Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 10, Is. 4, pp. 158-164, 2016

DOI: 10.13187/vesp.2016.10.158
www.ejournal21.com

UDC 004.056.53

The Information Security Incident Management

Natalya S. Ralnikova [a, *], Xenia A. Kudryavtseva [a]

[a] ITMO University, Russian Federation

Abstract

This article is devoted to a question of management of incidents of information security – one of the most important procedures of management of information security in the organizations. The authors reviewed the domestic and international standards in the management of information security incidents, defined the concept of the incident, and as a result, the entire incident management process with a detailed description of each of the stages.

Keywords: incident information security incident management, incident management, information security management.

1. Введение

Существует большое количество примеров, когда после возникновения инцидентов безопасности, организации теряли важные данные, тратили немалые суммы на ликвидацию последствий инцидентов, и после этого много времени тратили на восстановление репутации и материального ущерба, а также реанимировали взаимоотношения с партнерами и клиентами. Безусловно, все эти обстоятельства отрицательно влияют на бизнес-деятельность компании.

Для своевременной идентификации инцидента и минимизации нанесенного им ущерба необходимо иметь четкий, спланированный и эффективный процесс управления инцидентами информационной безопасности. Для этого вначале необходимо определить стандарты, которыми следует руководствоваться, и на их основе построить план процесса управления инцидентами ИБ.

Система управления инцидентами ИБ является одной из главных задач системы управления ИБ в организации.

2. Материалы и методы

Основным источником для написания данной статьи стали международные и российские стандарты в области менеджмента информационной безопасности и менеджмента инцидентов информационной безопасности в частности, а также последние работы специалистов в области управления информационной безопасностью.

* Corresponding author
E-mail addresses: natalya.ralnikova@gmail.com (N.S. Ralnikova), kudriavtseva.ksyu@yandex.ru (X.A. Kudryavtseva)

Методологическую основу данного исследования составили логические приемы, определения, описания, анализа и синтеза. Также использован общенаучный метод анализа.

3. Обсуждение

Для наиболее эффективной разработки процессов управления инцидентами ИБ необходимо руководствоваться требованиями международных и российских стандартов. К настоящему времени разработано достаточное количество нормативных документов, регламентирующих вопросы управления инцидентами ИБ.

Международный стандарт ISO\IEC 27001-2005 и его отечественный аналог ГОСТ Р ИСО/МЭК 27001:2006 дает общие рекомендации к построению системы управления ИБ и к процессам управления инцидентами, в частности. Здесь речь идет о необходимости создания системы управления инцидентами и документации, необходимой для ее регулирования (ГОСТ Р ИСО/МЭК 27001-2006).

В рамках отечественного стандарта ГОСТ Р ИСО/МЭК 18044-2007 процесс управления инцидентами представляется в виде циклической модели PDCA. Модель состоит из этапов планирования, эксплуатации, анализа и улучшения процесса. Также здесь приводятся требования по сопроводительной документации (ГОСТ Р ИСО/МЭК ТО 18044-2007).

Нормативный документ США NIST SP 800-61 является собранием «лучших практик» по построению процессов управления инцидентами ИБ и реагирования на них. Здесь рассматриваются вопросы реагирования на такие инциденты как атаки «отказ в обслуживании», распространение вредоносного программного обеспечения, несанкционированный доступ, нерегламентированное использование и распределенные атаки (США NIST SP).

Международный стандарт ISO/IEC 27035:2011 предлагает организованный подход к выявлению инцидентов, их оценке и к управлению инцидентами в целом, в том числе совершенствованию данного процесса (ISO/IEC...).

Таким образом, на сегодняшний день существует большое количество стандартов, дающих рекомендации и инструкции к построению системы управления инцидентами в организации, которыми стоит воспользоваться при планировании и построении системы управления инцидентами ИБ (Зосимовская).

Для того, чтобы строить процесс управления инцидентами ИБ необходимо определить, что именно понимается под инцидентом. Для начала определим понятие события ИБ. В ГОСТ Р ИСО/МЭК 27001:2006 дается следующее определение события ИБ: «Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью». В этом же стандарте инцидент в системе защиты информации определяется как «инцидент информационной безопасности: любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность» (ГОСТ Р ИСО/МЭК 27001-2006). В ГОСТ Р ИСО/МЭК 18044-2007 дается следующее определение: «Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ» (ГОСТ Р ИСО/МЭК ТО 18044-2007).

Итак, в качестве вывода определим главные характеристики инцидента:

- это событие;
- происходит угроза или нарушение ИБ;
- неблагоприятные последствия (Рыженкова);

Основные виды инцидентов информационной безопасности, согласно ГОСТ Р ИСО/МЭК 27001:2006:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;

• сбои программного обеспечения и отказы технических средств;
• нарушение правил доступа (ГОСТ Р ИСО/МЭК 27001-2006).

