УДК 004.056.55 **Ткаченко В.В., Карпенко С.В., Гнатюк С.А., Артеменко Т.М.**

"ДОРОЖНАЯ КАРТА" СПЕЦИАЛИСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вступление. Большинство специалистов по информационной безопасности (ИБ) наверняка посещали профильные мероприятия (семинары, конференции) и сайты компаний, которые позиционируют себя как консультанты, аудиторы и поставщики оборудования и услуг в сфере защиты информации (ЗИ). Условно их можно разделить на две большие группы – иностранные компании (или их представительства) и локальные украинские компании. Это вовсе не означает, что украинские компании занимаются только отечественными решениями в сфере ИБ. Большинство из них предлагают, в основном, зарубежные решения по ИБ. Данная классификация не говорит ни хорошо, ни плохо о той или иной компании. Отличия между отечественными и иностранными игроками заключаются лишь в подходах к реализации проектов, уровне подготовки персонала, правовых вопросах и ценовой политике. **Целью данной работы** является анализ решений по ИБ с точки зрения специалиста по ИБ предприятия, а также анализ основных этапов внедрения мероприятий по безопасности в области информационных технологий (ИТ).

Поставщики решений на рынке ИБ Украины. Довольно часто персонал украинских компаний имеет квалификацию не ниже, а иногда и выше, чем иностранные специалисты, знаком с местным законодательством и реальными проблемами заказчиков. Ценовая политика у украинских компаний немного гибче, чем у иностранных коллег, так как последние находятся, как правило, в определенных корпоративных рамках в вопросах формирования цены. Вполне естественно, что и подходы к реализации проектов в украинских компаниях более приближены к "боевым" условиям ведения бизнеса на Украине. Если большинство вышеописанных различий далеко неочевидно, то основным следует считать, что все украинские компании, работающие более или менее серьезно на рынке ИБ, являются лицензиатами Государственной Службы специальной связи и защиты информации Украины (ГССЗЗИ) [1] либо в сфере технической ЗИ, либо в области криптографической ЗИ, либо имеют лицензии на оба вида деятельности. Таким образом, одним из основных критериев при подборе компании для реализации проекта по ИБ можно считать наличие лицензии на деятельность в сфере ЗИ, выданной ГССЗЗИ Украины. Это дает определенную гарантию заказчику, что компания имеет специалистов и оборудование для проведения работ в сфере ИБ надлежащим образом. Более корректно разделить поставщиков решений и услуг по другим признакам. А именно, по их позиционированию на рынке. Хотя достаточно сложно на сегодняшний день провести четкие границы, все же попытаемся "отделить зерна от плевел".

На сегодняшний день ситуация складывается для специалиста по ИБ примерно таким образом: 1. Предлагается некий продукт или набор продуктов (реже комплексное решение), который устраняет конкретную проблему (или совокупность проблем) в ИБ предприятия. 2. Далее проводится тендер по закупке продукта и выбирается его поставщик. 3. В зависимости от сложности и цены продукта (это влияет на наличие его на складе) заказчик должен подождать от 2 недель до 2 месяцев пока продукт придет в Украину, пройдет таможенную очистку, сертифицируется по УкрСЕПРО [2], или, как средство криптографической защиты в ГССЗЗИ, и попадет на площадку заказчика. 4. Компания поставщик предложит установить и настроить продукт (за дополнительные деньги), что, как правило, еще от 2 недель до месяца. 5. Компания поставщик обучит специалистов по ИБ и ИТ заказчика приемам использования продукта (еще 1-2 недели). 6. Продукт начинает выполнять возложенные на него функции (с момента процедуры закупки до внедрения прошло 3 месяца).

За это время либо угроза изменила свой характер, либо возникли новые, либо сменилась стратегия у руководства компании или, что еще хуже, продукт не учитывает бизнес-процессов компании и рядовой персонал постарается обходиться без его использования. Таким образом, имеется дорогая игрушка, которая либо не выполняет свои функции, либо работает не на полную мощность.

Вернемся к классификации компаний на рынке безопасности. Целесообразно выделить такие *виды компаний в области ИБ* (рис.1) [3]: разработчики продуктов (программных и аппаратных); системные интеграторы решений по ИБ; дистрибьюторы продуктов ИБ; консультанты по ИБ; аудиторы в сфере ИБ; компании, предоставляющие тренинги по ИБ; страховые компании в сфере ИБ; масс-медиа и информационные ресурсы в сфере ИБ. Каждый вид можно рассмотреть еще детальней, но верхушка айсберга примерно такова. Еще раз необходимо подчеркнуть, что большинство компаний стараются объединять эти функции, поэтому разделение достаточно условно. Кроме приведенных ниже участников, на рынок воздействуют регуляторы (ГССЗЗИ Украины, НБУ, НКРС) и общественные или негосударственные объединения.

