ВЗАИМОСВЯЗЬ ПРОЦЕССА УПРАВЛЕНИЯ СОБЫТИЯМИ С ДРУГИМИ ПРОЦЕССАМИ УПРАВЛЕНИЯ ПРЕДПРИЯТИЯ

Кузнецов А.В.[1]

Рассматривает взаимосвязи процесса управления событиями с другими процессами управления предприятия в рамках системы управления (менеджмента) информационной безопасностью предприятия, в том числе существующий подход, базирующийся на методологии IT Infrastructure Library, разработанной Британским правительственным агентством Office of Government Commerce. Предлагаемая автором схема взаимосвязи процесса управления событиями с другими процессами управления предприятия в разрезе обеспечения информационной безопасности предприятия, учитывает декомпозицию системы управления (менеджмента) информационной безопасностью предприятия на ряд процессов, наличие односторонних и двухсторонних связей между процессом управления событиями и другими процессами управления предприятия, а также позволяет приоритизировать финансовые, материальные, трудовые и/или временные ресурсы специалистов по защите информации при реализации мероприятий по выявлению (детектированию) инцидентов информационной безопасности на базе зарегистрированных событий, обогащенных сведениями об активах предприятия, уязвимостях данных активов и актуальных угрозах безопасности информации при их обработке в автоматизированных информационных системах предприятия. Данные сведения, направленные на обогащение событий, формируются при реализации соответствующих процессов управления в рамках системы управления (менеджмента) информационной безопасностью предприятия.

***Ключевые слова**: процесс управления, событие, инцидент, уязвимость, угроза, актив*

DOI: 10.21681/2311-3456-2017-5-17-22

Введение

Проблема обеспечения информационной безопасности предприятий не только не теряет своей актуальности, начиная с середины прошлого века, но и стремительно развивается и выходит на один из первых планов в научно-практической деятельности. При этом в последние годы в работе специалистов по защите информации на первое место выходит именно готовность своевременного выявления (детектирования) и расследования инцидентов информационной безопасности. Данное обстоятельство требует обеспечить помимо классической триады «конфиденциальность, целостность и доступность» однозначное прослеживание действий любого субъекта доступа в автоматизированных информационных системах предприятия, т.е. подотчетность. Обеспечение данного свойства возможно в рамках процесса управления событиями, который реализуется в составе системы управления (менеджмента) информационной безопасностью предприятия. Принимая во внимание, что система управления (менеджмента) информационной безопасностью предприятия являются частью общей системы управления предприятием [1], а также с технологической точки зрения относится к сетецентрическим системам реального времени и в ряде случаев даже к сетецентрическим системам ультрареального времени [2], то вопросы организации и качества взаимосвязи процесса управления событиями с другими процессами управления являются крайне актуальными. Стоит отметить, что без наличия данных взаимосвязей невозможно говорить о системе как таковой, т.к. система – это совокупность взаимосвязанных компонентов.

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*О– определение политики управления событиями;

– обеспечение инфраструктуры управления событиями;

– обработка событий в рамках их жизненного цикла;

– контроль инфраструктуры управления событиями и политики управления событиями;

1 Кузнецов Александр Васильевич, Финансовый университет при Правительстве РФ, Москва, Россия. E-mail: 1283_my@mail.ru

– коррекция инфраструктуры управления событиями и политики управления событиями в случае необходимости.

Существующие подходы, определяющие взаимосвязь процессов управления

На сегодняшний день полноценное описание взаимосвязи процесса управления событиями с другими процессами управления на предприятии представлено в документе «Процессы эксплуатации услуг» (Service Operation Processes) [6], разработанном Британским правительственным агентством Office of Government Commerce в рамках методологии IT Infrastructure Library. Все остальные существующие стандарты и рекомендации опираются и/или ссылаются на данный документ.

В рамках документа [6] отмечено взаимодействие процесса управления событиями со следующими процессами управления:

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

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 системы управления (менеджмента) информационной безопасностью предприятия двумя процессами – управление информационной безопасностью и управление доступом.

Таким образом, возникает необходимость в декомпозиции процессов в рамках системы управления (менеджмента) информационной безопасностью предприятия, как минимум на следующие первоочередные процессы:

– управление уязвимостями;
– управление угрозами (киберразведка);
– управление требованиями в части соответствия им,

и определения их взаимосвязи с процессом управления событиями.

