Родыгин Евгений Валентинович
CIISO АО «Кронштадт»
Соучредитель товарищества специалистов по ИБ RISC

Информационная безопасность
13 граней профессии

Введение.

Как алмаз становится по настоящему драгоценным бриллиантом только после его огранки, так и деятельность профессионала по информационной безопасности блистает только после многолетней огранки и шлифовки граней профессии. В этой статье, я попытаюсь поделиться своим опытом по нескольким ключевым граням профессии специалиста по информационной безопасности.

Грань 1 «Роль ИБ»

Прежде всего необходимо понять, что роль информационной безопасности в компании именно такая, какой ее воспринимает бизнес. Именно так, не больше и не меньше. При этом представления о роли, целях и задачах ИБ в компании могут быть самыми разными, от установки антивируса до поддержки выработки стратегии бизнеса. При прочих равных, эффективность ИБ в компании тем выше, чем шире охват роли ИБ в ее деятельности. Специалист по ИБ оперирует и стремится расширять 4 ключевых направления деятельности:

1) Знание (все активы, ИТ-инфраструктуру, бизнес-процессы и т.п.);
2) Контроль (состояние защищенности, изменения, каналы передачи информации и т.п.);

3) Защита (конфиденциальность, информационные активы, ИТ-инфраструктура, репутация и т.п.);
4) Влияние (на ИТ-инфраструктуру, планы развития, принимаемые решения, позицию руководства).

Сразу оговорюсь, указанные направления никогда не будут охвачены в достаточной степени. Уровень охвата зависит и от специалиста по ИБ и от руководства, и от массы других факторов. Никогда бизнес не будет в полной мере доволен направлением ИБ и наоборот. Это нужно принять как данность. Большинству специалистов по ИБ не удается добиться той роли, которую они считают достаточной.

Грань 2 «Взаимоотношения с бизнесом»

Прежде всего, при построении системы обеспечения информационной безопасности (СОИБ) и системы менеджмента информационной безопасности (СМИБ) важно понимать, что руководители бизнеса и топ-менеджмент мыслят своими понятиями и категориями. Бизнес оперирует своими категориями, а ИБ своими. Если этого не понять, можно породить конфликты, способные свести на нет поставленные цели. По сути, вам придется вникать в потребности всех участников бизнес-процессов и интерпретировать понятия, цели, задачи и возможно, заблуждения бизнеса, для решения задач информационной безопасности. В процессе такой интерпретации необходимо вплетать цели информационной безопасности, и эта работа требует большого терпения и дипломатии. Важно помнить, что демонстрация договороспособности ценнее демонстрации правоты.

Грань 3 «Современный облик службы безопасности»

Современное представление о безопасности подразумевает наличие трех направлений безопасности в компании: Экономической безопасности, Физической безопасности и

Информационной безопасности. Часто подразделение включает в себя Директора по безопасности (CSO) и менеджеров, по каждому из направлений. Забудьте про CISO! Взаимодействием с директорами и владельцами компании будет заниматься CSO, а вы будете взаимодействовать с CSO и руководителями департаментов в той степени и на том уровне, который воспринимается бизнесом.

При построении СМИБ в холдинге или группе компаний, необходимо сформировать роли в отдельных юридических лицах, с которыми будет производиться взаимодействие по вопросам ИТ и ИБ. Часто эти роли представлены одним человеком.

Грань 4 «Взаимоотношения с ИТ»

Современный облик взаимоотношений с департаментом ИТ обусловлен как объективными, так и субъективными факторами.

К объективным относится эволюция технической составляющей систем защиты информации. За последние 10-15 лет, чаша весов склонилась от преобладания навесных средств защиты к встроенным в информационные системы и платформы механизмам контроля и защиты. И если 15 лет назад, подразделение ИБ и ИТ обслуживали преимущественно собственные средства и системы, конкурировали и состязались в полномочиях и бюджетах, то теперь у них общие информационные системы. Исключение составляют инфраструктурные сетевые и специализированные системы защиты. В новой парадигме куда сложнее подготовить специалиста по ИБ, который досконально знает все особенности используемых прикладных информационных систем, чем “натаскать” инженера по прикладным системам по вопросам ИБ и координировать его работу.

К субъективным можно отнести особенности менеджмента конкретной компании, человеческий фактор и восприятие роли ИБ руководством компании и владельцами бизнеса.

Эти факторы определяют новый облик службы ИБ - координирующие, управляющие функции, и комплайнс обеспечивает менеджер по ИБ в связке с руководством ИТ-департамента, а эксплуатацией и выполнением требований занимаются специалисты ИТ подразделений. Исключение составляют специализированные системы контроля и защиты.

