общей экономической целесообразности этого подход относительно предыдущих имеет свои ограничения в виде дефицита квалифицированных кадров. Вопросы кадрового голода на рынке ИБ поднимаются чуть ли не на каждой конференции, поэтому остается лишь признать тот факт, что реализацию этого подхода могут позволить себе лишь единицы из числа самых привлекательных работодателей.

Таким образом, на любом выбранном пути по противодействию профессиональному злоумышленнику компании потребуются существенные инвестиции, и компания может выбрать для себя только наиболее комфортную статью расходов: дорогостоящие технологии, которые позволят после долгой докрутки автоматизировать часть работы, вложения в экспертизу специалистов для попытки выявления атак на существующих инструментах или инвестиции в процессы компании, когда проблемы кибербезопасности разделяются и руководством, и ИТ подразделением, и обычными пользователями. В любом из вариантов, в том числе промежуточном — это долгий и тяжелый путь. Но в любом случае стоять долго на месте, как витязь у камня, нельзя, потому что актуальность и критичность проблемы обеспечения кибербезопасности объяснять уже не нужно.

Список литературы

1. *Abdul B. Subhani.* Stay Safe! AbbottPress. 2016. 182 с.
2. *Дрозд А.* Обзор SIEM-систем на мировом и российском рынке. https://www.anti-malware.ru/

Дрюков Владимир Викторович *– директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар». Http:// rt-solar.ru*

DOI: 10.25728/avtprom.2020.07.02

Анализ методики аудита информационной безопасности предприятия с помощью аутсорсинговых компаний

А.А. Басырова, И.И. Лившиц (Университет ИТМО)

Раскрывается понятие аудита информационной безопасности, выполняемого с помощью компаний, оказывающих услуги аутсорсинга (ИБ-аутсорсинг). Представлен анализ существующих методик, а также состояние и тенденции развития современного рынка ИБ-аутсорсинг в РФ и за рубежом. Определено, что целью ИБ-аутсорсинга в современной ИТ-индустрии является сокращение финансовых затрат, применение новой концепции оценки защищенности и снижение времени проведения аудита системы менеджмента информационной безопасности.

Предложено к задачам ИБ-аутсорсинга относить обеспечение защиты конфиденциальной информации, а также прогнозирование рисков ИБ в соответствии с существующими практиками. Это позволит принимать обоснованные управленческие решения на основе объективных отчетов, оперативно выявлять схемы мошенничества, содействовать эффективному выполнению требований регуляторов по обеспечению безопасности объектов критичной инфраструктуры. Важным также представляется обеспечение возможности повышения эффективности контроля использования рабочего времени, исходя из анализа настроения в коллективе. Новизна работы заключается в разработке метода ИБ-аутсорсинга и предоставлении доказательств эффективности (как экономической выгоды) привлечения аудиторских компаний, занимающихся аудитом ИБ.

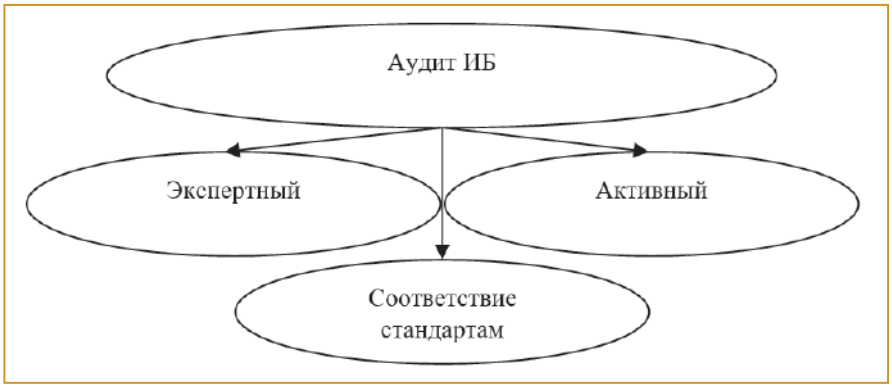
Ключевые слова: аудит, информационная безопасность, аутсорсинг, методики, уровень защищенности, система менеджмента информационной безопасности, информационные технологии.

Введение

Аутсорсинг аудита информационной безопасности (ИБ-аутсорсинг) — это процесс выполнения внешней оценки степени защищенности ИТ-сервисов компании с выдачей экспертных рекомендаций и минимизация рисков утечки конфиденциальных данных. Сегодня с помощью ИБ-аутсорсинга у многих компаний появляется возможность получить полную и объективную оценку степени защищенности собственных ИТ-сервисов, оперативно обнаруживать уязвимые места в бизнес-процессах, а также разработать план по улучшению системы менеджмента информационной безопасности (СМИБ). По этим причинам тема ИБ-аутсорсинга является устойчивым трендом отечественных и зарубежных компаний. Данный вид аудита затрагивает все области СМИБ, например, сюда можно отнести такие виды активов, как сетевая инфраструктура, операционные системы, системы визуализации, системы управления базами данных, средства защиты информации и критические процессы [1].