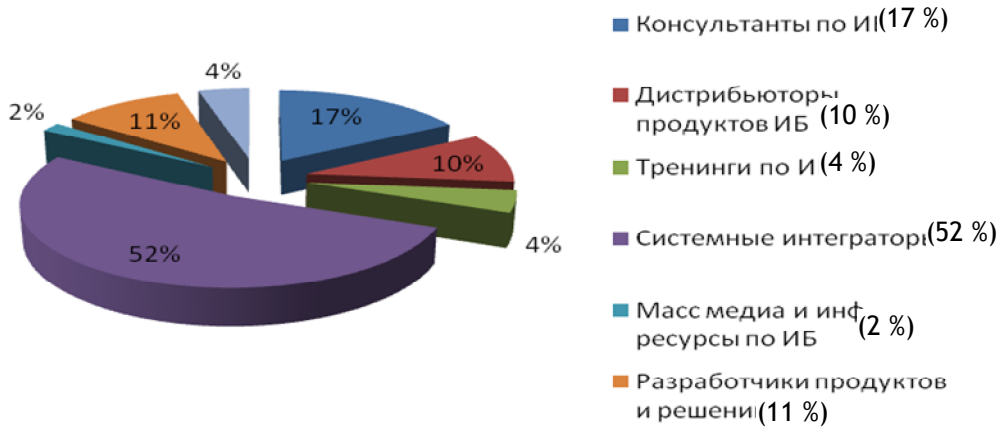


Рис. 1. Классификация поставщиков услуг и решений по ИБ в Украине

Сложно не заметить, что на диаграмме отсутствуют страховые компании. Дело в том, что в Украине отсутствует правовая база для классификации инцидентов ИБ, и нет четкого определения страхового случая по событию ИБ. Страхуются лишь отдельные виды рисков, косвенно влияющие на ИБ (стихийные бедствия и риски по качеству услуг и продуктов по ИБ). Таким образом, на сегодняшний день в Украине невозможно застраховать риски, связанные с технологическими ошибками (в том числе при реализации проектов), кибер-риски (уничтожение, искажение или повреждение данных, включая невозможность защитить их конфиденциальность, неспособность защитить от несанкционированного доступа (НСД), использования, заражения вирусами, отказов в обслуживании и потерь прибыли). В отличие от Украины, в Европе и США такие риски страхуют и достаточно давно.

Рассмотрим каждую группу компаний более детально. Как видно из. рис.1, большинство компаний занимается системной интеграцией в области ИБ (52%) и консалтингом в сфере ИБ (17%). Порядка 11% производят продукты и решения, которые впоследствии остальные 79% (интеграторы, дистрибьюторы и консультанты) реализовывают заказчикам. Оставшиеся 10% занимаются обучением специалистов, рекламой в сфере ИБ и аудитом информационных систем.

Очевидно, что *производители продуктов* являются одними из основных столпов индустрии. В основной массе это представительства российских и других зарубежных компаний, которые производят антивирусное программное обеспечение (ПО), средства защиты от НСД, средства криптографической защиты, ПО и оборудование для защиты периметра сети, оборудование для защиты от утечек конфиденциальной информации и др.

Постараемся описать, чем занимается *системный интегратор*. В идеале компания-интегратор анализирует ИТ инфраструктуру заказчика и предлагает комплекс технических решений по выявленным брешам в системе безопасности. Далее специалисты интегратора подбирают набор оборудования и/или ПО для решения задач по ИБ, устанавливают и настраивают его для работы в конкретной среде. Как правило, персонал заказчика обучается приемам эксплуатации оборудования и ПО и реакции на проблемы.

Консультанты по ИБ анализируют бизнес-процессы заказчика и взаимодействие систем в инфраструктуре, помогают организовать процессы управления ИБ и предлагают наиболее оптимальные варианты внедрения тех или иных решений предложенных системным

интегратором. Кроме этого, консультанты могут участвовать при внедрении продуктов и решений по ИБ в качестве экспертов и необходимы для оптимизации структуры ИТ и ИБ под реальные бизнес-требования заказчика.

Дистрибьюторы продуктов и решений в идеале являются связующим звеном между разработчиками и интеграторами. Их основная задача поддержка системного интегратора, в том числе консультантами при внедрении проекта. Иногда консалтинговые компании также пользуются услугами дистрибьюторов для непосредственной продажи заказчику ПО или оборудования, которое необходимо для реализации проекта по ИБ. Но в идеальной ситуации дистрибьюторы не взаимодействуют напрямую с заказчиком, они являются своего рода универсальным складом для интеграторов и консультантов, которые в силу специфики того или иного проекта не могут содержать на складе все варианты дорогостоящего оборудования или ПО.

