Раздел III. Защита объектов информатизации

УДК 004.056.5

Е.А. Максимова, Т.А. Омельченко, В.В. Алексеенко

ПРОБЛЕМЫ РАЗРАБОТКИ ЧАСТНОЙ ПОЛИТИКИ МЕНЕДЖМЕНТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Приоритетные задачи при решении проблем, формирования частной политики менеджмента инцидентов информационной безопасности (ЧПМИИБ) связаны с детализацией процедур управления ИИБ и построением формализованной модели менеджмента инцидентов ИБ. Для описания процедуры менеджмента ИИБ используется классическая модель непрерывного улучшения процессов – модель PDCA. Для формального представления ЧПМИИБ выбран комплексный подход, предусматривающий решение следующих задач: обнаружение, информирование и учет инцидентов информационной безопасности; реагирование на инциденты информационной безопасности, применение необходимых средств для предотвращения, уменьшения и восстановления нанесенного ущерба; анализ произошедших инцидентов с целью планирования превентивных мер защиты и улучшения процесса обеспечения информационной безопасности в целом. Формализованная модель представляется в теоретико-множественной и логической формах. Предлагаемая формализованная модель ЧПМИИБ не предупреждает нанесение ущерба компании, однако ее реализация на предприятии позволит повысить эффективность существующей системы защиты и снизить на предприятии вероятность повторения нанесения ущерба.

Инцидент; информационная безопасность; частная политика менеджмента; модель; формализация; комплексный подход; процедуры управления.

E.A. Maksimova, T.A. Omelchenko, V.V. Alekseenko

PROBLEMS OF PRIVATE POLICY OF INFORMATION SECURITY OF ENTERPRISE INCIDENTS MANAGEMENT DEVELOPMENT

Priority tasks in solving the problems associated with the formation of a private policy management of information security incidents (PPMISI) are associated with detailed management procedures of ISI and construction of a formalized model of management of information security incidents. To describe the management procedures ISI uses the classical model of continuous process improvement – model PDCA. For a formal presentation PPMISI chosen an integrated approach, which provides solution of following tasks: detection, information and accounting information security incidents; responding to information security incidents, the use of the necessary means to prevent, reduce and recover damages; analysis of incidents in order to plan preventive measures to protect and improve the process of information security in general. Formalized model is represented in the set-theoretic and logical forms. The proposed formalized model PPMISI does not prevent damage to the company, but its implementation in the company will increase the efficiency of the existing system of protection and reduce the likelihood of recurrence in the company of damage.

Incident; information security; private policy; management model; formalization; a comprehensive approach; management procedures.

Информация сегодня – это один из главных ресурсов, обеспечивающих конкурентоспособность предприятия, что и актуализирует вопросы ее защиты. При этом, слабые места в системе защиты информации могут привести к финансовым потерям, нанести ущерб коммерческим операциям и, в целом, вывести предприятие из «рыночной борьбы». Таким образом, первоочередная стратегическая зада-

ча на современном предприятии – создание эффективной системы защиты информации, одна из функций которой связана с возможностью управления возникающими в системе инцидентами информационной безопасности (ИИБ).

Согласно ГОСТ Р 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», «инцидент информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ». Их последствиями могут быть такие события, как несанкционированное раскрытие или изменение информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. Инциденты ИБ, о которых не было сообщено, но которые были определены как инциденты, расследовать невозможно и защитных мер для предотвращения повторного появления этих инцидентов применить нельзя. Не смотря на это, предположение о том, что в организации произошёл ИИБ, в соответствии должно базироваться на трёх основных факторах:

- сообщение об ИИБ поступают одновременно из нескольких источников (пользователи, IDS, журнальные файлы);
- IDS сигнализируют о множественном повторяющемся событии;
- анализ журнальных файлов автоматизированной системы даёт основание для вывода системным администраторам о возможности наступления события инцидента.

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» менеджмент информационной безопасности предприятия – «скоординированные действия по руководству и управлению предприятием в части обеспечения ее ИБ в соответствии с изменяющимися условиями внутренней и внешней среды предприятия». Согласно данного ГОСТа предприятие должно определить политику менеджмента информационной безопасности предприятия на основе характеристик бизнеса, организации, ее размещения, активов и технологий, которая:

1) содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере ИБ;
2) принимает во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности;
3) согласуется со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться менеджмент информационной безопасности;
4) устанавливает критерии оценки рисков;
5) утверждается руководством организации.

