УДК 004.056.52

ПРОЦЕСС УПРАВЛЕНИЯ СОБЫТИЯМИ КАК СОСТАВНАЯ ЧАСТЬ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Кузнецов А.В.,
*аспирант**,** Финансовый университет, Москва, Россия*
a.kuznetsov@ntc-vulkan.ru

Аннотация. *В статье автор рассматривает место процесса управления событиями в рамках системы менеджмента информационной безопасности предприятия и его взаимосвязь с другими процессами управления предприятия. Предлагаемая автором схема взаимодействия учитывает декомпозицию системы менеджмента информационной безопасности предприятия на ряд процессов, наличие односторонних и двухсторонних связей между ними.*

Ключевые слова: *процесс управления; система менеджмента; событие; инцидент; уязвимость; угроза; актив.*

EVENT MANAGEMENT PROCESS AS A COMPONENT OF THE INFORMATION MANAGEMENT SYSTEM OF ENTERPRISE

Kuznetsov A.V.,
graduate student, Financial University, Moscow, Russia
a.kuznetsov@ntc-vulkan.ru

Absrtact. *In the article the author considers the place of the process of event management within the framework of the enterprise information security management system and its relationship with other enterprise management processes. The interaction scheme proposed by the author takes into account the decomposition of the enterprise information security management system into a number of processes, the existence of unilateral and bilateral relationships between them.*

Keywords: *management process; management system; event; incident; vulnerability; threat; asset.*

Вопросы обеспечения информационной безопасности предприятий непрерывно развиваются и выходят на один из первых планов в научно-практической деятельности. При этом в последние годы в работе специалистов по защите информации акцент смещается в сторону готовности своевременного выявления и расследования инцидентов информационной безопасности. Данное обстоятельство требует обеспечить подотчетность помимо конфиденциальности, целостности и доступности. Обеспечение данного свойства возможно в рамках процесса управления событиями, который реализуется в составе системы менеджмента информационной безопасности (СМИБ) предприятия. Принимая во внимание, что СМИБ предприятия — это часть общей системы управления [1], которая с технологической точки зрения относится к сетецентрическим системам реального и в ряде случаев даже ультрареального

Научный руководитель: ***Шеремет И.А.,*** *доктор технических наук, профессор, Финансовый университет.*

времени [2], вопросы организации и качества взаимосвязи процесса управления событиями с другими процессами управления являются крайне актуальными.

В рамках настоящей публикации под событием понимается изменение или сохранение состояния, которое имеет значение для безопасности, управления и/или работоспособности компонента(ов) информационно-телекоммуникационной инфраструктуры или автоматизированной информационной системы предприятия, а также зарегистрированная в журнале (файле, таблице базы данных или ином месте) информация о данном событии [3, 4].

Событие в рамках математической постановки задачи представляется в виде лингвистической переменной [5]: E_i (например, E_1 = *{Вход с учетной записью выполнен успешно}*), где $i \hat{I} [1; n]$.

Предлагается следующее описание процесса управления событиями [1, 4]:

- определение политики управления событиями;
- обеспечение инфраструктуры управления событиями;
- обработка событий в рамках их жизненного цикла;
- контроль инфраструктуры управления событиями и политики управления событиями;
- коррекция инфраструктуры управления событиями и политики управления событиями в случае необходимости.

Полноценное описание взаимосвязи процесса управления событиями с другими процессами управления на предприятии представлено в документе «Процессы эксплуатации услуг» (Service Operation Processes) [6] в рамках методологии IT Infrastructure Library. Все остальные существующие стандарты и рекомендации опираются и/или ссылаются на данный документ.

В рамках документа [6] отмечена взаимосвязь процесса управления событиями со следующими процессами управления предприятия:

- управление информационной безопасностью;
- управление инцидентами;
- управление проблемами;
- управление доступом;
- управление изменениями;
- управление доступностью;
- управление мощностью;
- управление активами;
- управление конфигурациями;
- управление знаниями;
- управление уровнем сервиса.

