Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2019, 2: 143–147

DOI 10.26163/GIEF.2019.14.76.023
УДК 338.054.23

A.A. Grafov, V.A. Mordovets

MINIMIZATION OF DETRIMENT TO ECONOMIC ACTOR THROUGH INFORMATION SECURITY INCIDENTS MANAGEMENT

Aleksandr Grafov – Senior Lecturer, the Department of Economic Security, Saint-Petersburg State University of Economics, PhD in Economics, Saint-Petersburg; **e-mail: grafov_aa@mail.ru**.
Vitaly Mordovets – Senior Lecturer, the Department of Economic Security, St. Petersburg State University of Economics, PhD in Economics, Associate Professor, St. Petersburg; **e-mail: mordovets@mail.ru**.

The article focuses on relevant matters covering information security incidents management within a business entity in the global economy digitalization environment. It provides analysis of the definition, specifics and practical experience of investigating information security incidents. The authors offer a general approach to process analysis with regard to information security incidents.

***Keywords**: information security; economic security; intruder; investigation.*

А.А. Графов, В.А. Мордовец

МИНИМИЗАЦИЯ УЩЕРБА ХОЗЯЙСТВУЮЩЕМУ СУБЪЕКТУ ПУТЁМ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Александрович Графов – доцент кафедры экономической безопасности, ФГБОУ ВО «Санкт-Петербургский государственный экономический университет», кандидат экономических наук, г. Санкт-Петербург; **e-mail: grafov_aa@mail.ru**.
Виталий Анатольевич Мордовец – доцент кафедры экономической безопасности ФГБОУ ВО «Санкт-Петербургский государственный экономический университет», кандидат экономических наук, г. Санкт-Петербург; **e-mail: mordovets@mail.ru**.

В статье рассматриваются вопросы управления инцидентами информационной безопасности хозяйствующего субъекта в условиях глобальной цифровизации экономики. Анализируются определение, особенности и опыт расследования инцидентов информационной безопасности. Предлагается общий подход к анализу процессов инцидентов информационной безопасности.

***Ключевые слова:** информационная безопасность; экономическая безопасность; злоумышленник; расследование.*

Управление инцидентами информационной безопасности (далее – ИИБ) является неотъемлемой частью системы управления информационной безопасностью (далее – ИБ) любого хозяйствующего субъекта, обладающего ценными (чувствительными к утрате) информационными ресурсами. По данным всероссийского опроса IT-компаний, проведенного центром НАФИ в ноябре 2017 года, средний размер убытков организации составил 299 940 рублей, при этом сумма ущерба зависит от масштабов предприятия. В исследовании говорится, что в РФ потери от цифровых атак оцениваются в 115 967 204 788 рублей [4].

Инциденты ИБ могут быть целенаправленными или случайными (самой

частой причиной является в данном случае человеческий фактор). В общей своей массе инциденты можно сгруппировать по причине их появления на две группы: на внешние (спровоцированные извне – злоумышленником разной степени квалификации и мотивации) и внутренние (явившиеся следствием неосторожности или халатности сотрудников компании). Но и для внешних, и для внутренних инцидентов можно дать общее определение, цель, задачи и методы управления ими.

В общем случае **инцидент информационной безопасности** (ИИБ) – это единичное, нежелательное и/или неожиданное событие ИБ (а также совокупность этих событий), которое может скомпрометировать бизнес-процессы организации или угрожает ее ИБ (ISO/IECTR 18044:2004).

Стандарт ISO 27001:2005 указывает на необходимость разработки процесса менеджмента ИИБ, что говорит об актуальности указанной проблемы. Обычно данный процесс разрабатывается в рамках общей системы управления информационной безопасностью и содержится в модели непрерывного улучшения процедур, получившей название – модель PDCA (Plan ->Do->Check ->Act) (см. рис. 1).

Международный стандарт ISO 27001 рекомендует модель PDCA как базу функционирования процедур системы менеджмента ИБ [2].

На сегодняшний день в мире разработано немало нормативно-методических документов, описывающих вопросы управления ИИБ (ISO/IEC 17799:2000, ISO/IEC 27001:2005 и др.). Стандартом Банка РФ СТО БР ИББС 1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» заявлено, что мониторинг событий и инцидентов информационной безопасности используется в целях обеспечения защиты данных на высшем уровне в качестве исполнительной меры, а управление событиями информационной безопасности, полученными во время мониторинга, помогает избегать стагнации и обеспечить минимально допустимый уровень безопасности ценной информации [3]

Расследование ИИБ преследует несколько основных **целей** [1]:

- локализация и ликвидация последствий ИИБ;
- установление виновных лиц и их мотивации, сбор доказательной базы для привлечения таких лиц к ответственности;
- анализ ИИБ и принятие превентивных мер.