Система менеджмента ИБ на предприятии представляется в форме частной политики менеджмента ИИБ (ЧПМИИБ) предприятия, которая определяется как политика менеджмента инцидентов информационной безопасности на данном конкретном предприятии, направленная на нейтрализацию внешних и внутренних угроз и осуществляющаяся с учетом характера деятельности компании, и основных факторов, формирующих общие условия текущего развития предприятия.

При этом, для эффективной реализации ЧПМИИБ, на предприятии должны быть разработаны, внедрены, обеспечены в функциональном плане и введены в эксплуатацию системы мониторинга, поддержки и непрерывного сопровождения документированной системы менеджмента информационной безопасности применительно ко всей деловой деятельности предприятия и рискам, с которыми оно сталкивается.

Для получения результативной ЧПМИИБ после необходимого планирования следует выполнить ряд подготовительных действий, предусмотренных процедурами частной политики и включающих в себя:

1) формулирование и разработку политики менеджмента инцидентов ИБ, а также получение от высшего руководства утверждения этой политики;

2) разработку и документирование подробной системы менеджмента инцидентов ИБ. Согласно ГОСТ Р 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», документация системы менеджмента инцидентов ИБ должна содержать шкалу серьезности для классификации инцидентов ИБ и формы докладов о событиях и инцидентах ИБ, соответствующие документированные процедуры и действия, связанные со ссылками на нормальные процедуры использования данных и системы, сервисов и(или) сетевого резервирования, планами обеспечения непрерывности бизнеса;

3) ведение мониторинга потока входящих, выходящих или находящихся в атакованной системе, сервисе и (или) сети данных;

4) элементы активации нормальных дублирующих процедур и действий по планированию непрерывности бизнеса согласно политике безопасности системы, сервиса и (или) сети;

5) ведение мониторинга и организация защищенного хранения свидетельств в электронном виде на случай их востребования для судебного разбирательства или дисциплинарного расследования внутри организации;

6) передачу подробностей об инциденте ИБ сотрудникам своей организации и сторонним лицам или организациям;

7) тестирование функционирования системы менеджмента инцидентов ИБ, ее процессов и процедур;

8) обновление политик менеджмента и анализа рисков ИБ, корпоративной политики ИБ, специальных политик ИБ для систем, сервисов и (или) сетей для включения ссылок на менеджмент инцидентов ИБ и обеспечение регулярного пересмотра этих политик в контексте выходных данных системы менеджмента инцидентов ИБ;

9) фиксирование группы реагирования на инциденты ИБ (ГРИИБ) с соответствующей программой обучения ее персонала;

10) технические и другие средства поддержки системы менеджмента инцидентов безопасности ИБ (и деятельности ГРИИБ);

11) проектирование и разработку программы обеспечения осведомленности о менеджменте инцидентов ИБ, ознакомление с этой программой всего персонала организации.

На основании ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» частная политика должна устанавливать общие руководящие принципы мониторинга состояния информационной безопасности и использовать результаты для осуществления менеджмента инцидентов ИБ предприятия. Она должна распространяться на все технологические процессы предприятия, и является обязательной для выполнения всеми работниками предприятия. Мероприятия по обеспечению ИБ предприятия, которые будут выполнять и реализовывать требования данной частной политики, утверждаются внутренними нормативными документами в соответствии с установленным на предприятии порядком.

Обозначенные положения являются основой для неформального описания частной политики менеджмента инцидентов информационной безопасности предприятия. Для формального представления ЧПМИИБ, на наш взгляд, необходимо использовать комплексный подход, предусматривающий решение следующих задач:

1) обнаружение, информирование и учет инцидентов информационной безопасности;
2) реагирование на инциденты информационной безопасности, применение необходимых средств для предотвращения, уменьшения и восстановления нанесенного ущерба;
3) анализ произошедших инцидентов с целью планирования превентивных мер защиты и улучшения процесса обеспечения информационной безопасности в целом.