К недостаткам данного подхода стоит отнести:

- ориентацию данного подхода на информационно-телекоммуникационные сервисы (услуги), а не на обеспечение информационной безопасности предприятия;
- представление группы процессов в рамках СМИБ предприятия только одним процессом — управление информационной безопасностью.

Таким образом, возникает необходимость в декомпозиции процессов в рамках СМИБ предприятия как минимум на следующие первоочередные процессы:

- управление уязвимостями;
- управление угрозами;
- управление требованиями в части соответствия им, и определение их взаимосвязи с процессом управления событиями.

Автором предлагается схема взаимосвязи процессов управления, учитывающая предыдущие результаты исследования данного вопроса [3, 7].

В рамках данной схемы процесс управления событиями является:

- процессом первичным для всех остальных процессов управления;
- одним из двух доступных вариантов взаимодействия автоматизированных информационных систем предприятия со специалистами по эксплуатации, сопровождению и/или защите информации (альтернативным вариантом является прямое обращение пользователей к данным специалистам), а также, что существуют односторонние и двухсторонние связи данного процесса с рядом процессов управления, которые будут рассмотрены далее;
- односторонняя взаимосвязь с процессом управления инцидентами;
- односторонняя взаимосвязь с процессом управления проблемами;
- односторонняя взаимосвязь с процессом управления изменениями;
- односторонняя взаимосвязь с процессом управления требованиями;
- двухсторонняя взаимосвязь с процессом управления активами;

• двухсторонняя взаимосвязь с процессом управления уязвимостями;

• двухсторонняя взаимосвязь с процессом управления угрозами.

Взаимосвязь с процессом управления инцидентами направлена на формирование (создание) инцидента(ов) информационной безопасности на базе одного или нескольких событий, а также на дальнейшее обогащение данных об инциденте информационной безопасности новыми событиями, в том числе путями:

• агрегации однотипных событий;

• корреляции событий по различным параметрам, в том числе временным, а также с использованием логических операций.

Взаимосвязь с процессом управления проблемами направлена на формирование (создание) проблем(ы), выступающей неизвестной причиной нескольких однотипных инцидентов информационной безопасности на базе нескольких событий.

Взаимосвязь с процессом управления изменениями направлена на инициацию изменений в автоматизированной информационной системе предприятия на базе нескольких событий.

Взаимосвязь с процессом управления требованиями направлена на обеспечение анализа и оценки соответствия требованиям на базе событий, в том числе путем автоматизации процедур подготовки и заполнения отчетных документов, связанных с соблюдением требований действующего международного законодательства, законодательства Российской Федерации и/или внутренних локальных актов предприятия.

Взаимосвязь с процессом управления активами направлена на обогащение событий сведениями об активах предприятия. Необходимо отметить, что в зависимости от потребностей каждого конкретного предприятия под активом понимается определенный объект, например:

• автоматизированная информационная система;

• набор узлов (хостов) локальной или распределенной вычислительной сети, идентифицированных по IP-адресам и/или DNS-именам;

• узел (хост) локальной или распределенной вычислительной сети, идентифицированный по IP-адресу и/или DNS-имени;

• совокупность программного обеспечения;

• отдельно взятый экземпляр (инстанс) программного обеспечения;

• персонал.

Это позволяет операторам решений класса Security Information and Event Management, осуществляющих сбор данных от различных источников событий (средств защиты информации, средств контроля и анализа защищенности и т.п.) [7], оперировать не просто IP-адресами и/или DNS-именами, а следующими параметрами актива:

• категория актива [среда разработки, тестовая среда, предпродакшн среда, рабочая (продакшн) среда и т.п.];

• важность актива (высокий, низкий, средний и т.п.);

• конфигурационные данные (состав и версии программного обеспечения).

Данная информация позволяет приоритизировать финансовые, материальные, трудовые и/или временные ресурсы специалистов по защите информации для выявления (детектирования) инцидентов информационной безопасности, затрагивающих наиболее критичные активы предприятия.

Взаимосвязь с процессом управления уязвимостями направлена на обогащение событий сведениями об уязвимостях, присущих активам предприятия, в том числе:

• факт наличия уязвимости актива;

• идентификаторы и описание уязвимостей (например, Common Vulnerabilities and Exposures);

• уровень критичности уязвимости (например, Common Vulnerability Scoring System).

