Н. Г. Милославская, А. И. Толстой

INFORMATION SECURITY INTELLIGENCE – ОСНОВА СОВРЕМЕННОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Введение

В настоящее время на рынке технологий обеспечения информационной безопасности (ИБ) наметился переход от простых средств управления журналами регистрации (англ. Log Management) и систем управления информацией и событиями информационной безопасности (SIEM-систем, от англ. Security Information and Event Management — управление информацией и событиями ИБ) к системам, поддерживающим аналитику в области безопасности.

В англоязычной литературе данная область получила название Information Security Intelligence, что можно перевести по-разному: аналитика в области ИБ, разведка ИБ, интеллект ИБ. Устоявшегося русскоязычного термина на сегодня пока еще не сформировалось. По аналогии с business intelligence, что переводится как бизнес-аналитика, далее будем использовать наиболее подходящий, по мнению авторов, краткий термин — ИБ-аналитика (при этом ἀναλυτικά в др.-греч. — искусство анализа).

Организации долго шли к осознанию среды обеспечения ИБ (ОИБ). В опросе 2010 г. журнала CSO, спонсированном компанией Deloitte, отмечается, что о семи из десяти инцидентов никогда не сообщается [1]. Более того, в большинстве случаев организации-жертвы даже не знают, что они были атакованы. Кроме того, отчет 2010 г. Verizon Data Breach Investigations показал, что более трети атак не были обнаружены в течение нескольких месяцев, а три пятых из них были выявлены третьими лицами, а не организацией-жертвой. В этом докладе разного рода «неизвестность» отмечается как причина 43 % атак: неизвестные активы; данные, о существовании которых не было известно для конкретного актива; активы, которые имели неизвестные сетевые подключения или доступность; неизвестные учетные записи или привилегии пользователей.

Очень часто в ответ на новые угрозы ИБ разрабатываются частные решения с точки зрения конкретной затрагиваемой технологии или противодействующие этим угрозам новые политики или правила. Причина в значительной степени кроется в наличии для организации унифицированной программы ОИБ, основанной на автоматизированном анализе единой информации обо всей ИТ-инфраструктуре, что дорого, сложно и неэффективно реализовывать на практике. В результате большинство организаций не могут точно распознавать атаки и обоснованно управлять рисками ИБ.

Конкурентоспособные организации преуспевают в значительной степени потому, что они знают, как заставить работать свою информацию на благо бизнесу. Для этого они активно используют аналитику и автоматизирующие ее технологии, что помогает им извлекать максимальную выгоду из имеющихся у них огромных объемов данных. Аналогичный подход следует применять и к защите этой информации, внедряя ИБ-аналитику. Как бизнес-аналитика помогает организациям принимать решения, максимизирующие возможности и минимизирующие бизнес-риски, так и ИБ-аналитика позволяет им качественнее идентифицировать потенциальные угрозы и риски ИБ, выявлять области несоответствия различным требованиям и устанавливать приоритеты в области обеспечения и управления ИБ.

ИБ-аналитика, построенная на тех же понятиях, что и столь значимая для современных организаций бизнес-аналитика, является следующим очень важным шагом для тех из них, кто признает важность ОИБ для ведения бизнеса.

1. Актуальность и основные цели ИБ-аналитики

Современные организации разного размера, подчинения и профиля деятельности получают огромное количество данных, способных помочь обнаруживать угрозы ИБ и выделять области, подверженные высокому риску. Но это возможно только в случае, если организация владеет соответствующими средствами и готова собирать, агрегировать и, что еще важнее, анализировать данные. Эти данные поступают не только от отдельных средств защиты, но и из таких источников, как конфигурация сетевых устройств, серверы, сетевой трафик, приложения, конечные пользователи и их деятельность.

Модель безопасности десятилетней давности уже неадекватна современным проблемам, как интернет-хулиганство далеко отстало от организованной преступной деятельности с использованием специальным образом созданных преступных сетей — ботнетов. Эта модель существенно устарела и не соответствует в полной мере сегодняшним угрозам ИБ и ИТ-среде. Объект защиты «выделенный периметр безопасности» требует расширения до сильно распределенной среды, поскольку сотрудники, партнеры и клиенты организаций ведут свой бизнес удаленно через Интернет, для которого преступники разрабатывают новые направления атак, подрывая доверие пользователей.