Обобщенная схема взаимосвязи процессов управления

Обобщенная схема взаимосвязи процессов управления, предлагаемая автором, в том числе учитывающая предыдущие результаты исследования данного вопроса [3,7], приведена на рисунке (рис.1).

Из приведенной схемы видно, что процесс управления событиями является:

– процессом первичным для всех остальных процессов управления, стоит отметить, что на практике ошибочно в качестве первичного процесса рассматривают процесс управления инцидентами [8];
– 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.

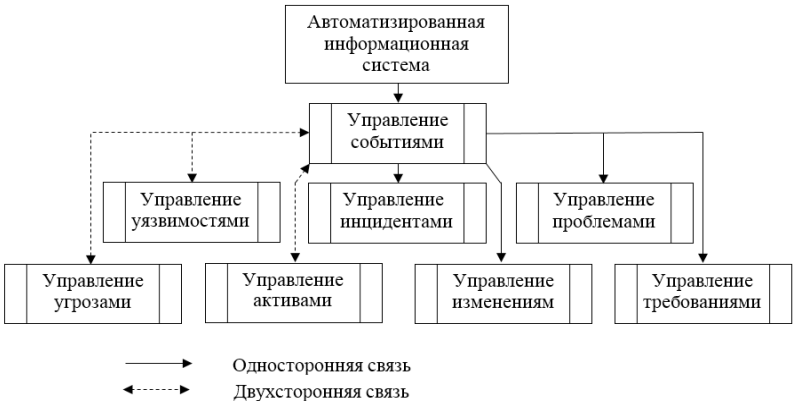

***Рис.1**. Обобщенная схема взаимодействия процессов управления*

Взаимосвязь с процессом управления инцидентами

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 (за определенный промежуток времени), а также с использованием логических операций (И, ИЛИ, НЕ, включая, не включая и т.п.).

Взаимосвязь с процессом управления проблемами

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

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

Взаимосвязь с процессом управления требованиями

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 законодательства Российской Федерации и/или внутренних локальных актов предприятия.

Взаимосвязь с процессом управления активами

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;

– пул узлов вычислительной сети, идентифицированных по IP-адресам и/или DNS-именам;

– узел вычислительной сети, идентифицированный по IP-адресу и/или DNS-имени;

– совокупность программного обеспечения;

– отдельно взятый экземпляр 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.) [9,10], 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).

Отдельно стоит отметить возможность обогащения событий сведениями о персонале, получаемыми из зачастую неподдерживаемых штатно решениями класса Security Information and Event Management источниками событий класса Enterprise Resource Planning [11,12]. В данном случае можно выявлять события, связанные с действиями определенных групп пользователей, например:

– привилегированных пользователей с правами системных администраторов или администраторов безопасности информации;

– руководство предприятия;

– пользователей, работающих с автоматизированными информационными системами предприятия в рамках аутсорсинга или аутстаффинга;

– работников, находящихся в отпуске;

– работников, находящихся на испытательном сроке или в процессе расторжения трудовых отношений с работодателем.

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

Взаимосвязь с процессом управления уязви-

мостями 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

Взаимосвязь с процессом управления угрозами (киберразведкой) направлена на обогащение событий сведениями об актуальных угрозах безопасности информации, возникающих при их обработке в автоматизированных информационных системах предприятия, полученных из внутренних и/или внешних центров (сервисов) компетенции [13], в том числе:

– центров операционной безопасности (Security Operations Centers);

– центров реагирования на инциденты информационной безопасности (Computer Emergency Response Teams);

– центров киберразведки (Threat Intelligence Centers).

В данном случае осуществляется обогащение событиями 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.

Выводы

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

Достоверность результатов подтверждается корректным использованием теоретических методов, а также тем, что предложенный способ получил практическое подтверждение в ряде проектов по автоматизации процесса управления событиями и его интеграции на технологическом уровне с автоматизированными информационными системами предприятия, обеспечивающими автоматизацию соответствующих смежных процессов управления (средства инвентаризации активов предприятия, средства контроля и анализа защищенности, средства класса Enterprise Resource Planning, средства доставки данных из соответствующих центров (сервисов) компетенции), с использованием следующих решений класса Security Information and Event Management на базе Научно-технического центра «Вулкан» (г. Москва):

1. RSA Security Analytics.
2. IBM QRadar Security Intelligence Platform.
3. McAfee Enterprise Security Manager.

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.