Считаем, что приоритетным при решении проблем, связанных с формированием ЧПМИИБ, является разработка:

1) модели менеджмента инцидентов ИБ;
2) процедур управления ИИБ.

Для описания процедуры менеджмента инцидентов информационной безопасности (рис. 1) воспользуемся классической моделью непрерывного улучшения процессов PDCA (Планируй – Plan, Выполняй – Do, Проверяй – Check, Действуй – Act), которая согласно ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», может быть применена при структурировании всех процессов системы менеджмента информационной безопасности.

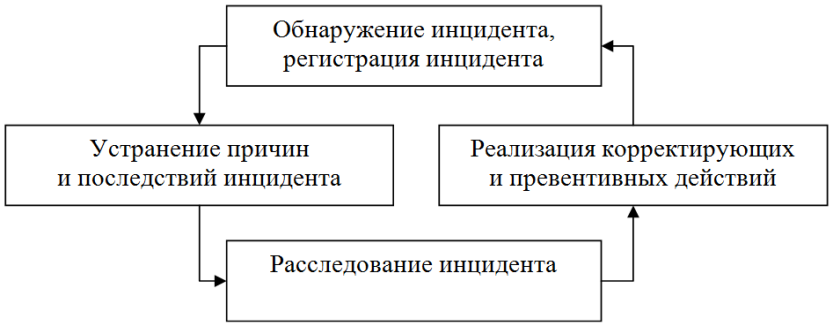

Рис. 1. Процедуры менеджмента инцидентов информационной безопасности

Воспользуемся данной моделью для описания процедур управления ИИБ.

В качестве составляющих этапов реализации модели управления инцидентами информационной безопасности определим следующие процедуры.

Этап управления ИИБ Е1: «Обнаружение инцидента, регистрация инцидента».

Процедура 1.1: «Реагирование пользователя на инциденты ИБ» (в соответствии с рабочей инструкцией).

Процедура 1.2: «Реагирование специалиста на инциденты ИБ» (в соответствии с рабочей инструкцией).

Этап управления ИИБ Е2: «Устранение причин и последствий инцидента».

Процедура 2.1: «Анализ общих предпринимаемых действий».

Процедура 2.2: «Составление диагностической матрицы».

Процедура 2.3: «Определение уровня приоритета инцидента».

Процедура 2.4: «Определение сроков устранения инцидента».

Этап управления ИИБ Е3: «Расследование инцидента».

Процедура 3.1. «Сбор доказательств и улик инцидент».

Процедура 3.2. «Определение виновных в возникновении инцидента».

Процедура 3.3. «Определение соответствующих дисциплинарных взысканий».

Этап управления ИИБ Е4: «Реализация корректирующих и превентивных действий».

Процедура 4.1. «Проведение мероприятий по предотвращению повторного возникновения инцидента».

В качестве базовой основы для содержательной реализации этапов можно воспользоваться: на этапе E1 – [1, 2], на этапе E2 – [3, 4, 5] , на этапе E3 – [4], на этапе E4 – [5, 6].

Необходимо отметить, что для эффективной реализации процедур управления ИИБ необходимо через определенное время (как правило, через полгода или год) пересматривать базу инцидентов, форму отчета и пр., внедрять обновленную процедуру в информационную систему, проверять ее функционирование и реализовать превентивные действия.

Для формализации модели управления ИИБ выполним детализацию этапов управления ИИБ (табл. 1).

Таблица 1

Формализованная детализация этапов управления инцидентами информационной безопасности