Государственные и отраслевые надзорные органы применяют к поднадзорным организациям все более серьезные санкции и требуют более четкого соблюдения своих требований в отношении ОИБ.

В ответ индустрия технологий ОИБ начала производить новые и усовершенствовать старые продукты для противодействия отдельным новым угрозам ИБ. Такие средства повышают общую защищенность организации, но, по сути, являются отдельными «островками безопасности». Они не способствуют созданию единой риск-ориентированной программы ОИБ в масштабах всей организации в целом, а реализуют лишь ее отдельные фрагменты.

Во многих случаях организациям приходится иметь дело с неполными данными, потому что имеющиеся средства защиты могут не распознать атаку и вычислить ее риск без корреляции собранной информации с данными из других источников. И даже если данные собираются из различных источников, аналитики сталкиваются с проблемой огромного объема информации, что делает чрезвычайно трудным выбор из этого объема действительно полезной информации.

Поэтому актуальность применения ИБ-аналитики очевидна. Она позволяет современным организациям поддержать принятие критически важных решений за счет автоматизации процессов анализа данных на таком уровне, на котором ручной анализ вряд ли подойдет. Применяя компьютеризированую бизнес-аналитику в уникальных условиях ведения бизнеса, успешные организации получают максимально возможную отдачу от накопленных терабайт и петабайт данных. Данные становятся новым «бизнес-сырьем» наравне с трудом и капиталом. Поэтому сегодня, как никогда прежде, важны обеспечение беспрепятственного защищенного прохождения потоков данных, управление ими и их анализ.

ИБ-аналитика решает эти проблемы на всех стадиях жизненного цикла ОИБ, централизуя данные из различных источников, нормализуя их (для сравнимости) и проводя в режиме реального времени сложный автоматизированный анализ, основанный на выявлении взаимосвязей между данными и охватывающий большой интервал сбора данных. При таком подходе организации могут выставлять приоритеты обработки рисков ИБ и экономически эффективно использовать ресурсы ОИБ для обнаружения, предотвращения, реагирования и ликвидации последствий инцидентов ИБ [2].

ИБ-аналитика снижает риски ИБ, облегчает соблюдение различных требований (законодательных, договорных и иных), демонстрирует рентабельность инвестиций и увеличивает отдачу от затрат на существующие технологии безопасности.

Следовательно, основные цели ИБ-аналитики, как и бизнес-аналитики, таковы:

1) передавать большие объемы информации в эффективный процесс принятия решений, уменьшая миллиарды единиц данных до разумного, обозримого количества действительно значимых элементов;

2) внедрять сбор и анализ данных за счет автоматизации и простоты использования;

3) предоставлять ценные приложения, которые помогают организациям извлекать максимальную пользу от своих данных для понимания и контроля риска, выявлять проблемы и приоритеты ОИБ;

4) подтверждать наличие на местах правильных политик;

5) гарантировать, что используемые средства управления эффективно следуют этим политикам.

2. Недостатки систем управления журналами регистрации и SIEM-систем

Конечной целью эффективного управления ИБ является комплексная ИБ-аналитика всей информации о функционировании ИТ-инфраструктуры организации (включая активность всех пользователей), зафиксированной в различных журналах регистрации (англ. log files) [3—4].

Основная идея ИБ-аналитики частично реализуется в SIEM-системах, коррелирующих и анализирующих агрегированные и нормализованные данные журналов регистрации. Средства управления журналами регистрации централизуют и автоматизируют протоколирование различных запросов, но им не хватает гибкости, возможностей сложной корреляции и анализа, как у SIEM-систем, и, в конечном счете, ИБ-аналитики.

SIEM-системы следует рассматривать как хорошее средство сбора информации. Они сильны с точки зрения управления событиями ИБ и играют особенно важную роль в выявлении направлений возможных атак. Комплексная же ИБ-аналитика должна охватывать и анализировать гораздо более широкий спектр информации: она требует постоянного мониторинга всех имеющихся в ИТ-инфраструктуре источников данных и оценки собранной информации в контекстах, выходящих за рамки типичных возможностей SIEM-систем. Для ИБ-аналитики требуются самые разнообразные данные, характеризующие весь контекст работы ИТ-инфраструктуры, включая, но не ограничиваясь следующим: журналы регистрации сетевых устройств; уязвимости; конфигурационные данные; сетевой трафик; события и активность приложений; идентификационные данные пользователей; активы, географическое положение; прикладные вопросы. Очевидно, что при этом порождается огромное количество данных, подлежащих анализу.