Грань 5 «Угрозы и уязвимости»

Всем, кто занимается информационной безопасностью необходимо понять, что не существует никаких угроз информационной безопасности. Существуют только угрозы бизнесу. И работать необходимо исходя из этих реалий. Это помогает понимать роль информационной безопасности для Бизнеса, а не тратить силы на доказывание владельцам бизнеса своей роли. Всякий раз вам необходимо связать какую-либо обнаруженную уязвимость с какой-то угрозой, которую, в свою очередь, связать с угрозой бизнесу.

Когда вы поймете какие угрозы бизнесу воспринимаются как актуальные, вы сможете попробовать построить обратную цепочку, от уязвимостей к актуальным угрозам. Помните, формировать мнение бизнеса об актуальности тех или иных угроз не простая задача.

Грань 6 «Риски»

С рисками та же история, что и с угрозами. Существуют только те риски, которые воспринимает бизнес. Других просто не существует! Начинающие специалисты по информационной безопасности часто упоминают троицу: Конфиденциальность, Целостность Доступность. Со временем, для многих становится

очевидным, что их обучали обеспечивать прежде всего Конфиденциальность, но на практике требуется обеспечивать непрерывность бизнес-процессов и устойчивость функционирования информационных систем.

Оценка рисков приводит к тому, что обеспечение конфиденциальности необходимо только для очень узкого круга информации. Например, финансовой, тендерной, и т.п. Если компания разрабатывает ПО, то разработчикам куда страшнее потерять исходные тексты, документацию и базы, нежели они будут украдены!

При существовании многих методов оценки рисков - все количественные оценки разбиваются или о расчётные формулы, в которых решающее значение имеет субъективный "корректирующий коэффициент", или о необходимость сбора массы данных от производственных, финансовых и управляющих подразделений. Попробуйте обеспечить такой сбор данных, их достоверность и т.п. Вы столкнётесь с жестким противодействием и прослывете негодяем, который всех достал и заставляет выполнять массу никому не нужной работы!

Качественная оценка рисков часто проводится раньше количественной. На ее результаты и особенно оценку этих результатов сильно влияет мнение руководства. После проведения качественной оценки - попробуйте предоставить результаты количественной оценки, отличные от принятых ранее.

Грань 7 «Средства и системы защиты информации»

Системы и средства, обеспечивающие базовые механизмы защиты, формирующие «периметр» и функционирующие на «периметре». Данный класс обеспечивает выполнение правила – все информационные технологии, включённые в периметр, могут

делать что угодно, находиться в любом состоянии внутри периметра, но влияние на них извне и влияние их вовне контролируется. К таким системам и средствам можно отнести межсетевые экраны, защищенные шлюзы и прокси, анти-спам, антивирусы на периметре и т.п.

1. Системы и средства, обеспечивающие базовые механизмы защиты внутри периметра на “системном уровне”. (средства AD, антивирусы, средства архивирования, встроенные механизмы ИС и т.п.)
2. Системы и средства, выполняющие свои функции на “прикладном уровне” (DLP, IPS, WAF, SIEM, IDS и т.п.)
3. Системы и средства поддержки системы менеджмента информационной безопасности. К таким системам и средствам можно отнести системы автоматизации менеджмента рисков, построения моделей, аналитические системы, системы отчётности и т.п.

Тут важно понимать, очерёдность внедрения тоже идёт от первого к четвертому классу. Любая система автоматизирует одно из указанных выше направлений.

При выборе средств и систем защиты выбирайте не те, которые кажутся лучшими на момент выбора, а те, которые долго держатся среди лучших, и есть уверенность что они будут стабильно развиваться и оставаться в лидерах. Опыт показывает, что продукт-лидер в той или иной области - событие временное. Сегодня - лидер, а завтра - разработчик или перестал осуществлять поддержку продукта, или обанкротился, или его купил другой вендор, или …

Необходимо выбирать продукты из группы лидирующих с уверенностью в том, что они будут развиваться, обновляться и осуществлять поддержку. И не забывайте, все системы содержат

уязвимости и недокументированные возможности/недостатки. Часто о них не знают даже поставщики.

При оценке стоимости важно помнить, что система защиты стоит ровно столько, насколько вы её используете! Если вы уверены, что сможете эффективно использовать 20% функций системы - попробуйте договориться о снижении цены или рассмотрите другие средства. Часть функций обеспечивается лицензиями - не набирайте в корзину заказа все сразу. И помните, каким бы красивым не представлялось средство в презентации вендора или поставщика, любое "коробочное" решение через какое-то время становится "ландшафтным". Помните, руководству не нравится увеличение бюджета на информационную безопасность - уменьшение бюджета вызывает еще больше вопросов.