Компании, занимающиеся тренингами по ИБ, рассматривают их как дополнительные услуги к основному пакету (обычно тренинги по ИТ, консалтинг в сфере ИТ и т.п.). В основном полезны тренинги по организации отдельных аспектов системы управления ИБ или связанные с конфигурацией безопасности каких-то базовых платформ (операционных систем или систем управления базами данных). Тренинги по конкретным продуктам желательно все-таки получать из первых рук, т.е. компаний интеграторов.

Аудиторские компании по ИБ в основном представлены представителями крупных зарубежных аудиторов с известными именами (т.н. Big4 [4]) и несколькими украинскими компаниями. Большинство интеграторов и консалтинговых компаний также предлагают услуги аудита ИБ, но объективность такого аудита вызывает закономерные вопросы. Как правило, аудит ИБ специалисты рассматривают только под углом этического хакинга (тестов на проникновение в систему) или сканирования на уязвимости. Однако это представление в корне неверно. Под аудитом ИБ понимается анализ текущего состояния бизнес-процессов компании, с точки зрения их соответствия задекларированным правилам, безопасности, порядку выполнения, соответствия законодательным требованиям и полезности для предприятия. При анализе рассматриваются ИТ системы (ПО и ресурсы), вовлеченные в процесс. Аудит ИТ (ИБ) опирается на процесс управления рисками, т.е. информационный актив с более высоким уровнем риска проверяется более интенсивно и чаще, чем информационные активы с меньшими рисками. В результате аудита менеджмент предприятия получает текущую картину по ИБ с рекомендациями по улучшению ситуации.

Масс-медиа и информационные ресурсы - естественный сегмент для рекламы на рынке ИБ. Обычно данный сегмент представлен специализированными периодическими изданиями (журналы, бюллетени) и компаниями, фокусирующимися на PR (организуют выставки, конференции и семинары).

Таким образом, приблизительная картина к кому и в каких случаях вам следует обращаться налицо. Если точно знаете, что вам нужно (например, 100 антивирусов на рабочие станции) – к дистрибьютору. Знаете приблизительно – к консультантам. Уже знаете и готовы внедрять комплексное решение – к системным интеграторам. Но весьма желательно перед началом проекта и после его окончания провести аудит и получить независимую оценку текущей ситуации. Перед внедрением проекта, чтобы сравнить ваши ожидания, заключение аудиторов и коммерческое предложение интеграторов. Кроме того, есть возможность проводить аудит аутсорсинговых компаний, на предмет соблюдения ими обязательств перед вами, в том числе по защите вашей коммерческой тайны.

Что предлагают поставщики решений? Постараемся нарисовать карту услуг и решений по ИБ почти на все случаи жизни (или жизненного цикла вашей информационной системы). И понять, что и на каком этапе нам может понадобиться, а что нет и когда прибегать к услугам тех или иных компаний, специализирующихся на ИБ.

С точки зрения ИТ инфраструктуры компании можно выделить несколько аспектов ИБ, требующих внимания со стороны специалиста по безопасности. (рис. 2):