Этап	Элементы	Выполняемые действия
$E_{1:}$	Множество инструкций реагирования пользователя на инциденты ИБ $I_п (f_1, f_2, \ldots f_n)$. Множество инструкций реагирования специалиста на инциденты ИБ $I_c (\varphi_1, \varphi_2, \ldots \varphi_m)$	Реакция пользователя на инциденты ИБ $R_п=(Vf_i)$. Реакция специалиста на инциденты ИБ $R_c=(V\ \varphi_j)$
E2	Множество предпринимаемых действий $D(d_1, d_2,\ldots,d_n)$. Множество признаков инцидентов {PRIZNAKinc}. Множество типов инцидентов {TIPinc}. Параметры: t – предположительное время устранения инцидента; T – фактическое время устранения инцидента	Составление диагностической матрицы A({PRIZNAKinc},{TIPinc}). Определение уровня приоритета инцидента: PRIZNAKinc(i) ⋀ TIPinc(j) → Uinc, где Uinc$\{u_1, u_2, u_3\}$: u_1 – низкий; u_2 – средний; u_3 – высокий уровни приоритета инцидента. Определение сроков устранения инцидента T^*
E3	Множество доказательств и улик наличия инцидента $S(s_1, s_2,\ldots,s_n)$	Определение виновных в возникновении инцидента $Vin(v_1, v_2, \ldots , v_n)$. Определение соответствующих дисциплинарных взысканий $DV(dv_1, dv_2, \ldots , dv_n)$
E4	Множество мероприятий по предотвращению повторного возникновения инцидента: $M(m_1, m_2, \ldots, m_n)$.	Проведение мероприятий по предотвращению повторного возникновения инцидента

Таким образом, формализованная модель управления ИИБ имеет следующую логическую структуру

$$E=E(E1,E2,E3,E4): (E1\rightarrow(E2/\backslash E3))\rightarrow E4,$$

где все компоненты управляющей функции имеют следующие теоретико-множественные и логические структуры:

$$E1=E1(\{R_п\}, \{R_c\}) =E1(R_п(f_1, f_2, \ldots f_n),R_c(\varphi_1, \varphi_2, \ldots \varphi_m))$$

или

$$E1: ((\vee f_i)/\backslash(\vee\varphi_j))\backslash/((\ \vee f_i) \vee (\backslash/\varphi_j\ ));$$

$$E2=E2(A(\{PRIZNAKinc\},\{TIPinc\}),t,T)=E2(Uinc,T^{*}),$$

где

$$PRIZNAKinc(i) \wedge TIPinc(j) \rightarrow Uinc;\ \ Uinc\{u_1, u_2, u_3\};$$

$$E3=E3(\{S\},\{Vin\},\{DV\})=$$

$$=E3(S(s_1, s_2,\ldots,s_n), Vin(v_1, v_2, \ldots, v_n), DV(dv_1, dv_2, \ldots, dv_n))$$

или

$$E3: S\rightarrow(Vin/\backslash DV);$$

$$E4: S\rightarrow M, \text{ где } S(s_1, s_2,\ldots,s_n), M(m_1, m_2, \ldots, m_k).$$

Таким образом, на каждом этапе модели формируются соответствующие элементы, и выполняется определенный набор действий общей формализации.

Выводы. Для эффективной реализации частной политики менеджмента ИИБ, все этапы модели PDCA должны иметь непрерывный и системный характер. Предлагаемая формализованная модель ЧПМИИБ не предупреждает нанесение ущерба компании (как правило, компания уже понесла ущерб, связанный с инцидентом). Однако ее реализация на предприятиях позволит повысить эффективность существующей системы защиты и снизить вероятность повторения нанесения ущерба. При этом статистику инцидентов следует регулярно анализировать в рамках аудита системы управления информационной безопасностью, так как она представляет особую ценность для компании как показатель эффективности функционирования системы управления информационной безопасностью в целом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Никишова А.В.* Архитектура типовой информационной системы для задачи обнаружения атак // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 104-109.
2. *Никишова А.В.* Анализ источников сведений о состоянии сервера для задачи обнаружения атак // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: Материалы Всероссийской науч.-практ. конф., г. Волгоград, 27 апреля 2012г. – В.: Изд-во ВолГУ, 2012. – С. 165-167.
3. *Аткина В.С.* Система анализа катастрофоустойчивости // Известия Томского политехнического университета. Управление, вычислительная техника и информатика. – 2013. – Т. 322, № 5. – С 117-120.
4. *Аткина В.С.* Оценка эффективности катастрофоустойчивых решений // Вестник Волгоградского государственного университета. Сер. 10. "Инновационная деятельность". Научно-теоретический журнал. – 2012. – Вып. 6. – С. 89-92.
5. *Максимова Е.А., Корнева В.А.* Оптимизация технологии безопасного информационного взаимодействия в корпоративных системах // Материалы XII Международной научно-прак-тической конференции «ИБ-2012». Ч. II. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 124-129.
6. *Максимова Е.А., Корнева В.А.* Формализация действий злоумышленника при прогнозировании вторжений в корпоративную информационную систему // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: Материалы II Всерос. научн.-практ. конф., г. Волгоград, 26 апр. 2013 г. – Волгоград: Изд-во ВолГУ, 2013. – С. 71-78.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Максимова Елена Александровна – Волгоградский государственный университет; e-mail: Maksimova@volsu.ru; 400062, г. Волгоград, пр. Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; к.т.н.; доцент.