4. Результаты

Система управления инцидентами ИБ (СУИИБ) – часть общей системы управления организации, предназначенная для обнаружения и регистрации, оценки, классификации и приоритезации, всестороннего исследования, обработки, извлечения уроков и предотвращения инцидентов ИБ в дальнейшем и включающая организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области реагирования на инциденты ИБ (Милославская и др., 2014).

Задачами СУИИБ являются:

• выявление и регистрация инцидентов, в том числе оповещение о них;
• предупреждение инцидентов, реагирование на инциденты, восстановление или уменьшение последствий после возникновения инцидента;
• анализ произошедших инцидентов с целью улучшения системы управления инцидентами.

Построение процесса управления инцидентами – задача далеко не тривиальная, поэтому нередко организации обращаются в специализированные компании за помощью в построении СУИББ. Опытным специалистам не составит труда организовать процесс управления инцидентами для любого предприятия с учетом его специфики.

В соответствии со стандартом ГОСТ Р ИСО/МЭК 18044-2007 управления инцидентами ИБ делится на 4 основных этапа:

• планирование и подготовка;
• использование;
• анализ;
• улучшение.

Рассмотрим каждый из этапов подробнее.

1. Этап планирования и подготовки процесса управления инцидентами.

Эффективное управление инцидентами ИБ требует надлежащего планирования и подготовки. Для того чтобы реакция на инциденты была эффективной на данном этапе проводят следующие мероприятия:

• разработка, документирование и обновление политики управления инцидентами ИБ, а также ее поддержка со стороны высшего руководства, включая утверждения им данной политики;
• разработка и документирование системы управления инцидентами ИБ (формы, процедуры и инструменты поддержки для обнаружения, оповещения, оценки и реагирования на инциденты ИБ, а также градация шкалы серьезности инцидентов ИБ);
• проектирование и разработка программы обеспечения осведомленности об управлении инцидентами ИБ;
• создание в организации группы по расследованию инцидентов ИБ – ГРИББ) с соответствующей обучающей программой для персонала, с установленными обязанностями и ответственностью персонала, способного адекватно реагировать на все известные типы инцидентов ИБ;
• ознакомление всего персонала организации посредством инструктажей или иными способами о существовании СУИИБ;
• тестирование СУИИБ (Милославская и др., 2014).

2. Этап использования системы управления инцидентами ИБ.

На данном этапе проходят следующие мероприятия:

• обнаружение событий ИБ и оповещение (информирование) о них;
• оценка и принятие решения, является ли данное событие инцидентом ИБ;
• реагирование на инцидент ИБ и ликвидация его последствий.

Обнаружение событий ИБ может производится непосредственно людьми, заметившими что-либо подозрительное, охранной сигнализацией, детекторами дыма или огня, межсетевыми экранами, антивирусными программами, системами обнаружения вторжений и т.д. После выявления события сообщение о нем передается ответственным за

прием событий ИБ сотрудникам, которые должны произвести оценку, является ли данное событие инцидентом или нет. Оценка производится на основе полученных сведений о событии ИБ и экспертного мнения, принявшего сообщение специалиста. Также инциденту присваивают тип (инцидент физической безопасности, программно-технический инцидент и т. д.) и степень серьезности.

Далее информация об инциденте ИБ поступает сотрудникам, ответственным за устранение инцидента в соответствии с его типом. В ходе реагирования производится непосредственное разрешение и закрытие инцидента ИБ.

Инциденты ИБ самой низшей степени опасности обычно не требуют немедленного реагирования и все необходимые действия выполняются, в большинстве случаев, одним специалистом и нет необходимости сбора ГРИИБ для реагирования на него. При регистрации инцидента ИБ высшей степени опасности для реагирования на него необходим сбор ГРИИБ. Помимо этого, производится информирование собственников активов и руководителей организации, отвечающих за бизнес-процессы, вовлеченные в инцидент ИБ (Милославская и др., 2014).

Операция по устранению последствий инцидента информационной безопасности должна оформляться согласно внутреннему регламенту и непосредственно зависит от особенности работы информационной системы организации и типа инцидента. Работа персонала во время процесса ликвидации последствий инцидента должна быть согласована как с техническими специалистами, которые осуществляют поддержку системы, так и с руководством подразделений, чья информация стала объектом злоумышленника (Романовский, ч. 3).