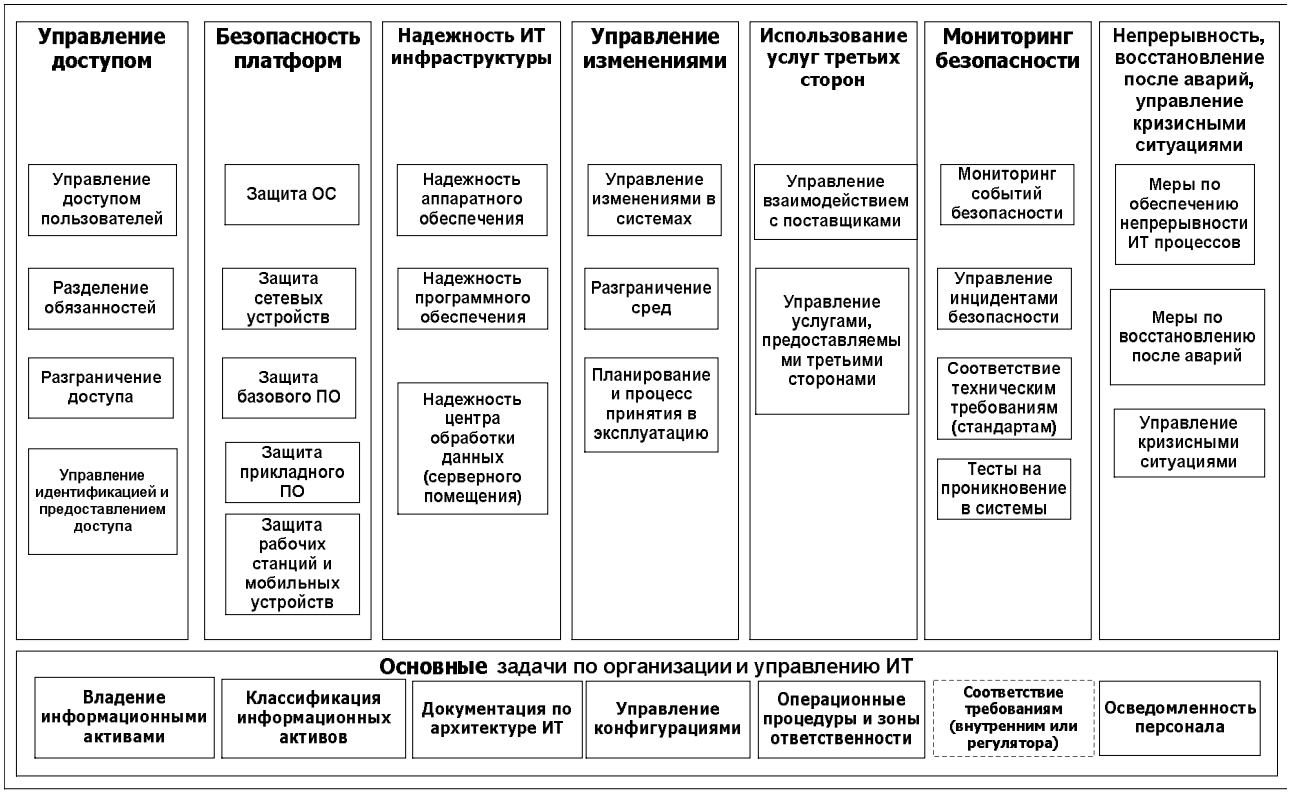


Рис.2. Области ИБ, подлежащие анализу с точки зрения специалиста по безопасности ИТ.

Обратите внимание, что все остальные области, находящиеся в сфере внимания специалиста по ИБ, опираются на организационные вопросы по управлению ИТ инфраструктурой в целом. Большинство задач помогут решить консультанты в сфере ИБ. Обладая необходимыми методиками и специалистами, они могут помочь в течение месяца (в зависимости от размеров предприятия) решить большинство вопросов по организации и управлению информационными активами. Однако необходимо подчеркнуть, что без поддержки менеджмента самого предприятия, эти меры будут носить формальный характер. Поэтому нужно обязательно привлечь менеджеров и владельцев предприятия к данному вопросу. Это в дальнейшем поможет достичь взаимопонимания при внедрении проектов по ИБ в других областях.

Основные решения и продукты по управлению доступом, обеспечению безопасности серверных платформ, надежности инфраструктуры, и мониторинга безопасности можно разбить на группы, как показано на рис.3. Частично, некоторые решения помогают решить вопросы по обеспечению непрерывности бизнеса.