***Рецензент**: Дворянкин Сергей Владимирович, доктор технических наук, профессор кафедры информационной безопасности Финансового университета при Правительстве Российской Федерации, Москва, Россия. E-mail: SVDvoryankin@fa.ru*

Литература

1. Kuznetcov A. Going Beyond the Technical in SIEM. - ISACA Journal. N 3. 2016. - 1-3 p.
2. Шеремет И.А. Гибкие технологии как средство повышения боевой эффективности вооруженных сил и конкурентоспособности экономики. // Институт инженерной физики. - 2015 - 82-85 с.
3. Кузнецов А.В., Муравьева Д.С. Создание систем управления событиями и инцидентами ИБ (SIEM). - М.: Информационная безопасность № 3. - 2012. - 28-29 с.
4. Кузнецов А.В. Способ организации процесса управления событиями, в части их обработки, в рамках системы управления информационной безопасностью предприятия - М: Вопросы защиты информации № 2. - 2015. - 57-62 с.
5. Кузнецов А.В. Способ определения событий, регистрируемых в журналах аудита. - М:Безопасность информационных технологий № 1 - 2016. - 59-63 с.
6. ITIL Service Operation Second edition. - 2011. - 58-72 с.
7. Кузнецов А.В. Процесс управления событиями как основа обеспечения информационной безопасности при эксплуатации телекоммуникационных систем органов внутренних дел. - Воронеж: Материалы международной научно-практической конференцию. Часть 2. - 2016. - 98-100 с.
8. Maria B. Line, Inger Anne Tøndel, Martin Gilje Jaatun. Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations. - International Journal of Critical Infrastructure Protection. - December 2015. - DOI: 10.1016/j.ijcip.2015.12.003.
9. Марков А.С., Фадин А.А., Цирлов В.Л., Рауткин Ю.В. О централизации управления информационной безопасностью предприятия // В сборнике: Региональная информатика и информационная безопасность Сборник трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2015. С. 345-347.
10. Марков А.С., Фадин А.А. Конвергенция средств защиты информации. // Защита информации. Инсайд. 2013. № 4 (52). С. 80–81.
11. Кузнецов А.В., Волкович Е.К. Методика подключения неподдерживаемых источников событий к системам класса Security Information and Event Management (SIEM). «Безопасные информационные технологии». Сборник трудов Шестой всероссийской научно-технической конференции /под ред. Матвеева В.А.: - М:Изд-во Научно-учебный комплекс «информатика и системы управления» МГТУ им. Н.Э. Баумана. - 2015. - 249-254 с.
12. Кузнецов А.В., Волкович Е.К. Методика подключения ERP-системы как неподдерживаемого источника событий к системе класса Security Information and Event Management (SIEM). - М: Молодежный научно-технический вестник. № 02 [Электронный ресурс]: http://sntbul.bmstu.ru/doc/834709.html Проверено 18.05.2016.
13. Hakan Kilinc, Ugur Cagal. A Reputation Based Trust Center Model for Cyber Security. - 4th International Symposium on Digital Forensics and Security. - April 2016. - DOI: 10.1109/ISDFS.2016.7473508

THE RELATIONSHIP OF THE EVENT MANAGEMENT PROCESS WITH OTHER MANAGEMENT PROCESSES OF THE ENTERPRISE

***A. Kuznetcov*[2]**

In the present article, the author considers relationships of event management process with other management processes of the enterprise within information security management system, including the existing approach, which is based on methodology of IT Infrastructure Library developed by the British government agency Office of Government Commerce. The diagram of relationships of event management process offered by the author with other management processes of the enterprise in a section of support of information se–

2 Aleksandr Kuznetcov, Financial University under the Government of the Russian Federation, Moscow, 1283_my@mail.ru

curity of the enterprise, considers decomposition of information security management system on a row of processes, existence of one–sided and two–way communications between event management process and other management processes of the enterprise, and also allows to prioritize financial, material, work and/or temporal resources of specialists in information security in case of implementation of actions for detection of information security incidents on the basis of the registered events enriched with data on assets of the en–terprise, vulnerabilities of these assets and actual security threats in case of their processing in automated enterprise information systems. These data directed to enrichment of events are created in case of imple–mentation of the appropriate management processes within information security management system.