Омельченко Татьяна Александровна – e-mail: omelchenkotanya@mail.ru; кафедра информационной безопасности; студентка.

Алексеенко Валерий Владимирович – e-mail: infsec@volsu.ru; кафедра информационной безопасности; аспирант.

Maksimova Elena Aleksandrovna – Volgograd State University; e-mail: Maksimova@volsu.ru; 100, Universitetsky pr. Volgograd, 400062, Russia; phone: +78442460368; the department of informational security; cand. of eng. sc.; associate professor.

Omelchenko Tatyana Aleksandrovna – e-mail: omelchenkotanya@mail.ru; the department of informational security; student.

Alekseenko Valerii Vladimirovich – e-mail: infsec@volsu.ru; the department of informational security; postgraduate student.

УДК 004.056.5, 004.89

А.М. Цыбулин, В.А. Балдаев, А.А. Бешта

АУТСОРСИНГ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Российские компании стали использовать аутсорсинг с целью отказаться от непрофильных активов и сконцентрироваться на основном направлении своего бизнеса. При реализации своих услуг компания аутсорсер получает доступ к ресурсам и компонентам информационной системы, что приводит к изменению уровня угроз безопасности информации, уменьшаются и совсем исчезают одни риски и появляются новые риски. Актуальными проблемами являются своевременная идентификация, оценка и минимизация старых и новых рисков, а также автоматизация этих процессов. Проводится анализ услуг аутсорсинга, строится дерево угроз информационной системе при аутсорсинге и рассчитывается остаточный риск. Для обеспечения безопасности ИС при передаче ее на аутсорсинг проводятся работы по минимизации рисков: подготовка ИС к передаче на аутсорсинг, оценка уровня информационной безопасности в процессе и после аутсорсинга, а в случае снижения уровня, проведение работы по восстановлению уровня информационной безопасности. Предлагаются модель и алгоритмы по оценке и минимизации рисков при аутсорсинге на основе данных мониторинга, аудита, инвентаризации программного и аппаратного обеспечения. Разработан программный комплекс, который позволяет автоматизировать процесс минимизации рисков.

Аутсорсинг; аутсорсер дерево угроз; инсайдерская деятельность; информационная безопасность; инвентаризация; мониторинг; остаточный риск.

A.M. Tsybulin, V.A. Baldaev, A.A. Beshta

OUTSOURCE AND INFORMATION SECURITY

The Russian companies began to use outsourcing in order to abandon non-core assets focus on the general direction of their business. When implementing its services company - outsourcer gets access to resources and components of the information system, which leads to change of a level of information security threats, reduce and completely disappear, some risks and new risks are emerging. The actual problems are timely identification, assessment and minimization of old and new risks, as well as the automation of these processes. Outsourcing services are analyzed, a tree of threats to the information system in outsourcing is built, and residual risk is calculated. To ensure the security of information system when sending it to outsourcing a number of works to reduce the risks is carried out. It is proposed to include in this work: preparation of information system to the outsourcing, assessing the level of information security during and after outsourcing, and in the case of level reduce carrying out repair work. Algorithms are proposed for the assessment and minimizing risks during outsourcing based on monitoring data, inventory of hardware and software. The program complex, which allows to automate the process of minimizing the risks is developed.

Outsourcing; outsourcer; tree of threats; insider activity; information security; inventory; monitoring; the residual risk.

В связи с постоянным усложнением информационных систем компаний и ростом потребности в них, найти квалифицированный ИТ-персонал становится всё сложнее, да и сам персонал постоянно дорожает. Для разрешения этой проблемы всё