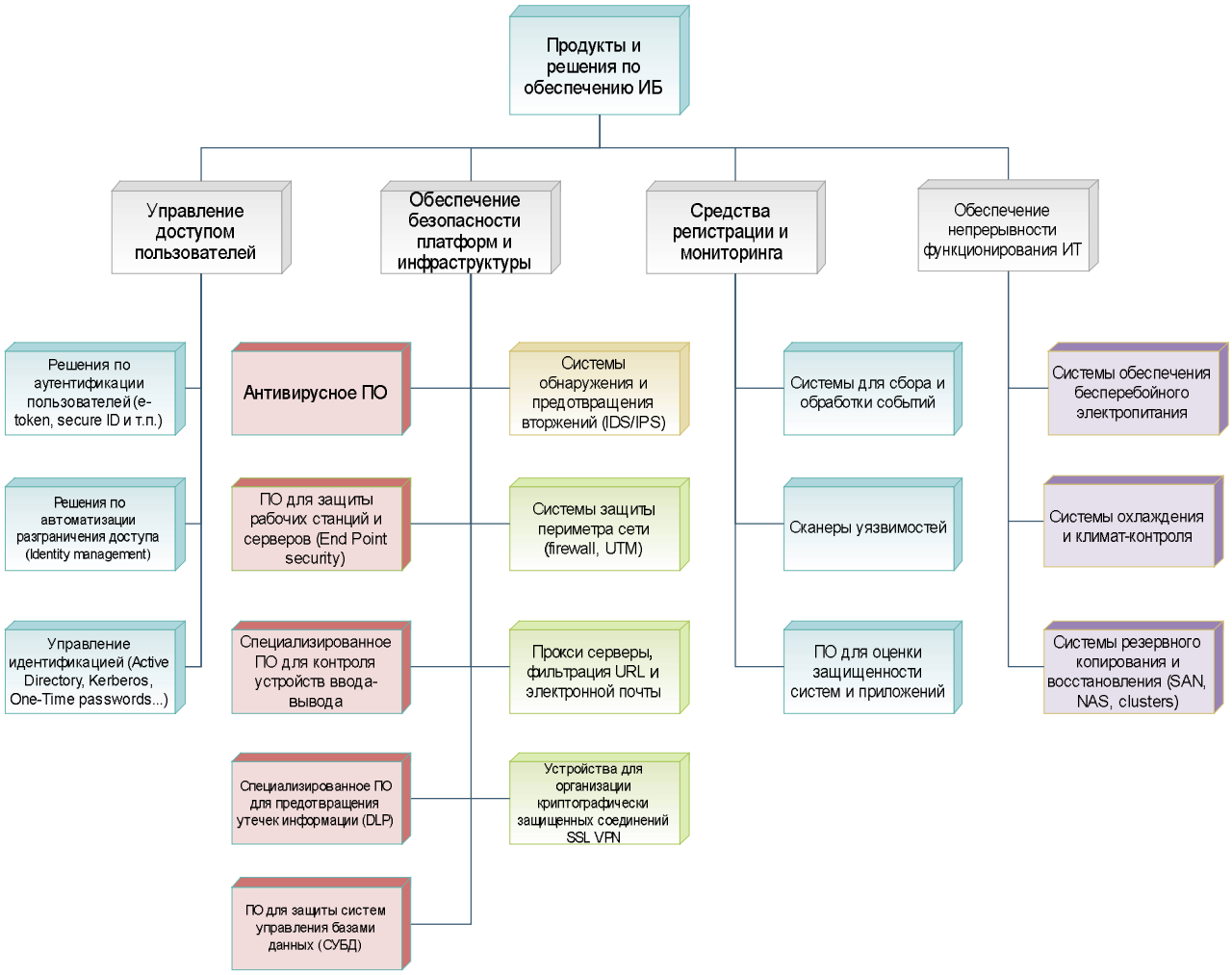


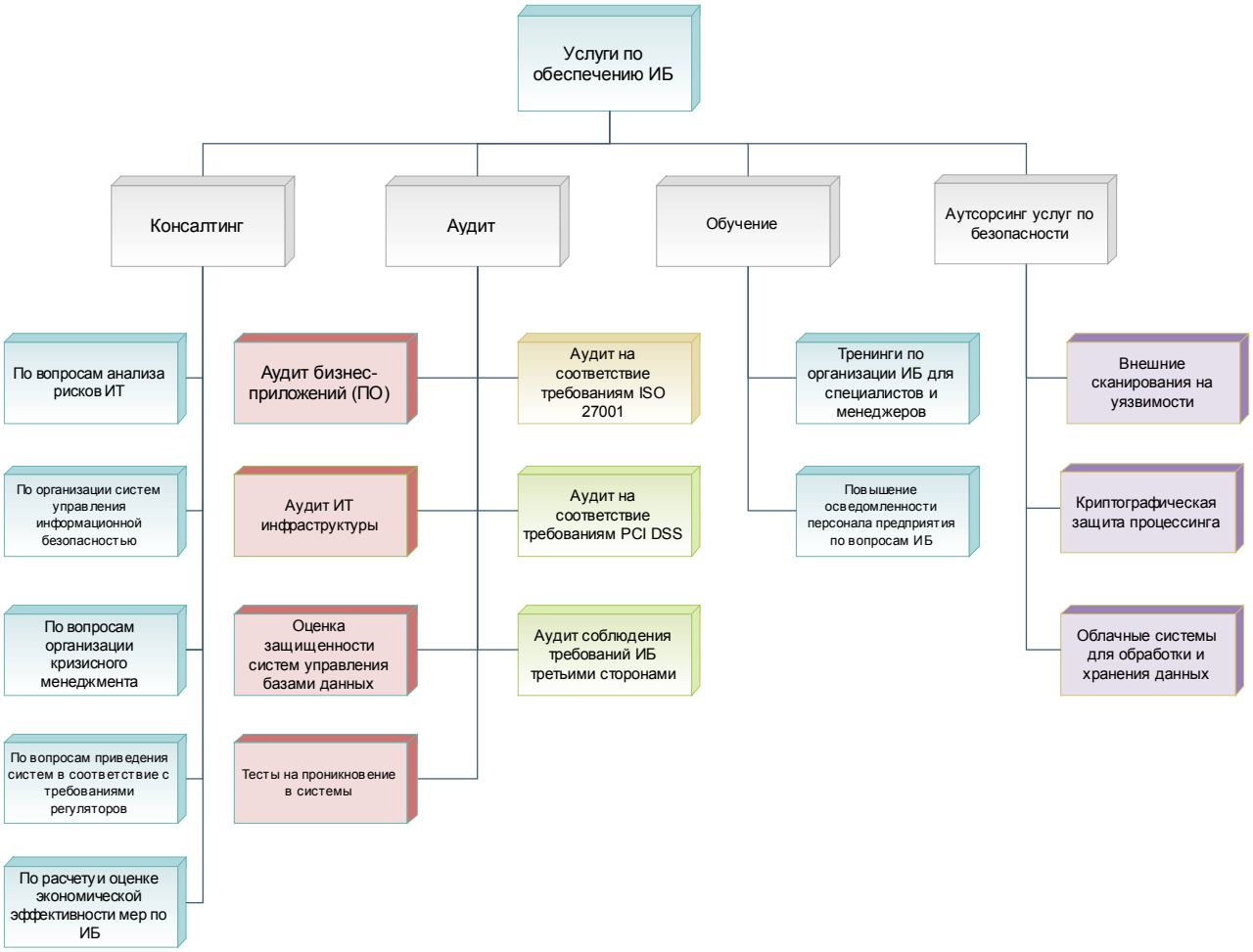
Рис.3. Карта продуктов для обеспечения ИБ