Указанная информация особенно актуальна в совокупности с данными от процесса управления угрозами. Данная совокупность позволит приоритизировать ресурсы специалистов по защите информации в отношении способов реализации угроз безопасности информации, которые могут быть реализованы с использованием существующих уязвимостей активов и в первую очередь затрагивают наиболее критичные активы предприятия.

Взаимосвязь с процессом управления угрозами направлена на обогащение событий сведениями об актуальных угрозах безопасности информации, возникающих при их обработке в автоматизированных информационных систе-

мах предприятия, полученных из внутренних и/или внешних центров (сервисов) компетенции, в том числе:

- центров операционной безопасности (Security Operations Center);
- команд реагирования на инциденты (Computer Emergency Response Team);
- центров киберразведки (Threat Intelligence Center).

В данном случае осуществляется обогащение событий индикаторами компрометации (Indicator of Compromise), которые позволят при обработке событий оперировать не просто публичными IP-адресами и/или DNS-именами, которые фигурируют в журналах событий в полях отправителей или получателей сообщений, а информацией о принадлежности данных узлов информационно-телекоммуникационной сети Интернет (групп узлов) к ботнетам, в том числе центрам управления ботнетами (Command & Control), источникам распространения вредоносного программного обеспечения или спама, фишинговым ресурсам и т.п.

Используя данные сведения, операторы решений класса Security Information and Event Management смогут уделить первостепенное внимание событиям с участием подозрительных узлов информационно-телекоммуникационной сети Интернет, а также на базе данных индикаторов компрометации формировать соответствующие корреляционные правила, которые позволят своевременно выявлять реализацию наиболее актуальных атак в отношении информационно-телекоммуникационных инфраструктур предприятий.

Предложенная схема взаимосвязи процесса управления событиями с другими процессами управления предприятия учитывает недостатки существующих подходов, в том числе отсутствие декомпозиции СМИБ, и позволяет обеспечить комплексный подход к построению СМИБ предприятия, а также позволяет приоритизировать финансовые, материальные, трудовые и/или временные ресурсы специалистов по защите информации для выявления инцидентов информационной безопасности на базе событий, обогащенных сведениями об активах, уязвимостях и угрозах безопасности информации.

Предлагаемая автором схема взаимосвязи процесса управления событиями с другими процессами управления предприятия является инвариантной к реализации источников событий и решений класса Security Information and Event Management, что позволяет применять ее для различных информационно-телекоммуникационных инфраструктур предприятий, в том числе тех, которые появятся в ближайшие годы в результате развития информационных технологий.

Стоит отметить, что данный способ может быть перенесен для решения аналогично поставленных задач в других научно-практических областях.

Список источников

1. *Kuznetcov A.* Going Beyond the Technical in SIEM. ISACA Journal. 2016. № 3 С. 1–3.
2. *Шеремет И.А.* Гибкие технологии как средство повышения боевой эффективности вооруженных сил и конкурентоспособности экономики. Издательство: Межрегиональное общественное учреждение «Институт инженерной физики» (Серпухов), 2015. С. 82–85.
3. *Кузнецов А.В., Муравьева Д.С.* Создание систем управления событиями и инцидентами ИБ (SIEM) // Информационная безопасность. 2012. № 3. С. 28–29.
4. *Кузнецов А.В.* Способ организации процесса управления событиями в части их обработки, в рамках системы управления информационной безопасностью предприятия // Вопросы защиты информации. 2015. № 2. С. 57–62.
5. *Кузнецов А.В.* Способ определения событий, регистрируемых в журналах аудита // Безопасность информационных технологий. 2016. № 1. С. 59–63.
6. ITIL Service Operation Second edition. 2011. С. 58–72.
7. *Кузнецов А.В.* Процесс управления событиями как основа обеспечения информационной безопасности при эксплуатации телекоммуникационных систем органов внутренних дел // Материалы международной научно-практической конференцию. Ч. 2. Воронеж, 2016. С. 9–100.