ИБ-аналитика ценна тем, что в рамках каждой потенциально проблемной области данные анализируются в очень специфическом контексте и выполняются сложные аналитические преобразования для точного обнаружения все возрастающего количества различных типов событий ИБ. Это снижает ложно положительные срабатывания (false positives), показывает не только из-за каких уязвимостей может произойти событие ИБ, но и каковы его последствия, а также обеспечивает более быстрое распознавание и реагирование на инциденты ИБ. Например, потенциальное использование уязвимости веб-сервера, выявленное системой обнаружения вторжений, может быть подтверждено обнаружением необычной исходящей сетевой активности за счет аномалии в поведении сети, и наоборот. Или другой пример: был опубликован отчет, показывающий, что для сервера в конкретной конфигурации только что найдена новая уязвимость. Но в организации таких серверов может быть сотни. Как тогда оценивать угрозу для каждого из них?

ИБ-аналитика может проанализировать все имеющиеся доступные данные и показать следующее:

- наличие или отсутствие уязвимости в контексте конкретной топологии сети;
- ценность активов и/или данных, присвоенную им организацией;
- вероятность использования уязвимости, основанную на пути атаки из модели угроз ИБ;

- установление всех коммуникаций злоумышленника, которые логически привели или могут привести к реальной атаке;
- конфигурационную информацию, которая может свидетельствовать, например, что конкретный сервер не доступен, потому что настройки по умолчанию были изменены;
- наличие средств управления ИБ, таких как система обнаружения (СОВ) или предотвращения (СПВ) вторжений (англ. Intrusion Detection System, IDS, и Intrusion Protection System, IPS).

Или рассмотрим угрозу со стороны инсайдера. 250 000 секретных дипломатических телеграмм США, переданных WikiLeaks, были получены авторизированным пользователем — профессором Мэннингом, который действовал в рамках своих полномочий [5]. Скорее всего, любой защитный механизм не сможет обнаружить такого рода действия, но анализ скоррелированных данных от нескольких источников позволил бы остановить утечку информации, прежде чем она привела к реальному ущербу.

3. Преимущества ИБ-аналитики

Этапы применения ИБ-аналитики представлены на рис. 1 [2]: за сбором данных от различных источников следует их нормализация (приведение к единому формату представления) и категорирование, после чего в результате анализа происходит выявление нарушений в ОИБ, для которых устанавливаются приоритеты их устранения.

Одно из наиболее убедительных преимуществ ИБ-аналитики — ее высокая работоспособность: более эффективное использование людских, временных и инфраструктурных ресурсов. ИБ-аналитика может объединять несколько технологий ОИБ и сетевых технологий в единую систему, а не полагаться на отдельные средства, работающие независимо друг от друга.

ИБ-аналитика становится важнее и важнее, по мере того как ответственность за ОИБ все чаще передается персоналу, обеспечивающему поддержку функционирования сети организации. Тогда имеет смысл объединить ответственность этого персонала за функционирование с проведением аналитической работы. Учет возможности выполнения нескольких задач на единой платформе и развитие разных функциональных навыков персонала в рамках всей организации далее потребуют предоставления ролевого доступа.

Кроме того, ИБ-аналитика усиливает ценность других ИТ-областей, таких как диагностика системных ошибок, разрешение проблем на уровне сети, поддержка пользователей и анализ полномочий.

Для решения различных проблем ОИБ ИБ-аналитика позволяет организациям на единой основе использовать все интегрированные средства и консолидированный (объединенный) набор данных. Преимущества такого подхода можно проиллюстрировать следующими пятью случаями применения ИБ-аналитики (они представлены на рис. 1).