Итак, вне зоны нашего внимания остались продукты по управлению конфигурациями и кризисными ситуациями. Очевидно, что большинство продуктов и решений требуют дополнительных затрат на их установку и наладку. Кроме того, большинство из них требуют периодического обновления лицензии (обычно 1 раз в год), стоимость которой составляет 15-20% стоимости продукта (иногда встречается и больше). Также их цена учитывает количество устройств подлежащих защите (рабочих станций, серверов или IP адресов). Подчеркнем, что *приступать к закупке подобного оборудования или ПО стоит лишь после следующих мероприятий:* оценки рисков для информационных активов (программных и аппаратных); проведения внутреннего аудита ИТ инфраструктуры; расчета показателей возврата инвестиций в ИБ; обязательно заручившись поддержкой менеджмента и владельцев информационных активов.

В первом и втором вопросах помогут консультанты по ИБ или можно выполнить данные мероприятия самостоятельно. Для расчета показателей возврата инвестиций в ИБ требуется собрать несколько коммерческих предложений от системных интеграторов, чтобы представлять порядок стоимости системы и расходы на ее внедрение. Отдельные консалтинговые компании помогут вам также рассчитать параметры возврата инвестиций (Return On Security Investments – ROSI), но они будут бессильны, если отсутствует оценка рисков для объектов защиты. Поэтому начинать следует именно с нее. По требованиям международного стандарта по ИБ ISO 27001 [5] все мероприятия по организации системы управления ИБ опираются на оценку рисков критических систем и приложений.

Попробуем составить *карту консультационных услуг в сфере ИБ* (рис. 4). Основными услугами, как правило, являются: услуги по организации процесса анализа рисков ИТ; услуги по организации систем управления ИБ; аудит состояния ИБ приложений, систем или инфраструктуры ИТ в целом; аудит аутсорсинговых компаний; услуги по внедрению и

поддержке нормативных требований регуляторов или государства; услуги по организации непрерывности бизнеса; услуги по анализу защищенности информационных систем (не путать с аудитом состояния!); услуги по повышению осведомленности пользователей в вопросах ИБ; расчет показателей эффективности и возврата инвестиций в ИБ; обучение менеджеров и специалистов по вопросам ИБ.



Ри

с. 4. Карта услуг для обеспечения ИБ

Многие консультанты предлагают пакеты услуг, иногда включая вопросы аудита. В этом нет ничего плохого, если только далее консалтинговая компания не заинтересована продать вам определенный продукт или решение по ИБ. В этом случае, будьте уверены, такой аудит будет выглядеть как "поход на рыбалку" (в обиходе западных коллег "fishing expeditions") и основная его задача – найти что-нибудь, что неправильно. Следует обращать внимание, на резюме специалистов, которые проводят аудит или консалтинг. Весьма желательно, если их квалификация подтверждена международными сертификатами (ISO 27001 internal/external auditor от BSI или CISA, CISM [6] от организации Information Security Audit and Control Association – ISACA или другими). Это ваше право – знать, кто получает доступ к конфиденциальной информации предприятия. Ведь схема сети вашей компании с адресами и устройствами – это конфиденциальная информация, не так ли? Существуют также элементы контроля качества работ и самих аудиторов, и консультантов. Например, Комитет по стандартам безопасности в индустрии платежных карт (PCI Security Standards Committee – PCI SSC) после сертификации может попросить вас об отзыве на работы проведенные компанией, проводившей аудит. Также можно обжаловать действия компании в этом комитете и даже лишить ее лицензии.