Инциденты ИБ самой низшей степени опасности, обычно, не требуют немедленного реагирования и все необходимые действия выполняются, в большинстве случаев, одним специалистом и нет необходимости сбора ГРИИБ для реагирования на него. При регистрации инцидента ИБ высшей степени опасности для реагирования на него необходим сбор ГРИИБ. Помимо этого, производится информирование собственников активов и руководителей организации, отвечающих за бизнес-процессы, вовлеченные в инцидент ИБ (Милославская и др., 2014).

Операция по устранению последствий инцидента информационной безопасности обязана быть оформлена в виде внутреннего регламента и непосредственно зависит от особенности работы информационной системы организации и типа инцидента. Работа персонала во время процесса ликвидации последствий инцидента должна быть согласована как с техническими специалистами, которые осуществляют поддержку системы, так и с руководством подразделений, чья информация стала объектом злоумышленника (Романовский, ч. 3).

3. Анализ процесса управления инцидентами ИБ.

После разрешения инцидента ИБ руководитель ГРИИБ анализируют все произошедшее с целью оценки и определения степени результативности реагирования на инцидент ИБ. На основе полученных результатов делаются выводы и составляются рекомендации по улучшению процессов ИБ в целом и управления инцидентами ИБ в частности.

На данном этапе проводится также расследование инцидента, которое включает в себя идентификацию нарушителя и сбор и анализ свидетельств инцидента, необходимых для получение законных оснований для привлечения к ответственности нарушителя за умышленное или непреднамеренное действие или попытку действия, направленную на нанесение ущерба организации. В крупных компаниях, как правило, выделяют комиссию по расследованию инцидентов информационной безопасности (Куканова).

Для облегчения процесса расследования и анализа инцидентов необходимо вести журнал расследований, который может включать в себя следующие пункты:

- описание инцидента;
- статус расследования;
- действия, производимые командой реагирования при реагировании на инцидент;
- лица, задействованные в расследовании инцидента, и их роли;
- свидетельства и улики;
- комментарии участников расследования инцидента.

В ходе расследования инцидента все свидетельства должны быть защищены от дискредитации, поскольку данные могут содержать информацию о действенных уязвимостях информационной системы (Романовский, ч. 2).

4. Совершенствование процесса управления инцидентами ИБ

На этапе совершенствования исполняются рекомендации, разработанные на предыдущем этапе. Здесь могут проводиться следующие мероприятия:

1) На основе имеющихся рекомендаций внедрение улучшений в систему информационной безопасности организации, а именно введение новых мер защиты или совершенствование старых. Это могут быть технические, физические, программно-аппаратные или организационные меры. Здесь также происходит обновление соответствующей документации, вплоть до политики безопасности организации. Также необходимо обновление материала для проведения инструктажей с целью информирования об изменениях в системе защиты.

2) Введение улучшение в СУИИБ и изменение соответствующей документации. Изменения в системе управления инцидентами должны быть тщательно протестированы перед их применением на практике (Милославская и др., 2014).

5. Заключение

Управление инцидентами – это основа безопасности организации. Без системы управления инцидентами невозможно эффективное функционирование системы управления информационной безопасности. Правильно спланированная и спроектированная с учетом специфики организации система управления инцидентами позволит не только адекватно и своевременно выявлять инциденты безопасности, но и оперативно на них реагировать, уменьшая ущерб, который мог быть нанесен. Кроме того, результаты анализа инцидентов и собранная на их базе статистика позволяют совершенствовать систему безопасности на предприятии и принимать в будущем все более точные решения.

Примечания

ISO/IEC... – ISO/IEC 27035:2011. Information technology. Security techniques. Information security incident management. Введен – 01.09.2011.

ГОСТ Р ИСО/МЭК 27001-2006 – ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введен 27.12.2006.

ГОСТ Р ИСО/МЭК ТО 18044-2007 – ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Введен 27.12.2007.

Зосимовская – Зосимовская Н. Информационная безопасность: управление инцидентами [Электронный ресурс]. Режим доступа: http://iso27000.ru/chitalnyi-zai/upravlenie-incidentami-informacionnoi-bezopasnosti/informacionnaya-bezopasnost-upravlenie-incidentami, свободный.

Куканова – Куканова Н. Управление инцидентами информационной безопасности [Электронный ресурс]. Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-incidentami-informacionnoi-bezopasnosti/upravlenie-incidentami-informacionnoi-bezopasnosti, свободный.

Милославская и др., 2014 – *Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* (2014). Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. 2-е изд., испр. Москва: Горячая линия-Телеком, 170 с. Серия «Вопросы управления информационной безопасностью. Выпуск 3».

Романовский, ч. 2 – Романовский С. Обработка инцидентов информационной безопасности. Часть 2 [Электронный ресурс]. Режим доступа: http://iso27000.ru/chitalnyi-zai/upravlenie-incidentami-informacionnoi-bezopasnosti/obrabotka-incidentov-informacionnoi-bezopasnosti-chast-2, свободный.

