ПЛЕНАРНЫЕ ДОКЛАДЫ И ВЫСТУПЛЕНИЯ ЭКСПЕРТОВ

УДК 004

Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Аннотация. В статье рассмотрены вопросы о назревшей необходимости автоматизации информационной безопасности на предприятии, особенности подхода к автоматизации в области управления информационной безопасности как процессу, рассмотрены уровни функционального персонала предприятия, нуждающихся в автоматизации своих функциональных, штатных процедур. Рассмотрены вопросы направленности процесса на предприятии. Затронуты некоторые системы автоматизации в области ИБ, такие как СиММА и автоматизации в области ИБ.

Ключевые слова: открытый исходный код, проприетарное программное обеспечение, метрика, скрипт, платформа автоматизации.

На сегодняшний день созрели все условия для автоматизации в области ИБ, поскольку рутинные процедуры, выполняемые специалистами ИБ, с каждым годом количественно только нарастают. Небезызвестно, что рутина в любом рабочем процессе, занимая порой все рабочее время, поглощает сотрудника как личность, подавляет творческую активность, так скажем угнетает креативную составляющую, как творческих групп, так и всего предприятия, мешает выстраивать необходимые мероприятия по коррекции своих действий во все быстрее и быстрее меняющемся в информационном мире. Скажем так – хочешь, чтобы рабочая структура перестала функционировать в области прямого своего назначения – завали ее отчетной рутиной. Так в свое время нейтрализовал девятый технический отдел разведки Великобритании МИ-6, завалив своих подчиненных рутинным составлением всевозможных отчетов и прочих бумаг, Георг Блэйк, который являлся одновременно резидентом внешней разведки СССР в период проведения нашей контрразведкой операции «Берлинский тоннель» в 1953 г., обеспечив полное фиаско чаяниям разведки противника [1].

Покажем три уровня, нуждающиеся в уходе от рутины с помощью автоматизации:

1. Уровень инженеров. Люди, работающие руками, например, создающие виртуальные машины. Когда количество создаваемых виртуальных машин достигает до нескольких десятков в день, то на их создание требуется огромное количество рабочего времени. Инженер начнет

использовать Antibl, напишет один раз Скрипт- и будет «разливать» эти виртуальные машины.

2. Уровень руководства. Средний менеджмент в тот момент, когда одна и та же задача постоянно разрастается, масштабируется и привлекает все большее количество людей, порой до нескольких сот единиц для ее решения, а именно- вовремя набирать отчеты по требованию топ-менеджмента. Что бы решить такого рода разрастающуюся проблему и необходима автоматизация.

3. Уровень топ менеджмента. Несвоевременность выполнения запросов, отчетов из-за больших объемов работ требуют автоматизации этих процессов.

Рассмотрим ситуацию. Если у компании есть какое-то решение или компания берется решать какие-то свои задачи самостоятельно изнутри, то она начинает использовать Open Source – открытый исходный код – модель разработки программного обеспечения, где исходный программный код доступен для открытого просмотра в отличие от закрытого, проприетарного программного обеспечения, которое является собственностью разработчика и не доступно для просмотра посторонними, тогда появляется необходимость в том, чтобы все эти внутренние разработки были безопасными, а анализ кода, все процессы с DLP- они так или иначе завязаны на автоматизацию, потому что иначе человеку «вручную» проверить все это невозможно.

Заметим, автоматизация впрок абсурдна, процесс должен быть воспроизводим не единожды, случись иначе, получится только автоматизированный хаос. Если процесс воспроизведен не раз, то процесс формализуем, и если его можно разложить по шагам, то его вероятно можно автоматизировать, не факт, что это будет эффективно, но пригодность автоматизированных процедур будет налицо.

Для автоматизации подобных процессов уже успешно используется СиММА – система многослойного моделирования, каталогизации и структуризации данных, согласно архитектуре предприятия с отражением ее в виде цифровых различных объектов реальности инженерной, организационной и программной природы, а также автоматизация обработки рисков.

СиММА разработана российскими специалистами, согласно программе по импортозамещению, а именно, замены импортного продукта VISIO [2].