В первом приближении в большинстве компаний процесс управления ИИБ может быть построен следующим образом [3]:

- получение сигнала об инциденте;
- получение доп. информации об ИИБ;
- анализ ситуации, локализация ИИБ и срочное применение контрмер;
- установление слабых мест в системе

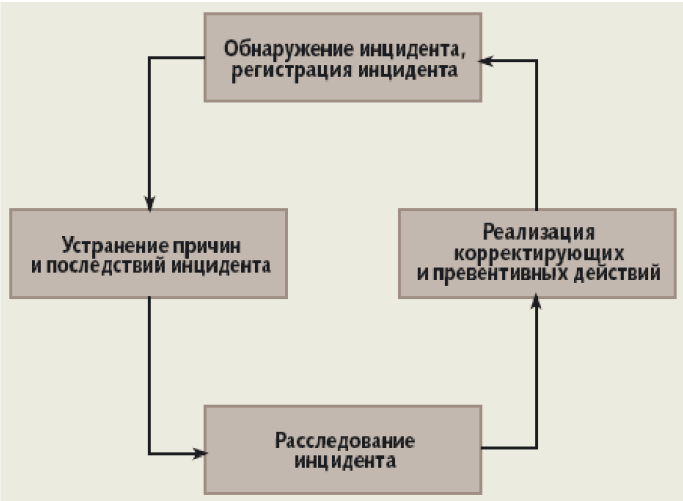

Рис. 1. Модель PDCA

защиты организации, по которым была реализована угроза, определение круга ответственных;

- проведение корректирующих и профилактических процедур;

- разработка рекомендаций по принятию мер по минимизации в дальнейшем угроз ИБ;

- архивация и обеспечение целостности материалов расследования.

На сегодняшний день разработан и внедрён на практике порядок действий сотрудников отделов организаций, принимающих участие в расследовании инцидента нарушения режима ИБ, которого придерживаются авторы данного исследования:

- получение информации об ИИБ;

- проверка полученной информации;

- принятие экстренных мер (например, срочное отключение питания сервера, подвергнутого атаке злоумышленником);

- разработка приказа о создании группы по расследованию инцидента, её выезд на объект;

- сбор информации ИИБ на месте;

- разработка доказательной базы, изъятие жёстких дисков и журналов записей операционных систем, разработка акта;

- анализ полученной информации и разработка отчетных форм для сотрудника, принимающего административные решения;

- определение степени вины персонала и оценка ущерба, нанесённого хозяйствующему субъекту.

Несмотря на выше сказанное, процесс расследования ИИБ является сложно формализуемой задачей, потому что зависит от особенностей работы каждого хозяйствующего субъекта: сложности структуры управления, среднесписочной численности сотрудников, объёмов продаж и числа контактов с деловыми партнёрами, частоты проверок компании регуляторами и т.д. Однако изучив опыт разных компаний, имеющих в своей структуре отдел обеспечения информационной безопасности, можно постараться определить единый подход к ее решению. Схематично процесс расследования ИИБ можно описать на рис. 2.

События от технических (программно-аппаратных) систем обеспечения информационной безопасности являются важным поставщиком сведений о процессах, происходящих в управляющей системе, об угрозах и рисках. Большое развитие получили системы обнаружения и предотвращения вторжений (IDS, IPS) встраиваемые в современные межсетевые экраны (МЭ), применяемые для обнаружения сетевых атак, эксплойтов и рут-китов;

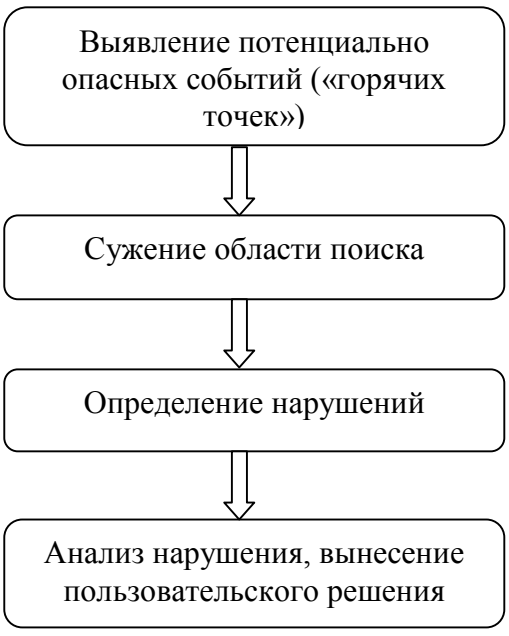

Рис. 2. Процесс расследования инцидента информационной безопасности
Источник: [2].