Романовский, ч. 3 – Романовский С. Обработка инцидентов информационной безопасности. Часть 3 [Электронный ресурс]. Режим доступа: http://iso27000.ru/chitalnyi-

zai/upravlenie-incidentami-informacionnoi-bezopasnosti/obrabotka-incidentov-informacionnoi-bezopasnosti-chast-3, свободный.

Рыженкова – Рыженкова А. Управление инцидентами информационной безопасности: о чем говорят стандарты [Электронный ресурс]. Режим доступа: http://www.elvis.ru/upload/iblock/5d0/Rizenkova_connect7-8_SOC.pdf, свободный.

США NIST SP – США NIST SP 800-61. Revision 2. Computer Security Incident Handling Guide. Введен 08.2012.

References

ISO/IEC... – ISO/IEC 27035:2011. Information technology. Security techniques. Information security incident management. Vveden – 01.09.2011.

GOST R ISO/MEK 27001-2006 – GOST R ISO/MEK 27001-2006. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoi bezopasnosti. Trebovaniya. Vveden 27.12.2006.

GOST R ISO/MEK TO 18044-2007 – GOST R ISO/MEK TO 18044-2007. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment intsidentov informatsionnoi bezopasnosti. Vveden 27.12.2007.

Zosimovskaya – Zosimovskaya N. Informatsionnaya bezopasnost': upravlenie intsidentami [Elektronnyi resurs]. Rezhim dostupa: http://iso27000.ru/chitalnyi-zai/upravlenie-incidentami-informacionnoi-bezopasnosti/informacionnaya-bezopasnost-upravlenie-incidentami, svobodnyi.

Kukanova – Kukanova N. Upravlenie intsidentami informatsionnoi bezopasnosti [Elektronnyi resurs]. Rezhim dostupa: http://www.iso27000.ru/chitalnyi-zai/upravlenie-incidentami-informacionnoi-bezopasnosti/upravlenie-incidentami-informacionnoi-bezopasnosti, svobodnyi.

Miloslavskaya i dr., 2014 – *Miloslavskaya N.G., Senatorov M.Yu., Tolstoi A.I.* (2014). Upravlenie intsidentami informatsionnoi bezopasnosti i nepreryvnost'yu biznesa. Uchebnoe posobie dlya vuzov. 2-e izd., ispr. Moskva: Goryachaya liniya-Telekom, 170 s. Seriya «Voprosy upravleniya informatsionnoi bezopasnost'yu. Vypusk 3».

Romanovskii, ch. 2 – Romanovskii S. Obrabotka intsidentov informatsionnoi bezopasnosti. Chast' 2 [Elektronnyi resurs]. Rezhim dostupa: http://iso27000.ru/chitalnyi-zai/upravlenie-incidentami-informacionnoi-bezopasnosti/obrabotka-incidentov-informacionnoi-bezopasnosti-chast-2, svobodnyi.

Romanovskii, ch. 3 – Romanovskii S. Obrabotka intsidentov informatsionnoi bezopasnosti. Chast' 3 [Elektronnyi resurs]. Rezhim dostupa: http://iso27000.ru/chitalnyi-zai/upravlenie-incidentami-informacionnoi-bezopasnosti/obrabotka-incidentov-informacionnoi-bezopasnosti-chast-3, svobodnyi.

Ryzhenkova – Ryzhenkova A. Upravlenie intsidentami informatsionnoi bezopasnosti: o chem govoryat standarty [Elektronnyi resurs]. Rezhim dostupa: http://www.elvis.ru/upload/iblock/5d0/Rizenkova_connect7-8_SOC.pdf, svobodnyi.

SShA NIST SR – SShA NIST SR 800-61. Revision 2. Computer Security Incident Handling Guide. Vveden 08.2012.

УДК 004.056.53

Управление инцидентами информационной безопасности

Наталья Сергеевна Ральникова [a, *], Ксения Александровна Кудрявцева [a]

Университет ИТМО, Российская Федерация

[*] Корреспондирующий автор
Адреса электронной почты: natalya.ralnikova@gmail.com (Н.С. Ральникова), kudriavtseva.ksyu@yandex.ru (К.А. Кудрявцева)

Аннотация. Данная статья посвящена вопросу управления инцидентами информационной безопасности – одной из важнейших процедур управления информационной безопасностью в организации. Авторами рассмотрены отечественные и международные стандарты в области управления инцидентами информационной безопасности, определено понятие инцидента, и в качестве результата приведен весь процесс управления инцидентами с подробным описанием каждого из этапов.

Ключевые слова: инцидент информационной безопасности, менеджмент инцидентов, система управления инцидентами, управление информационной безопасностью.