Подходя к вопросу автоматизации, нужно подразумевать не бесконечное множество инцидентов, что могут произойти в инфраструктуре, а выделить недопустимые ключевые события, которые могут произойти, например хищение денежных средств со счетов, оборотные штрафы в результате утечки персональных данных, и далее смоделировать ситуацию возможной или невозможной реализации этого риска. Если есть возможность верифицировать, то есть, выявить высокую вероятность реализации риска, соответственно, можно спроектировать такую

автоматизированную систему безопасности, которая позволит этот риск устранить. Если это возможно, то можно говорить, что автоматизация необходима.

Автоматизация может происходить либо сверху вниз, либо снизу вверх.

Когда происходит автоматизация рутинных операций, то автоматизирование идет снизу вверх, например, проявилась проблема – написали скрипт и автоматизировали, проявилась еще одна проблем – написали скрипт и автоматизировали, потом пишется скрипт, который автоматизировал скрипты, написанные ранее, и появляется большая «гора скриптов», сложно поддерживаемая.

Но если автоматизация происходит сверху вниз, процесс развивается упорядочено, согласно разработанной стратегии, плану, проекту. Автоматизация процесса целиком – задача, цель которой не автоматизировать ради автоматизации, а достичь определенной цели, например реализовать проверки технических и организационных мер. Определить из чего состоит этот процесс и анализ, что в этом процессе можно автоматизировать на основе комплексного решения, которое по реализации выдает итог: автоматизирован контроль проверок [3].

Но при автоматизации снизу вверх картина получается несколько другая. Если автоматизировать какой-то кусочек, потом трудно будет найти место, куда его еще можно интегрировать, где он принесет пользу.

Регулярно все замечательные инициативы сверху с точки зрения пересмотра процессов рушатся из-за отсутствия четкого целеполагания, то есть определения характера и направленности действий внутри организации, обусловленных показаниями метрик, и если имеется возможность снимать метрики и построить дерево метрик, то можно легко определить на какую бизнес – метрику будет направлена централизованная автоматизация [4].

И все-таки, на практике чаще всего происходит автоматизация рутины, потому что наверху по тем или иным причинам не получается перераспределить или перепроектировать работающий, приносящий уже определенный результат, процесс. К тому же аналитик, уставший от рутинного однообразия измерения метрик, может подойти снизу, автоматизировав такой процесс.

Так что же понимается под платформами автоматизации, какие средства необходимы для этого. Автоматизация ИБ довольно-таки разнообразна и вот одна из систем:

– SGRC (Security Governance, Risk Management and Compliance) – Система управления безопасностью, рисками и соответствием законодательству. То есть, фактически, SGRC – это система для автоматизации построения комплексной системы управления информационной безопасностью (СУИБ). Системы SGRC включают в себя три основных подхода к построению СУИБ:

1. Governance. Управление, руководство – управление информационной безопасностью директоратом компании, который на основе полученных данных о системе управления информационной безопасностью, обработанных программным комплексом SGRC, вырабатывает бизнес - обоснованные директивы.

2. Risk Management. Управление рисками – создание высокого уровня информационной безопасности за счет проведения мероприятий, призванных эффективно исключать уязвимости и минимизировать риски системе ИБ.

3. Compliance. Соответствие, т.е. исключение инцидентов, связанных с нарушением законодательных предписаний, установленных государством, корпоративных стандартов и соблюдения политик и режимов на предприятии, развитие которых приводит к потере репутации, незапланированным затратам, штрафам, выставляемым со стороны контролирующих организаций.

Системы SGRC призваны для автоматизации процесса строительства СУИБ и настроены, прежде всего, на автоматизацию процессов информационной безопасности и ограниченно на ИТ-процессы. В функции SGRC-систем входят:

- управление ИТ-активами;
- управление рисками ИБ;
- документальную обработку инцидентов ИБ (поддержку расследования инцидентов ИБ, протоколирование, накопление базы знаний);
- соответствие нормативным требованиям информационной безопасности- законодательным, отраслевым, корпоративным;
- поддержку проведения внутренних аудитов ИБ и самооценок;
- управление процессами обеспечения непрерывности бизнеса и восстановления работоспособности;
- построение отчетности и дашбордов с функционалом drill-down (возможность «проваливаться» вглубь предоставляемой информации для получения детальных сведений по элементам отчета) [5].