Преимущество ИБ-аутсорсинга состоит в том, что с его помощью решается проблема отсутствия возможности у компании собрать в своем штате достаточное число высококвалифицированных специалистов в области ИБ и ИТ. Решив эту проблему, компания смо-

жет не ограничиваться существующим уровнем ИБ, а обеспечить планомерное повышение степени защищенности собственных ИТ-сервисов. Второй причиной обращения к аутсорсингу является экономическая сторона проблемы, например, с ежегодным ростом стоимости затрат на поддержание СМИБ сегодня все чаще возникает вопрос о том, каким образом можно сэкономить на этой статье расходов. Третьим преимуществом является возможность использования новейших технологий защиты информации, оценки степени соответствия новым применимым требованиям регуляторов, в том числе для обеспечения безопасности объектов критической информационной инфраструктуры (КИИ) без существенных затрат [2].



Методы проведения аудита ИБ

История развития аутсорсинга ИБ

Рынок ИБ-аутсорсинга развивался в качестве финансового инструмента, позволяющего сократить затраты на персонал, путем обращения к сторонним организациям за квалифицированными сотрудниками. Спустя некоторое время услуги аутсорсинговых служб стали применять для разделения труда. Здесь главной идеей было то, что бизнесу следует концентрироваться на развитии собственного продукта, а вопросы, связанные с ИТ-технологиями, можно отдать в руки сторонних специалистов. Первыми услугами аутсорсинговых компаний начали пользоваться зарубежные фирмы, приходящие на отечественный рынок, но начиная с 2006 г. данной функцией заинтересовались и российские организации. Вплоть до 2014 г. многих интересовало лишь сокращение финансовых издержек за счет аутсорсинга, но сейчас ключевым приоритетом компаний является повышение качества получаемых услуг, нежели экономическая выгода.

Изначально компании, специализирующиеся на услугах ИБ-аутсорсинга, назывались Managed Security Service Providers (MSSP). В их сферу деятельности входило управление межсетевыми экранами, управление системами обнаружения вторжения (COB/IDS), управление SIEM-системами (Security Information and Event Management), управление системами аутентификации и авторизации. Но с увеличением спроса на подобные функции появилось такое понятие, как Security Operations Center (SOC). Это совокупность специалистов, процессов и технологий, направленных на обнаружение угроз информационной безопасности и реагирование на них. В SOC теперь входит MSS (Manager Security Services), направленный на выявление простых и средних массовых угроз, и MDR (Manager Detectionand Response), предназначенный для обнаружения продвинутых целевых атак [3].

Методология проведения аудита

При проведении аудита принято обращаться к международным и отечественным стандартам ИТ-аудита. К ним относятся такие нормативные документы и лучшие практики проведения аудита в области ИТ, как BSI/IT Baseline Protection Manual[1], ISO/IEC 27001:2005, Международный стандарт по аудиту ISO 27006 и 27007, Международный стандарт ISO 15408 «Общие критерии», методология COBIT (Control Objectives for Information and related Technology) и др. При этом такие стандарты позволяют охватить только ключевые моменты проведения аудита, а для реализации дополнительных и специфических задач могут быть использованы узконаправленные стандарты [4].

Поскольку до сих пор не существует единого документа, описывающего требования проведения аудита ИБ, аутсорсинговые организации самостоятельно выделили три метода аудита. К таким методам принято относить активный аудит, аудит на соответствие стандартам и экспертный аудит (рисунок) [5].

Общее описание рассматриваемых методов

Активный аудит

Данный метод является одним из самых распространенных видов аудита. Обнаружению подлежит подозрительная активность компонентов информационной системы (ИС), начиная от действий пользователей, заканчивая инцидентами программных системам и аппаратных устройств. Анализ ИС здесь проводится с точки зрения злоумышленника, обладающего высокой осведомленностью в области ИТ. Технология активного аудита состоит в сборе информации о состоянии системы защиты с использованием специального программного обеспечения и различных методов воздействия. В этом случае на систему производится большое число сетевых атак с учетом того, что хакер изначально обладает лишь тем минимумом информации, который он получил из открытых источников. Спектр производимых атак на ИС

[1] BSI/IT Baseline Protection Manual - стандарт "Руководство по обеспечению безопасности ИТ" (Германия).

