обрабатывает входное дерево, начиная от листьев и заканчивая корнем.

Разработка расширенного параллельного автомата для моделирования и обнаружения фактов реализации атак на ключевые системы

Предлагается ряд модификаций дерева атак для повышения его эффективности при оценке рисков реализации угроз ИБ в отношении активов КСИИ. Во-первых, существуют деревья атак, в которых цели или подцели могут быть достижимы, если все потомки типа И обходятся в заданной последовательности. В этом случае невозможно использовать потомков И или ИЛИ для формирования заданного порядка. Например, «Отключение клиента» в сети WLAN можно реализовать, выполнив атаки типа «Подслушивание MAC-адреса точки доступа», «Подмена AP» и «Отправление сообщения об отключении MAC-адреса жертве» в заданной последовательности. Такие типы потомков назовем У-И (операция «упорядоченное И»).

Еще одна модификация – учет времени жизни (ВЖ) и атрибутов конфиденциальности узла. Атрибут ВЖ определяет время жизни для событий на листьях и для подцелей. В примере «Отключение клиента» клиент получает сообщение «отключен» от точки доступа, но пытается восстановить соединение. Клиент осуществляет последовательность определенных операций для восстановления соединения. Эти операции включают поиск точки доступа с лучшим сигналом, выбор способа аутентификации и подключение к выбранной точке доступа. Атакующий имеет ограниченное время на завершение атаки до того, как жертва восстановит подключение. Таким образом, если с момент достижения подцели прошло времени больше, чем ВЖ, то подцель становится неактуальной. ВЖ позволяет снизить количество ложных срабатываний, что является одной из основных проблем систем обнаружения вторжений, используемых в КСИИ.

Дадим следующее определение. Расширенное дерево атак (РДА) – это дерево атак, в котором дочерние узлы могут быть узлами типа И, У-И или ИЛИ, при этом узлы имеют атрибуты ВЖ и степень конфиденциальности (СК).

Механизм аутентификации протокола 802.1*x* можно обойти путем перехвата сеанса аутентификации или с использованием атаки типа «Человек посередине», чтобы получить аутентификационную информацию пользователя. Каждое событие имеет атрибут ВЖ, каждая подцель имеет атрибуты СК и ВЖ, а каждое ребро имеет тип И, У-И или ИЛИ. Для достижения цели атакующий должен выполнить атаку «Перехват сеанса аутентификации 802.1*x*» или « Человек посередине в сеансе 802.1*x*». Подцель «В-Перехват сеанса аутентификации 802.1*x*», в свою очередь, может быть достигнута за счет подцели «Отключение клиента» и «Подмена аутентифицированного клиента 802.1*x*» в заданном порядке (У-И). Построение дерева продолжается, пока не будут созданы все листья, описывающие все возможные события.

В качестве примера рассмотрим ситуацию, когда пользователь проходит процесс аутентификации 802.1*x*, используя аутентификационную информацию другого активного пользователя. В этом случае можно сделать вывод, что дерево атак не полностью построено, так как атакующий перехватывает сеанс и легальный пользователь пытается подключиться, или атакующий уже получил аутентификационную информацию пользователя с использованием атаки «Человек посередине» (например, подобрав слабый пароль, используя шпионское ПО, методы социальной инженерии и т.п.). Таким образом, дерево не только моделирует атаку, но и является средством самодиагностики для проверки законченности моделей известных атак.

Разработка расширенных автоматов деревьев атак

Существует несколько недостатков недетерминированных конечных автоматов деревьев (НКАД), в связи с чем они не подходят для использования с расширенными деревьями атак. Во-первых, НКАД предполагает дерево в качестве входа, обрабатывая его, когда достигается финальное состояние. В нашей системе входом является поток сообщений, среди которых ищутся конкретные деревья.

Логическая переменная *x* принимает значение *true,* если соответствующее событие *x* появляется во входном потоке не позже, чем ВЖ(*x*). Переменная принимает значение *false,* если событие не появляется или если появляется ранее, чем ВЖ(*x*).

Расширенный автомат атак обеспечивает следующие функциональности: обнаружение атак, обнаружение частей атак, проверку законченности дерева атак. Расширенный автомат атак основан на НКАД, но улучшен путем ведения состояний частей атак наряду с финальными состояниями, деривационных правил для подцелей и правил обратных переходов для отката автомата, когда истекает время жизни для события или подцели. Входом автомата является поток значений целочисленных переменных, принимающих значения от 1 до *n*. Когда автомат достигает одного из состояний части атаки, он сообщает об атаке с атрибутом СК. Когда автомат достигает одного из состояний, он сообщает об атаке в совокупности с последовательностью событий, которые к ней привели. Автомат автоматически сбрасывается в начальное состояние, когда достигается финальное состояние, и продолжает обрабатывать входной поток.

Расширенный автомат деревьев получается из расширенного дерева атак, т.е. создается для обнаружения единственного дерева, формируемого из потока входных значений. Более сложные атаки, которые являются комбинацией нескольких расширенных деревьев атак, могут быть обработаны двумя способами. Во-первых, можно создать отдельный расширенный автомат деревьев атак для каждого расширенного дерева атак и передать копию входного потока в каждый автомат. Во-вторых, можно создать расширенный параллельный автомат, который является комбинацией расширенных деревьев атак и использует единый входной поток для параллельного обнаружения нескольких атак.

Результаты эксперимента

Эксперимент проводился с использованием специального ПО, имитирующего поведение системы обнаружения атак и генератора событий. Генерируемые события представляли собой как элементы атак на протокол 802.11, так и обычные сетевые события. Генератор событий отправлял как случайные события со случайными интервалами времени, так и детерминированные последовательности, имитирующие атаки или их элементы. Определялась зависимость количества ложных срабатываний от процента сообщений, свидетельствующих об атаке, в общем потоке сообщений. Результаты эксперимента доказывают эффективность предложенного подхода по использованию ме-

тодологии деревьев атак в процессе оценки рисков ИБ КСИИ в рамках расширенной модели управления ИБ.

Заключение

Приведены общесистемные решения по модели СИБ КСИИ. Приведена расширенная модель управления ИБ, реализуемая в рамках СИБ КСИИ, базирующаяся на основе PDCA-модели Шухарта–Деминга.

Выявлен перечень угроз ИБ с указанием типов активов КСИИ, на которые данные угрозы ИБ могут воздействовать, а также перечень угроз ИБ КСИИ с указанием уязвимостей, при помощи которых данные угрозы могут быть реализованы; эти перечни необходимы для эффективного управления ИБ в рамках разработанной расширенной модели управления ИБ КСИИ.

Осуществлена разработка расширенного дерева атак, расширенных автоматов деревьев атак, расширенного параллельного автомата, используемых для эффективного моделирования и обнаружения инцидентов ИБ в рамках расширенной модели управления ИБ КСИИ.

Литература

1. Нормативно-методический документ «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры». – М.: ФСТЭК России, 2008.
2. ISO/IEC 27002:2005 Information technology. Security techniques. Code of practice for information security management.
3. Нормативно-методический документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры». – М.: ФСТЭК России, 2008.

Арустамов Сергей Аркадьевич – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, доктор технических наук, профессор, sergey.arustamov@gmail.com

Гатчин Юрий Арменакович – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, доктор технических наук, профессор, gatchin@mail.ifmo.ru

Липатов Алексей Леонидович – ЗАО "ОТКРЫТЫЕ ТЕХНОЛОГИИ 98", технический руководитель направления отдела информационной безопасности, alipatov@ot.ru

Григорьева Анастасия Сергеевна – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, студентка, yojik2@yandex.ru