С чего начать и как успешно закончить проект по ИБ? Для суровых реалий бизнеса в Украине специалист по ИБ должен вооружиться … цифрами. Рассмотрим зачем. Менеджеры, распоряжающиеся бюджетом на те или иные задачи, обычно руководствуются следующими

критериями: затратная часть проекта и ожидаемая прибыль от проекта (сколько и когда); что будет, если проект по ИБ не внедрять (административные, дисциплинарные санкции) и можно ли как-то без этого обойтись (есть миллион более важных дел); стоимость владения и ресурсы, нужные для обслуживания; как проект повлияет на имидж менеджера в случае провала или успешной реализации (карьера); насколько проект облегчает, или усложняет пользователям выполнение повседневных задач.

Как видно без расчетов по возврату инвестиций в ИБ, нельзя получить цифры, нужные менеджеру. А расчет невозможно провести без оценки рисков (или хотя бы статистики инцидентов ИБ с финансовыми показателями). Конечно, желательно, чтобы кроме вас еще и регуляторы рынка в лице ГССЗЗИ Украины, НБУ или международных организаций тоже "хотели такую штуку". Найдите к тому же плюсы лично для менеджера санкционирующего проект по ИБ. Убедите его аргументировано в том, что дивиденды от реализации проекта достанутся ему (профессиональные заслуги, уважение и позитивное реноме в глазах руководства). Как только первые 4 критерия выполнены, маловероятно, что будет дан "задний ход" из-за пользователей.

Таким образом, в самом начале нужно иметь нормативно-правовую базу внутри предприятия, которая бы декларировала его стремление в рамках бизнес стратегии к определенному уровню информационной безопасности. Прежде всего это могут быть стратегия развития ИТ с разделом по развитию ИБ и политика информационной безопасности. Иногда крупные компании разрабатывают (и финансируют) отдельную программу по ИБ. Но чаще достаточно первых двух документов. Для обеспечения их функционирования требуется оценить текущее состояние информационных активов и классифицировать их по важности для компании. Далее необходимо оценить риски для информационных активов и на их основе разработать план мероприятий по защите. Здесь появляется возможность для расчета возврата инвестиций в информационную безопасность, т.е. именно те цифры, которые так нужны менеджеру. Теперь можно собирать коммерческие предложения от системных интеграторов, руководствуясь планом мероприятий по защите. После расчета показателей возврата инвестиций в ИБ можно готовить краткий документ (заявку) на проект по ИБ (Project initiation document). В нем кратко излагается цель проекта, технико-экономическое обоснование и расчет ресурсов и времени, требуемых на реализацию. Далее с владельцами систем или данных, подлежащих защите, разрабатываются требования к решению или продукту по ИБ, как правило, они оформляются в виде технического задания согласно ГОСТ 34.602-89, действующего в Украине до сих пор. На этих этапах могут помочь консалтинговые компании по ИБ.

После утверждения технического задания находим подрядчика (обычно это системный интегратор) и он готовит проектную документацию согласно ГОСТ 34.601-90 и РД 50.34-90 (в отдельных случаях, например при внесении изменений в центры обработки данных или при прокладке кабельных линий требуется и строительная документация согласно ДБН А.2.2-2-96 и другим строительным нормам и ГОСТ Украины). В принципе при создании проектной документации можно руководствоваться положениями [7], разработанными ГССЗЗИ в 2005 году. Свою актуальность они не потеряли и сегодня.

По утвержденному сторонами проекту проводятся работы по внедрению средств и/или мероприятий по защите информации. Далее проводятся предварительные испытания систем и оборудования. Затем, в зависимости от сложности систем ИБ, от 1 недели до 1 месяца проводится ее опытная эксплуатация. В течение этого периода проверяются все режимы работы и моделируются ситуации по обработке событий в реальной ИТ инфраструктуре клиента. Начало и окончание опытной эксплуатации подтверждаются соответствующими двусторонними актами. И, наконец, проводятся приемные испытания внедренной системы ИБ. Все виды испытаний и документация по ним описаны в ГОСТ 34.603-92 «Виды испытаний автоматизированных систем». Таким образом, достигаются гарантии эффективного функционирования систем ИБ интегрированных в инфраструктуру предприятия. Также этот, на первый взгляд, громоздкий процесс позволяет определить ответственность должностных лиц, которые участвовали в каждом этапе внедрения и ввода средств и мероприятий по ИБ в

эксплуатацию. Естественно, что в процессе эксплуатации будут возникать изменения и модификации (обновление версий ПО, изменение конфигурации и количества устройств и т.п.). Эти действия на основании проектной документации можно легко согласовывать с поставщиками оборудования и услуг или собственными разработчиками. Более эффективно управлять этим процессом позволит управление изменениями в инфраструктуре (Change management).

Основная идея процесса управления изменениями в системе (или инфраструктуре в целом) заключается в сохранении контроля над системой или совокупностью систем. Как правило, данный процесс организуется внутри ИТ департамента и представляет собой еженедельное или (1 раз в 2 недели) совещание представителей разработчиков ПО, администраторов систем и корпоративной сети, специалиста по ИБ, ответственных ИТ менеджеров и (если необходимо) владельцев систем, куда будут вноситься изменения.