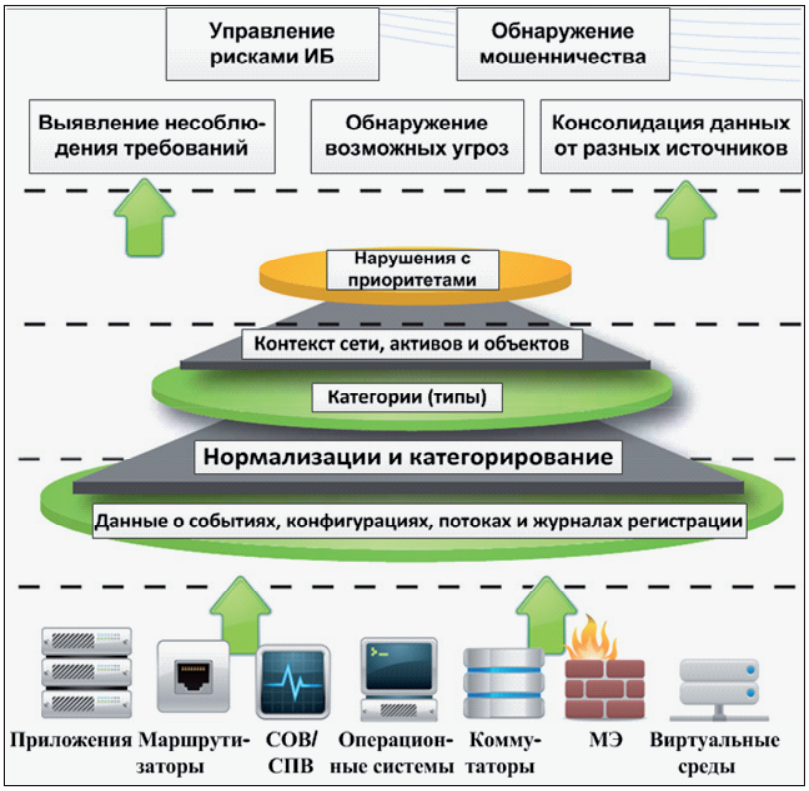

Рис. 1. Этапы применения ИБ-аналитики

Консолидация больших объемов данных

Бизнес-аналитику трудно выполнить без автоматизированной технологии. Данные, которые позволяют оценить возврат от инвестиций, проследить цепочки поставок и т. д., доступны, но находятся в разных приложениях и базах данных. Все дальнейшее зависит от того, каким образом аналитик объединит данные из всех этих источников и внесет их в электронные таблицы или базы данных для последующего анализа вручную. При анализе ИБ возникают похожие проблемы, с которыми эффективно справляется ИБ-аналитика.

С точки зрения ИБ данные могут быть трех типов:

- данные, находящиеся в разрозненных средствах защиты, приложениях и базах данных;
- данные, которые собраны от отдельных устройств, приложений и т. д., — это по сути другие базы данных, где данные хранятся; они, например, не связаны с базами конфигурационных настроек;
- имеющиеся в организации данные, разделенные по ее подразделениям, оперативным группам и т. д.

В первых двух случаях ИБ-аналитика разрушает границы таких данных, интегрируя на общей основе потоки данных от разрозненных устройств для автоматизированного анализа с применением различных технологий ОИБ и ИТ. С точки зрения безопасности это дает расширенные возможности обнаружения и оценки рисков, базирующиеся на консолидированной оценке происходящего в ИТ-инфраструктуре организации. С точки зрения руководителя ИТ-подразделения, сокращение источников таких данных позволяет рационально использовать средства защиты, которыми в противном случае необходимо управлять каждым по отдельности.

Третий тип данных требует значительного взаимодействия между группами персонала, которые обычно разделены, перепрофилирования процессов и изменения зон ответственности и, возможно, вмешательства со стороны руководства организации.

Общий совокупный объем всей этой разрозненной информации существенно усугубляет проблему. Каждый из этих типов данных может породить огромные массивы данных, представленных в разных форматах для разных целей и в некоторых случаях с разными политиками и даже требованиями по ОИБ. Только автоматизированная ИБ-аналитика может эффективно управлять огромными объемами разных типов данных, относящихся к ИБ, и анализировать их.

Выявление возможных нарушений и явных атак

В последние несколько лет организации широко используют интернет-коммерцию и часто взаимодействуют с пользователями удаленно. В связи с этим задача ОИБ стала решаться не для периметра защиты со всеми политиками, сосредоточенными на межсетевом экране (МЭ), а для распределенной среды. Обеспечивать ИБ в настоящее время требуется для хостов (устройств с уникальными адресами), приложений и самого содержания информации, исходящей из организации.