Грань 8 «Вендоры и интеграторы»

С производителями средств и систем защиты информации нужно дружить. Лучше всего наладить общение непосредственно с разработчиками. Разработчикам очень часто не хватает прямого общения с практическими потребителями. Вы всегда сможете организовать "бартер”: вы предоставляете площадку для пилота, формулируете потребности в функционале систем, а получаете продукт "заточенный" под ваши потребности. По этой же причине необходимо стараться приобретать средства и системы непосредственно у производителя или, если это не предусмотрено жесткой политикой вендора, всегда советоваться с вендором при выборе поставщика.

Не могу рассказать, как осуществляются продажи средств и систем защиты информации (зато знаю к кому обращаться за советом), но приобретение редко происходит без опроса друзей и знакомых по отрасли. Часто совет коллеги имеет

определяющее значение по отношению к маркетингу производителей или поставщиков. Нужно отметить, что за последние годы, в отрасли сформировалось некое доверительное сообщество специалистов, которое оказывает значительное влияние на выбор тех или иных средств, систем и услуг. Формирование репутации в этом сообществе очень важно не только для специалистов, но для всех участников этого рынка.

Грань 9 «Стандарты и требования регуляторов»

Стандарты, требования, рекомендации, лучшие практики. Их внедрение и применение всегда проводится через призму конкретных условий применения и тщательную адаптацию к реальным условиям. Какими бы строгими не были требования, они никогда не смогут учесть все тонкости и особенности конкретной компании.

При формировании СМИБ и СОИБ важно не ударяться в крайности. Кто знает, до каких состояний на предприятиях доводили системы менеджмента качества, поймет меня. Формируйте те документы, которые будут применяться. Всегда смело адаптируйте стандарты и рекомендации к особенностям вашей компании. Просите у друзей и коллег поделиться их наработками и делитесь сами!

Грань 10 «Интерпретатор»

Каждый сотрудник на своей позиции в компании видит только часть общего. Нет человека, который видит все. Это относится к любым процессам и активам компании. По сути, любая информационная система или процесс отражается частично в различных видах деятельности. Бухгалтер видит вашу систему в финансовой плоскости, администратор системного отдела департамента ИТ в технической плоскости, эксплуатант в прикладной, специалист отвечающий за сетевую инфраструктуру

в виде используемых узлов, адресов и каналов, а потребитель отчетов вообще про нее ничего не слышал.

Проблемы использования всех информационных систем, ИТ и сетевой инфраструктур так же воспринимаются по-разному. Это необходимо учитывать. Так как специалистам по ИБ часто приходится иметь дело с проблемами, а точнее с людьми, воспринимающими эти проблемы по-своему, то и решения этих проблем лежат на всех уровнях восприятия. Как я уже указывал выше, вам придется интерпретировать и вплетать вопросы ИБ во все бизнес-процессы компании. Хочу пожелать Вам удачи в этом не простом деле.

Грань 11 «Учет и контроль»

Есть мнение, что защитить канал или систему куда проще, чем их контролировать. И это действительно так! С точки зрения информационной безопасности, порядок задач по отношению к защищаемой инфраструктуре должен быть следующий: знать предмет, контролировать предмет, защищать предмет, влиять на предмет или его состояние.

Контроль ИТ-инфраструктуры позволяет накапливать такой уровень знаний, который позволяет формировать очевидные решения по защите. Необходимо отметить, что в половине случаев, решения по изменению архитектуры или порядку взаимодействия, или применения конкретной информационной системы влияют на защищенность информации больше, нежели закупка и внедрение дополнительных дорогостоящих средств защиты.

Грань 12 «Аутсорсинг»

Старайтесь переводить на аутсорсинг все инфраструктурные проекты и информационные системы. Причина такого решения - просто дешевле! Вы можете взять в штат специалистов, но

соотношение полезной нагрузки и фонда оплаты труда окажется очевидно не эффективным. Компании, занимающиеся обслуживанием, как правило, обладают значительным опытом и классными инженерами, специализирующимися на обслуживании систем подобным вашим. К тому же, уволить своего сотрудника сложнее, чем приостановить действие договора на обслуживание. Так же, в некоторых случаях, вы сможете отказаться от прямой технической поддержки вендора и воспользоваться правами и средствами аудита и мониторинга нанятой компании по оказанию таких услуг.

Конечно, речь не идет об эксплуатации специальных систем, которые должны эксплуатироваться собственными специалистами по ИБ. Хотя обслуживание таких систем тоже можно передать на аутсорсинг.

Грань 13 «Это Вы сами»

Роль личности всегда была высока. Какие бы технические средства не применялись, они не могут функционировать самостоятельно, без специалистов и не способны охватить все сферы деятельности компании. Эффективность защиты зависит прежде всего от человека, и заменить специалиста по информационной безопасности попросту нечем! Необходимо формировать репутацию и демонстрировать доверие в компании и отрасли.