напрямую зависит от квалификации аудитора, что еще раз подтверждает факт того, что обращение к специализированным аутсорсинговым компаниям позволит получить большее число уязвимостей системы за счет высокой компетенции специалистов.

Активный аудит делится на два типа: внешний и внутренний. Отличие состоит в том, что атаки моделируются извне и изнутри соответственно. Внутренний активный аудит по составу работ аналогичен внешнему. По результатам активного аудита заказчик получает рекомендации по модернизации системы защиты, которые описывают опасные уязвимости. За счет этих рекомендаций появляется возможность повышения уровня защищенности системы и снижения затрат на обеспечение информационной безопасности путем конкретно прописанных средств и мер. Активный аудит требует периодичности минимум раз в полгода, поскольку возможности современных злоумышленников постоянно совершенствуются.

Аудит на соответствие стандартам

История возникновения этого метода переплетается с аудитом в финансовой сфере, так как именно в нем необходимо проводить сравнение состояния дел в организации с неким абстрактным описанием, приводимым в стандартах. В результате проведения аудита на соответствие стандартам заказчик получает отчет с указанием степени соответствия ИС современным стандартам и внутренним требованиям компании, рекомендации по модернизации системы обеспечения ИБ.

Экспертный аудит

Суть метода заключается в сравнение текущего состояния информационной безопасности с неким «идеальным» описанием системы безопасности, полученным из мировых и частных практик аудитора. Здесь обращение к аутсорсинговым компаниям играет выигрышную роль, так как приоритетом таких компаний является получение и изучение различного опыта проведения аудита по всему миру.

Экспертный аудит является самым объемным, поскольку в него входит большой фронт работ, сюда относится и интервьюирования заказчика касательно требований, предъявляемым к системе, и анализ информационных потоков организации, и разбор организационно-распорядительной документации на объекте, и опрос сотрудников. По результатам экспертного аудита делается довольно большой отчет, содержащий предложения по модернизации топологии сети и технологий обработки информации, варианты замены и установки новых средств защиты информации, предложения по изменению пакета документов, ориентировочные затраты на создание или совершенствование системы обеспечения ИБ (включая техническую поддержку и обучение персонала) [6].

Разработка нового метода аудита

Как показывает практика, наилучшим методом проведения ИБ-аудита является комплекс всех перечисленных выше методик. В составе общепринятого комплексного аудита безопасности присутствует активный аудит, подразумевающий осуществление инструментального анализа защищенности, экспертный аудит, в ходе которого выявляются недостатки в системе мер защиты информации и оценочный аудит, проверяющий соответствие стандартам и руководящим документам. С течением времени комплексный подход, состоящий из трех элементов, начинает себя исчерпывать и требовать изменений. Поэтому в данной статье предлагается дополнить комплексный метод проведения ИБ-аудита еще двумя составляющими [7].

Одним из дополнений является технический аудит, позволяющий подготовить и проанализировать информацию, а также выдать заключение по работе отдельного элемента инфраструктуры ИС. Технический аудит проводится довольно быстро, так как не требует большого объема работ, но с его помощью появится возможность оптимизировать работу определенного элемента информационной системы. Под инфраструктурой подразумеваются технические средства (серверы, центры обработки данных и пр.), средства связи (глобальные и локальные сети, маршрутизаторы и т. д.) и системное программное обеспечение (операционные системы и пр.). Одним из примеров совершенствования инфраструктуры может быть процесс улучшения производительности ERP (системы управления ресурсами предприятия).

Следующим дополнением является аудит критерия информационных технологий. Суть этого дополнения состоит в анализе информации и выдаче рекомендаций по какому-то определенному критерию ИТ (целостность, производительность, безопасность и пр.). Здесь важно проверять совокупность программных и аппаратных средств, а также процесс их сопровождения и обслуживания в компании. Рассмотрим в качестве примера проверку сервера на удовлетворение критериям ИТ. Необходимый перечень критериев берем из стандартов ГОСТ Р ИСО 13335-1 или ГОСТ Р ИСО 27001. Следующим этапов является оценка, которая подразумевает внешний пен-тест, проверку компетенции персонала, анализ плана аварийных мероприятий и пр.