Как видим, если следовать требованиям стандартов и рекомендаций мы обеспечим управляемость и постоянный контроль ИТ инфраструктуры на всех этапах ее развития. Естественно, что после внедрения системы ИБ, необходимо оценить ее эффективность, что достигается с помощью анализа определенных показателей.

Как проверить эффективность проекта по ИБ и что делать дальше? Вопрос оценки эффективности проекта по ИБ, да и в любой другой области, всегда волновал менеджеров ответственных за информационные технологии и безопасность предприятия. Наиболее реально и просто оценить эффективность проекта возможно с помощью специальных показателей риска (Key Risk Indicators – KRI). Эти показатели позволяют организовать оценку эффективности состояния рисков ИТ на предприятии в соответствии с требованиями международных актов в сфере обеспечения операционной и информационной безопасности, таких как американский Sarbanes-Oxley Act (SOX 404) и европейские требования Базельского Комитета по надзору за банковской деятельностью (Basel II).

Показатели ключевых рисков предоставляют возможность менеджерам и системным администраторам реагировать на реальные проблемы в сфере безопасности ИТ, а подразделениям внутреннего аудита и управления рисками осуществлять мониторинг этих действий. Рассматриваемые показатели также характеризуются так называемым допустимым уровнем – условной величиной, принятой менеджментом компании в отношении того или иного риска. Пример показателей рисков приведен ниже в табл. 1.

Выводы. Опираясь на данные инцидентов ИБ в той или иной области, которые влияют на формирование показателя рисков по подразделениям компании, можно оценить количество и характер инцидентов до и после внедрения проекта. Более того, как только показатели рисков вновь опустятся ниже допустимого уровня, можно смело говорить о новой проблеме или угрозе ИБ, которая требует внимания и возможно дополнительных затрат на ее решение.

Таблица 1. Шкала показателей рисков (фрагмент)

Событие ИБ	**Показатель риска**	**Описание**	**Область применения**	**Допустимый уровень**
Инцидент ИБ	Кол-во уязвимостей эксплуатируемых с высокой вероятностью и не закрытых с момента последнего теста на проникновение (этического хакинга)	Кол-во незакрытых критических уязвимостей с момента последнего теста на проникновение	Инфраструктура ИТ и бизнес приложения	Красный >1, Оранжевый=1, Зеленый = 0
Инцидент ИБ	% ИТ систем с антивирусным ПО с последними обновлениями	Выявление рабочих станций, серверов и систем без актуальных антивирусных баз или сигнатур атак	Инфраструктура ИТ	Красный < 75%, Оранжевый ≥ 75%, Зеленый = 100%
Инцидент ИБ	Кол-во инцидентов связанных с компьютерными вирусами, которые не могут быть выявлены имеющимся антивирусным ПО	Кол-во инцидентов в результате воздействия компьютерных вирусов, которые не определяются антивирусным ПО	Инфраструктура ИТ	Красный > 1, Оранжевый = 1, Зеленый = 0
Инцидент ИБ	% критических ИТ систем, находящихся под круглосуточным мониторингом	Степень покрытия критических и важных для бизнеса ИТ компонентов, которые контролируются системой обнаружения вторжений	Инфраструктура ИТ	Красный < 75%, Оранжевый ≥ 75%, Зеленый = 100%
Инцидент ИБ	Кол-во успешных попыток несанкционированного доступа в помещения с ограниченным доступом (в месяц)	Показатель успешности несанкционированного доступа	Помещения с ограниченным доступом	Красный > 1 успешной попытки, Зеленый = 0 попыток

Таким образом, в этой статье была сделана попытка провести качественный анализ решений и услуг по ИБ, а также определить порядок основных этапов внедрения проектов в области ИБ.

Список литературы

1. Державна служба спеціального зв'язку та захисту інформації України. [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua.
2. УкрСЕПРО. [Електронний ресурс]. – Режим доступу: http://www.ukrsepro.kiev.ua.
3. Information technology and services. [Електронний ресурс]. – Режим доступу: http://www.uisg.org.ua.
4. Big4. [Електронний ресурс]. – Режим доступу: http://www.big4.com.
5. ISO 27001 Security. [Електронний ресурс]. – Режим доступу: http://www.27001 – online.com.
6. CISM. [Електронний ресурс]. – Режим доступу: http://www.cism.com.ua.
7. НД ТЗИ 3.7-003-05 "Порядок проведения работ по созданию комплексной системы защиты информации в информационно-телекоммуникационной системе".

Рецензент: Конахович Г.Ф.
Поступила 24.09.2010