Более того, растет число инцидентов с четко направленными целями атак, такими как атаки на биржу NASDAQ [6] и на другие широко известные компании.

Сложные, четко нацеленные вторжения осуществляются, как правило, в несколько этапов и по многим направлениям. Их трудно обнаружить и еще труднее искоренить. Постоянные атаки повышенной сложности (англ. Advanced Persistent Threats, APT) характеризуются упорством нападающих и наличием необходимых ресурсов.

К различным технологиям ОИБ, разработанным в ответ на появление новых угроз ИБ, должна применяться более всесторонняя аналитика. Поэтому и важен контекст ОИБ, поскольку деятельность, которая безобидна для одной части ИТ-инфраструктуры, может быть определена как угроза при корреляции данных, полученных из разных источников. Например, злоумышленник может отключить ведение журнала регистрации, но не может «выключить» сетевую активность. Отдельные приложения могут не вести журналы регистрации; в некоторых частях сети могут не использоваться межсетевые экраны. В таких случаях ИБ-аналитика может также идентифицировать приложения и сервисы, работающие между хостом и сетью, и помечать это как потенциальную угрозу.

Обнаружение мошенничества

ИБ-аналитика совершенно необходима для эффективного обнаружения мошенничества. Ключевой элемент ИБ-аналитики, в дополнение к получению информации о значениях измеряемых параметров (телеметрии) сети, — это данные, получаемые от средств защиты и сетевого оборудования типа коммутаторов, маршрутизаторов и т. п. и помогающие понять данные пользователей и приложений.

Методы выявления мошенничества требуют мониторинга всего, что происходит в сети: сетевой активности и сетевых событий, активности хостов и приложений, активности отдельных пользователей. ИБ-аналитика позволяет ассоциировать пользователя с определенным активом. Например, объединяя в единое целое информацию о сетевой активности, активности сервера доменных имен (DNS-сервера) и активности приложений с информацией о подлежащих защите данных, ИБ-аналитика может связать отдельного пользователя с конкретным IP-адресом в рамках конкретной сессии, установленной с использованием виртуальной частной сети (англ. Virtual Private Network, VPN).

Управление рисками ИБ

ИБ-аналитика создает основу для управления рисками ИБ, анализируя последствия и моделируя угрозы. Очевидна разница между реагированием на сетевые атаки и проактивной защитой самых важных активов организации от них.

Анализ последствий основан на ценности, присваиваемой организацией конкретному активу, и негативных последствиях для бизнеса после атаки на него. ИБ-аналитика решает эту проблему

за счет выделения критически важных активов посредством их инвентаризации и классификации с точки зрения сохранения для них свойств ИБ при вовлечении в бизнес-процессы организации. Кроме того, устанавливается, насколько уязвим этот актив, имеет ли он прямой доступ в Интернет и известные уязвимости, для которых существуют использующие их хакерские программы — эксплойты (англ. exploits).

Моделирование угроз учитывает все эти факторы и идентифицирует не только уязвимости атакуемой системы, но и возможные направления атак за счет использования уязвимостей на пути между объектом атаки и Интернетом, например, плохо разработанные правила фильтрации межсетевого экрана, плохо настроенные списки доступа маршрутизаторов и т. д.

Выявление несоответствия различным требованиям

Проверка соответствия различным требованиям является основополагающей для ИБ-аналитики. Такие требования могут касаться всех аспектов мониторинга ИБ. Так, например, ИБ-аналитика показала, что организация не выполняет требования, предъявляемые к взаимосвязи периферийных компонентов (англ. Peripheral Component Interconnect, PCI), но удовлетворяет всем требованиям к мониторингу PCI таким образом, каким в одиночку не могут удовлетворять ни SIEM-системы, ни системы управления файлами регистрации.

ИБ-аналитика порождает данные, которые предоставляются всем проводящим аудит регулирующих органам и демонстрируют им выполнение соответствующих требований. Осуществляя мониторинг для всей ИТ-инфраструктуры с точки зрения событий, изменений в конфигурациях, сетевой активности, активности пользователей и приложений, ИБ-аналитика способна установить соблюдение определенных требований при использовании всего лишь одного набора средств, а не полагается на несколько разрозненных решений, каждое из которых предназначено для предоставления лишь части информации, необходимой аудиторам.