***Keywords**: management process, event, incident, vulnerability, threat, asset*

References

1. Kuznetcov A. Going Beyond the Technical in SIEM. - ISACA Journal #3 - 2016. - 1-3 c.
2. Sheremet I.A. Gibkie tekhnologii kak sredstvo povysheniya boevoy effektivnosti vooruzhennykh sil i konkurentosposobnosti ekonomiki. - Izdatel'stvo: Mezhregional'noe obshchestvennoe uchrezhdenie «Institut inzhenernoy fiziki» (Serpukhov). - 2015 - 82-85 s.
3. Kuznetcov A.V., Murav'yeva D.S. Sozdanie sistem upravleniya sobytiyami i intsidentami IB (SIEM). - M.: Informatsionnaya bezopasnost' № 3. - 2012. - 28-29 s.
4. Kuznetcov A.V. Sposob organizatsii protsessa upravleniya sobytiyami, v chasti ikh obrabotki, v ramkakh sistemy upravleniya informatsionnoy bezopasnost'yu predpriyatiya - M: Voprosy zashchity informatsii № 2. - 2015. - 57-62 s.
5. Kuznetcov A.V. Sposob opredeleniya sobytiy, registriruemykh v zhurnalakh audita. - M:Bezopasnost' informatsionnykh tekhnologiy № 1 - 2016. - 59-63 s.
6. ITIL Service Operation Second edition. - 2011. - 58-72 s.
7. Kuznetcov A.V. Protsess upravleniya sobytiyami kak osnova obespecheniya informatsionnoy bezopasnosti pri ekspluatatsii telekommunikatsionnykh sistem organov vnutrennikh del. - Voronezh: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsiyu. Chast' 2. - 2016. - 98-100 s.
8. Maria B. Line, Inger Anne Tøndel, Martin Gilje Jaatun. Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations. - International Journal of Critical Infrastructure Protection. – December 2015. - DOI: 10.1016/j.ijcip.2015.12.003.
9. Markov A.S., Fadin A.A., Cirlov V.L., Rautkin Yu.V. O centralizacii upravleniya informacionnoj bezopasnost'yu predpriyatiya. V sbornike: Regional'naya informatika i informacionnaya bezopasnost' Sbornik trudov. Sankt-Peterburgskoe Obshchestvo informatiki, vychislitel'noj tekhniki, sistem svyazi i upravleniya. 2015. S. 345-347.
10. Markov A.S., Fadin A.A. Konvergentsiya sredstv zashchity informatsii. Zashchita informatsii. Insayd. № 4 (52), 2013. 80–81 s.
11. Kuznetcov A.V., Volkovich E.K. Metodika podklyucheniya nepodderzhivaemykh istochnikov sobytiy k sistemam klassa Security Information and Event Management (SIEM). «Bezopasnye informatsionnye tekhnologii». Sbornik trudov Shestoy vserossiyskoy nauchno-tekhnicheskoy konferentsii /pod red. Matveeva V.A.: - M:Izd-vo Nauchno-uchebnyy kompleks «informatika i sistemy upravleniya» MGTU im. N.E. Baumana. - 2015. - 249-254 s.
12. Kuznetcov A.V., Volkovich E.K. Metodika podklyucheniya ERP-sistemy kak nepodderzhivaemogo istochnika sobytiy k sisteme klassa Security Information and Event Management (SIEM). - M:Molodezhnyy nauchno-tekhnicheskiy vestnik # 02 [Elektronnyy resurs]: http://sntbul.bmstu.ru/doc/834709.html Provereno 18.05.2016.
13. Hakan Kilinc, Ugur Cagal. A Reputation Based Trust Center Model for Cyber Security. - 4th International Symposium on Digital Forensics and Security. - April 2016. - DOI: 10.1109/ISDFS.2016.7473508