Кроме систем SGRC, которые ориентированы на управление и обеспечение информационной безопасности, существуют неспециализированные системы GRC (Governance, Risk Management and Compliance), которые могут быть сфокусированы на управлении финансами, ИТ, бизнес-рисками. Функционал таких GRC-систем общего назначения включает в себя:

- управление политиками, аудитами и рисками;
- автоматизацию соответствия законодательству;
- управление документами и версиями;
- управление взаимоотношениями с поставщиками и контрагентами
- контроль доступа и полномочий;

– мониторинг бизнес-процессов;
– построение отчетности и диаграмм/графиков/дашбордов.

Платформы SGRC используется для накопления и анализа данных, явлений, относящихся к области информационной безопасности, нормативным и законодательным документам в отношении построения мероприятий по защите информации на предприятии, к процессам функционирования информационной структуры предприятия. Данные для обработки SGRC поступают от автоматизированных систем, таких как ERP (Enterprise Resource Planning), которая призвана быть единым центром на предприятии для обработки поступающих данных от ответственных за определенные процедуры, таких как составление отчетов на основе результатов, полученных при проведении очередного или внепланового аудита, и хранения полученной и обработанной информации, противодействует дублированию получаемых данных, нивелирует до минимума предпосылки ошибок, и которая просто объединяет всевозможные слагаемые предприятия, такие как реализация и сбыт продукции, разработка и производство, финансовая деятельность, управление личным составом в единый информационный кластер. Таким образом, чем больше процедур в области информационной безопасности с применением подобного рода программных информационных систем получится подвести под автоматизацию, тем больше освободившегося персонала можно занять на решение других немаловажных, ключевых вопросах информационной безопасности, за счет уменьшения уровня занятости на каком-то определенном, рутинном вопросе. Давно замечено, если дело касается рутинных занятий, таких как мониторинг, требующих высокой точности измерений, человек на современном этапе развития технологий все более замещается автоматами, тем самым исключается риск получения ошибочных, не соответствующих реальному состоянию исследуемой среды данных, исключается так называемый человеческий фактор. И чем более расширенно будет осуществляться автоматизированный сбор данных для SGRC-системы. чем более эти данные будут соответствовать действительному положению дел по состоянию ИБ на предприятии, и тем более реальные результаты, полученные вследствии мониторинга системы безопасности, будут отражаться в отчетах по аудиту, тем более правильными будут приниматься решения высшим руководством фирмы, в отношении реагирования на инциденты, выработки корректирующих процедур, положений по совершенствованию информационной безопасности. И чем больше будет использовано ИТ-систем для предоставления данных для SGRC, при помощи которой будет выстроена система управления ИБ, тем более она будет выверена [2].

И все же, это вопросы частные, что касается общего, то при наличии дефицита специалистов ИБ, не говоря уже о высокопрофессиональных, появление все новых и новых преступных кибертехнологий и методов и,

соответственно, стремительного возрастания загруженности персонала, вопросы по автоматизации ИБ являются жизненно важными и необходимость в этом будет только возрастать.

Список использованных источников:

1. Биография советского разведчика Джорджа Блейка: URL: https://tass.ru/info/10359633.
2. Система многослойного моделирования архитектуры: URL: https://bm-symma.ru/?ysclid=mawaxo1iy324518933.
3. Автоматизация информационной безопасности. URL: https://falcongaze.com/ru/pressroom/publications/osnovy-ib/avtomatizaciya-informacionnoj-bezopasnosti.html.

Bayrushin F.T.
Ufa University of Science and Technology, Ufa

AUTOMATION OF INFORMATION SECURITY MANAGEMENT

Abstract. The article discusses the urgent need for automation of information security at the enterprise, the specifics of the approach to automation in the field of information security management as a process, and the levels of functional personnel of the enterprise who need automation of their functional, regular procedures. The issues of the orientation of the process at the enterprise are considered. Some automation systems in the field of information security, such as SiMMA and automation in the field of information security, are affected.

Keywords: open source code, proprietary software, metric, script, automation platform.