4. Функционал систем, автоматизирующих ИБ-аналитику

Обычно системы, автоматизирующие ИБ-аналитику, функционируют на унифицированной операционной платформе и управляются с единой консоли. Это программные решения, которые используют известные подходы для обнаружения несоблюдения установленных требований по ОИБ, выявления и противодействия мошенничества и т. п. Они имеют единую архитектуру для анализа журналов регистрации, потоков, уязвимостей, данных о пользователях и защищаемых активах [2—4, 7]. Такая реализация систем позволяет выявлять неизвестные до этого уязвимости и атаки (так называемые уязвимости и атаки «нулевого дня» — англ. zero day).

В системе, автоматизирующей ИБ-аналитику, реализован набор типовых сервисов — от рутинных до сложнейших, включая интеграцию данных, их нормализацию, единое хранилище, единую систему архивирования и собственно аналитику.

Такая система осуществляет детальный мониторинг сети, выявляя сложные аномалии в ее поведении, а не просто анализируя журналы регистрации. При мониторинге сети такая система на основе динамически изменяющейся информации анализирует все взаимодействия на уровне приложений, проверяет настройки сетевых устройств (маршрутизаторов, коммутаторов и т. п.) и средств защиты (межсетевых экранов, IPS и т. д.), контролирует использование протоколов и содержимое пакетов. Она проводит не только детальный анализ пакетов (англ. Deep Packet Inspection, DPI), реализованный в современных МЭ (англ. Next Generation Firewalls, NGFW), но и потоков данных (англ. Deep Flow Inspection, DFI).

Объектом анализа могут быть сложные виртуальные среды и облачные технологии.

В разрезе пользовательской активности такие системы осуществляют мониторинг привилегированных и обычных пользователей, отличают ошибки пользователей от злонамеренной активности, нормализуют информацию о пользователях и учетных записях, профилируют поведение

пользователей и обнаруживают в нем отклонения от нормы и подозрительную активность, а также коррелируют доступ к данным с сетевой активностью.

Все проанализированные данные составляют единый контент, в рамках которого и должно осуществляться ОИБ.

Системы, автоматизирующие ИБ-аналитику, поддерживают единую и согласованную последовательность выполнения всех подпроцессов, включая сбор, нормализацию, категорирование, корреляцию, собственно анализ, а также составление отчетов, выдачу оповещений и визуализацию информационных панелей. Они могут содержать предустановленные стандартные правила корреляции и анализа, а также позволять расширять этот набор специфическими для организаций правилами.

В результате всех операций осуществляемой в рамках ИБ-аналитики организация получает точные и практически применимые результаты, которые позволяют обеспечивать ИБ на операционном, управленческом и исполнительном уровнях и быстро подстраиваться под изменяющиеся со временем требования по ОИБ.

Заключение

ИБ-аналитика, как и бизнес-аналитика, позволяет организациям принимать более взвешенные бизнес-решения за счет более эффективной обработки большего объема доступной информации обо всей их ИТ-инфраструктуре. Применяя технологии бизнес-аналитики, организации могут производить больше аналитических действий с меньшими затратами: вместо того чтобы аналитики тратили долгие часы дорогого рабочего времени, вручную просматривая всего лишь часть имеющихся данных, бизнес-аналитика автоматизирует анализ сразу всех доступных данных и предоставляет основанную на ролевом подходе информацию, специфичную для каждой конкретной задачи.

ИТ, кроме всего прочего, автоматизирует бизнес-процессы — закупки, логистику и т. д. ИБ-аналитика автоматизирует процесс ОИБ, включая управление рисками ИБ, мониторинг ИТ-инфраструктуры с целью выявления угроз и уязвимостей и установления приоритетности устранения последствий.

За счет централизации средств зашиты и данных от ИТ-инфраструктуры ИБ-аналитика позволяет консолидированно управлять и более эффективно использовать ресурсы, предназначенные для ОИБ. Организации усовершенствуют свое ОИБ без дополнительных организационных и кадровых затрат и без приобретения, сопровождения и интеграции нескольких отдельных средств защиты.