системы предотвращения утечек по каналам передачи данных (DLP); различные программно-аппаратные средства и комплексы, контролирующие состояние ЛВС, информационные потоки от различных источников событий и действия пользователей (SIEM). Современные тенденции развития средств обеспечения ИБ демонстрируют переход от узкоспециализированных программных продуктов к комплексам, решающим сразу ряд задач по обеспечению ИБ (например, межсетевые экраны с модулями IPS), что значительно повышает эффективность получения данных об ИИБ и состоянии системы защиты информации в общем виде.

Если говорить о стоимости и экономической целесообразности применения в организациях указанных выше программных средств и программно-аппаратных комплексов, то в этом вопросе хозяйствующий субъект любого масштаба и бюджета может подобрать себе оптимальную конфигурацию. Рынок указанных выше средств очень объёмен, конкуренция между фирмами-производителями (как отечественными, так и зарубежными) – высока, кроме того, всегда есть возможность приобрести подержанное оборудование или взять его в аренду у компании-партнёра. В этом случае стоимость оборудования будет дешевле в 2–3 раза, пусть и не оформленная в собственность. В начале статьи мы упоминали, что размер ущерба в результате реализации одной утечки информации на предприятии составляет в среднем примерно 60 тысяч рублей. Для сравнения – стоимость одного нового промышленного МЭ компании Cisco линейки ASA550X варьируется на отечественном рынке от 40 до 50 тысяч рублей.

Таким образом, главными задачами, решаемыми с помощью аппаратных средств и систем реагирования на ИИБ, могут быть [3]:

- внедрение системы централизованного сбора, анализа и хранения (логирования) событий из множества распределённых источников таких событий;
- мониторинг атак, попыток НСД и нарушений политик ИБ;
- контроль устройств ввода/вывода информации, BIOS;
- контроль за действиями персонала;
- предоставление средств для целей реализации расследований инцидентов, формирования базы доказательств по ним.

Анализ полученных данных включает исследование т.н. «логов» различных устройств и систем, сообщений ИБ, просмотр состояния портов, журналов загрузки операционных систем, программ, протоколов, писем электронной почты и прикрепленных файлов, установленных приложений и т.д., в результате чего подтверждается или опровергается факт возникновения ИИБ.

В процессе анализа осуществляется категоризация и приоритезация ИИБ путём определения степени критичности рассматриваемой информации степени критичности воздействия на неё. Полученные данные подвергаются корреляции и выводятся на консоль офицера ИБ или сетевого администратора, назначенного приказом директора хозяйствующего субъекта ответственным за обеспечения той или иной системы информационных ресурсов (например, информационной системы персональных данных клиентов организации).

По технологии PDCA следующим этапом проводятся корректирующие действия, оценивается текущий уровень защиты, даётся оценка эффективности системы обеспечения информационной безопасности. Лишь обладая полным и исчерпывающим набором данных, можно провести расследование ИИБ на должном уровне, получить представление о состоянии системы экономической безопасности организации в целом. Важно, чтобы ни один инцидент не остался без внимания, чтобы было проведено расследование, выявлены виновники и, это главное, выполнены корректирующие и профилактические действия. Ведь доведение до общественности факта появления на предприятии инцидента ИБ, который привёл к утечке конфиденциальной информации, и не был расследован должным образом,

может повлечь за собой как финансовый, так и репутационный ущерб хозяйствующего субъекта и дальнейшую утечку данных из организации.

ЛИТЕРАТУРА

1. *Гарбузов Г.* Проведение расследований инцидентов ИБ: организационные и правовые аспект // Информационная безопасность: [сайт]. URL: http://information-security.ru/articles2/control/provedenie-rassledovaniy-incidentov-ib (дата обращения: 18.01.2019).

2. Методика проведения расследований. URL: https://www.infowatch.ru/sites/default/files/partners_docs/infowatch_traffic_monitor_enterprise_3_5_metodika_provedeniya_rassledovaniy.pdf (дата обращения: 17.01.2019).

3. *Писаренко И.* Выявление инцидентов информационной безопасности // Информационная безопасность: [сайт]. URL: http://lib.itsec.ru/articles2/control/vyyavlenie-incidentov-informacionnoy-bezopasnosti (дата обращения: 18.01.2019).

4. Потери организаций от киберпреступности // Tadviser: [сайт]. URL: http://www.tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности (дата обращения: 17.01.2019).