Крупные отечественные компании, предоставляющие услуги ИБ-аутсорсинга ИБ

Ниже будут перечислены компании, преимуществом которых является то, что заказчик напрямую не связан с внедрением, он лишь оставляет заявку, а компания-исполнитель разворачивает защитный программный комплекс в месте, удобном для заказчика. Здесь подразумевается возможность разворота программного комплекса как на мощностях клиента, так и в облаке исполнителя. Помимо этого, некоторые аутсорсинговые компании предлагают поставку собственного оборудования (сетевые сканеры и пр.) и программных средств. Вторым преимуще-

Таблица. Ведущие компании, занимающиеся аутсорсингом ИБ

Компания	Крупные промышленные предприятия-заказчики
Газинформсервис	– Различные подконтрольные организации ПАО «Газпром» (глобальная энергетическая компания); – ГК «Норникель» и пр.
Инфосистемы Джет	– Различные подконтрольные организации ПАО «Газпром» – Мосэнергосбыт; – Лукойл и пр.
АМПЕЛ-СЕРВИС	– «РАО Энергетические системы Востока»; – буровая компания «Евразия»; – «НК Роснефть» и пр.
ACT (Advanced System Technology)	– Santa Fe; – General Electric
Ростелеком SOLAR JSOC	– «НК Роснефть» – ГК «Калашников» и пр.

ством является повышение качества управление ИТ-инфраструктурой, так как работу будут осуществлять опытные специалисты. Это позволяет снизить финансовые затраты и сократить время решения косвенных проблем. В-третьих, снижается или вовсе исключается расход средств на поиск профильных специалистов, так как аутсорсинговая компания предоставит своих квалифицированных сотрудников. В-четвертых, ресурсы компании-заказчика полностью направляются на решение основных задач бизнеса.

На данный момент к услугам аутсорсинга обращаются крупные компании из разных областей. Сюда относятся такие отрасли, как: государственные структуры, наука и образование, нефтегазовая индустрия и энергетика, промышленность и транспорт, телекоммуникация, торговля, финансы и страхование. С конкретным списком фирм-заказчиков можно ознакомиться на официальных сайтах компаний-аутсорсеров (таблица).

Сроки и стоимость проведения ИБ-аудита рассчитываются индивидуально для каждой компании. В среднем проведение комплексного аудита занимает 5 рабочих дней, а стоимость услуги начинается от 30 тыс. руб. [8].

Заключение

В статье кратко описана история развития ИБ-аудита и рассмотрены три основных подхода к проведению ИБ-аудита, а также перечислены основные лидеры в данной области. Показано преимущество

Суть бизнеса заключается не в соблюдении формальностей, поиске выгоды, практическом результате, получении прибыли, стремлении продать, коммерческой игре или чём-то ещё. Бизнес – это, прежде всего, то, что вам не безразлично.

Ричард Брэнсон (британский предприниматель)

нового метода, заключающегося в дополнение классического комплексного подхода двумя составляющими, актуальными на сегодняшний день. Данный метод может быть применим для компаний, нуждающихся в анализе существующей информационной системы, так как с его помощью можно провести более качественный аудит ИБ.

Список литературы

1. *Аверченков В.И.* Аудит информационной безопасности [Электронный ресурс]: Уч. пособие. 3-е изд., стер. М.: ФЛИНТА. 2016 . 269 с. https://rucont.ru/efd/246516.
2. *Лонцих П.А., Лившиц И.И., Никифорова К., Лонцих Н.П., Дролова Е.Ю., Карасев С.Н., Карасева В.А.* Оптимизация программы аудитов информационной безопасности // Качество. Инновации. Образование. 2017. № 2 (141). – С. 48-58.
3. Аутсорсинг ИБ: взгляд внутрь // SecurityLab.ru 2016г. URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/321141.php.
4. *Серова А.Г.* Анализ теоретических основ и программных средств аудита системы управления информационной безопасностью // Социально-экономические и естественно-научные парадигмы современности. 2018. С. 829-837.
5. *Лившиц И.И.* Методика формирования численных метрик ИБ (Обзор) // Вопросы защиты информации. 2016. № 3 (114). С. 54-64.
6. *Иванченко В.В.* Аудит информационных технологий // Вестник МФЮА. 2015. №1. URL: https://cyberleninka.ru/article/n/audit-informatsionnyh-tehnologiy.
7. *Лившиц И.И.* Практические аспекты аудита информационной безопасности в соответствии с требованиями стандартов СТО БР ИББС (Точка зрения) // Деньги и кредит. 2016. № 2. С. 54-58.
8. Аутсорсинг ИБ — краткий обзор рынка // АМ Медиа. 2014. http://anti-malware.ru/analytics/Market_Analysis/Outsourcing_Information_Security_overview_of_the_market.

Басырова Альбина Альмировна *– университет ИТМО,*
Лившиц Илья Иосифович *– д-р техн. наук, университет ИТМО.*
Контактный телефон +7 (921) 934-48-46.
E-mail: E-mail: albinnaabas@mail.ru Livshitz.il@yandex.ru