ИБ-аналитика дает следующие основные преимущества в стоимости и эффективности бизнеса:

- снижает затраты, связанные с развертыванием и эксплуатацией средств управления ИБ. Вместо увеличения персонала он высвобождается для решения других задач, позволяющих усовершенствовать ОИБ для поддержки основных бизнес-целей;
- делает приобретение различных средств проще и дешевле. Организация приобретает единую платформу, а не несколько разрозненных систем;
- облегчает развертывание средств управления ИБ на единой платформе взамен установки нескольких отдельных систем (каждая в своей среде) с последующей их интеграцией;
- предоставляет организации широкий спектр возможностей по ОИБ, что раньше было доступно только для самых продвинутых из них;
- автоматизирует сбор, нормализацию и анализ больших объемов данных, относящихся к ИБ, из различных источников — технических и организационных. Эта возможность позволяет применять разнообразный контекст в рамках каждого анализа;

- улучшает обнаружение потенциальных угроз, применяя конкретный контекст для выявления возможных атак, которые могли остаться незамеченными при использовании некоторых технологий ОИБ;
- своевременно изменяет способ реагирования на инциденты посредством их более точного и быстрого обнаружения и категорирования;
- осуществляет типовой расчет возврата инвестиций. Организации могут внедрять новые сервисы ОИБ, такие как автоматическая доставка информации о постоянно обновляющихся всемирно известных базах данных по уязвимостям и актуальным угрозам ИБ (типа всемирно известной базы Common Vulnerabilities and Exposures [8]), без дополнительной рабочей силы;
- дает организациям возможность эффективно внедрять планы ОИБ, ежедневно обрабатывая огромные количества записей и производя множество управляющих действий с высокими приоритетами без перерыва 24 часа в сутки.

Перспективно мыслящие руководятели организаций признали и оценили значение технологий бизнес-аналитики, поскольку их успех основывается на способности анализировать и действовать в соответствии с важной аналитической информацией, полученной из огромных объемов данных. То же можно отметить и по отношению к ИБ-аналитике, поскольку ИБ является неотъемлемой частью ведения бизнеса в XXI в. Мощная, автоматизированная аналитика централизованных данных от источников, охватывающих все элементы ИТ-инфраструктуры, делает экономически эффективное ОИБ не только возможным, но и незаменимым.

Таким образом, со временем ИБ-аналитика может превратиться в интеллектуальную систему, позволяющую организациям наиболее результативно и экономически эффективно решать задачи управления и обеспечения ИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. Cyber crime: a clear and present danger Combating the fastest growing cyber security threat [Электронный ресурс]. URL: http://www.deloitte.com/assets/dcom-unitedstates/local%20assets/documents/aers/us_aers_deloitte%20cyber%20crime%20pov%20jan252010.pdf (дата обращения: 11.12.2013).
2. *Burnham J.* What is Security Intelligence and Why Does It Matter Today? [Электронный ресурс]. URL: http://securityintelligence.com/what-is-security-intelligence-and-why-does-it-matter-today/# (дата обращения: 11.12.2013).
3. Security Intelligence Operations [Электронный ресурс]. URL: http://tools.cisco.com/security/center/home.x (дата обращения: 11.12.2013).
4. SAS® Security Intelligence [Электронный ресурс]. URL: https://www.sas.com/software/security-intelligence (дата обращения: 11.12.2013).
5. Wikileaks опубликовала 250 000 секретных дипломатических телеграмм США [Электронный ресурс]. URL: http://www.gazeta.ru/news/lastnews/2010/11/28/n_1590477.shtml (дата обращения: 11.12.2013).
6. Сайт биржи Nasdaq упал на два дня из-за хакерской атаки [Электронный ресурс]. URL: http://www.gazeta.ru/business/news/2013/07/19/n_3053181.shtml (дата обращения: 11.12.2013).
7. *Rains T.* Microsoft Security Intelligence Report v15 Overview [Электронный ресурс]. URL: http://www.microsoft.com/security/sir/videos/default.aspx#!video_sirv15_overview (дата обращения: 11.12.2013).
8. Common Vulnerabilities and Exposures [Электронный ресурс]. URL: http://cve.mitre.org (дата обращения: 11.12.2013).