Шаханова М.В., Швец Е.Е., Шаханова Д.С. Обеспечение информационной безопасности на предприятии // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 97–103

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

[1]Шаханова М.В., Швец Е.Е., Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

Безопасность бизнес-информации является важнейшей задачей управления предприятием при управлении рисками. Современная эра технологической безопасности для бизнеса получает все большее признание, особенно в бизнес-стратегиях. Разъединение процедур информационной безопасности и коммерческих стратегических бизнес-целей для контроля расходов на безопасность и связанных с ними рисков, инцидентов и убытков. Операционная корпоративная система требует согласования методов обеспечения безопасности путем внедрения управления рисками информационной безопасности в организацию, однако она сталкивается с серьезными проблемами, связанными с поддержкой и запуском бизнеса. Выравнивание безопасности в бизнес-процессе — одна из самых больших проблем в хорошей организации, поскольку она требует вспомогательных ресурсов и управления временем, а также способов согласования безопасности для достижения бизнес-целей. Таким образом, роль управления информационной безопасностью важна как руководство по обеспечению безопасности деловой информации. Кроме того, систематическое управление безопасностью представляет собой бизнес-модель для защиты критической информационной инфраструктуры. Структура и стратегия организации, люди, процессы и технологии — элементы модели, которые играют эффективную роль в обеспечении информационной безопасности, но для этого требуется баланс между ними.

Ключевые слова: информационная безопасность бизнеса, управление рисками информационной безопасности, управление информационной безопасностью (ISM), information security serves for business.

ENSURING INFORMATION SECURITY AT THE ENTERPRISE

[1]Shakhanova M. V., Shvets E.E., Shakhanova D.S.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

The security of business information is the most important task of enterprise management in risk management. The modern era of technological security for business is becoming increasingly recognized, especially in business strategies. Separation of information security procedures and commercial strategic business objectives to control security costs and related risks, incidents and losses. The operational corporate system requires the coordination of security methods by implementing information security risk management in the organization, but it faces serious problems related to the support and launch of the business. Aligning security in a business process is one of the biggest challenges in a good organization, as it requires support resources and time management, as well as ways to align security to achieve business goals. Thus, the role of information security management is important as a guide to ensuring the security of business information. In addition, systematic security management is a business model for protecting critical information infrastructure. The structure and strategy of the organization, people, processes and technologies are elements of the model that play an effective role in ensuring information security, but this requires a balance between them.

Keywords: business information security, information security risk management, information security management (ISM), information security serves for business.

В настоящее время важность информационной безопасности в корпоративной среде имеет огромное значение. Информационная безопасность стала более важной для большинства организаций при принятии мер по снижению рисков. Деятельность по защите бизнеса должна быть первым и главным достижением любой программы безопасности. Эта точка зрения была поддержана специалистами по безопасности, подходами к обеспечению безопасности и используемыми государственными процессами. Призвание к информационной безопасности выросло из профессии проверки, групп соответствия и регулирования, а также агентств общественной безопасности, которые имеют профессию как безопасность, ориентированную на риски. Из-за некоторых проблем несколько предприятий не сделали это основной компетенцией. Это связано с тем, что ограничение организации должно открыть для некоторых организаций понимание важности их безопасности для достижения жизненно важных бизнес-целей и активного вовлечения заинтересованных сторон бизнеса в проблему безопасности. В результате она превратилась в развязанную программу, вялую и во многом безуспешную. Таким образом, есть много организаций, которые должны бороться, чтобы достичь решающего выравнивания. Согласование программ безопасности с предприятием требует глубокого понимания технической области, например, того, как различные вычислительные технологии позиционируются на предприятии и их значения для бизнеса, а также того, как конкретная защита поддерживает конкретные цели бизнес-стратегии.

Информационная безопасность в соответствии с управлением предприятием

Интересно отметить, что большая часть организаций использует подход, ориентированный на риски, для обеспечения безопасности и инвестиций. В основном риск может возникать из-за уязвимостей, угроз и связанных с ними рисков. Стратегия Business Security дает лучшие результаты по сравнению ориентированной на риски за счет использования подхода.

Однако существует предел того, какую защиту может предложить ИТ-отдел без комплексного бизнес-подхода — лучший в мире брандмауэр не помешает сотрудникам отправлять критически важные данные за пределы организации. Таким образом, роль ISM (управление информационной безопасностью) заключается в поддержке и управлении бизнес-деятельностью. Например, бизнес-анализ дает обслуживание анализа рисков информационной безопасности. Глубокое знание предприятия необходимо для поддержки настройки лучших руководств по упражнению в подходящем и эффективном исполнении, которое будет «принимать» в этой конкретной среде, культуре, бизнесе и организационной структуре. Менеджеры по информационной безопасности должны осознавать жизненный цикл информационных активов организации и планы на будущее, а бизнес-риски необходимо измерять, чтобы удостовериться, что риски оцениваются и должным образом снижаются на каждом этапе жизненного цикла. Чем успешнее это будет сделано, тем больше вероятность того, что функция ISM будет признана законной для предоставления ценности предприятию. Кроме того, должны быть разработаны политика ISM и ISMS (система управления информационной безопасностью), чтобы обеспечить защиту данных на всех этапах.

Чтобы достичь четкого и эффективного набора методов ISM, организация должна выполнить следующие шаги [1]:

1. знать политику и планы безопасности бизнеса;

2. понимание текущих и будущих требований безопасности бизнеса;
3. документирование всех мер безопасности и их работу, техническое обслуживание и связанные с ними риски;
4. управление всеми нарушениями безопасности и происшествиями;
5. управление поставщиками и контрактами в отношении доступа к системам и услугам в сочетании с функцией управления;
6. упреждающее улучшение средств контроля безопасности и управления рисками безопасности.

Проблемматика

Проблема информационной безопасности характеризуется сложностью и взаимозависимостью. Что содержит значительное количество факторов и элементов, которые взаимосвязаны друг с другом. Присутствие человеческого фактора еще больше усложняет ситуацию, поскольку люди обладают свободой воли и всегда будут действовать в своих интересах. Более того, растущая зависимость от Интернета практически во всех сферах деловой активности делает безопасность серьезной проблемой для многих заинтересованных сторон (частных лиц, предприятий, правительств и т. д.).

Существенным элементом любой системы защиты информации являются затраты, связанные с ее проектированием, разработкой, внедрением и выводом из эксплуатации. Необходимы значительные инвестиции для создания и обслуживания высоконадежных, быстро реагирующих и заслуживающих доверия систем информационной безопасности. Хотя очень немногие будут утверждать, что информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах, не сопряжена со значительными рисками, доводы в пользу инвестиций в надлежащие меры безопасности по-прежнему трудно обосновать. Можно утверждать, что основной причиной уделения информационной безопасности приоритетного внимания в повестке дня корпораций в последнее десятилетие были повышенные и строгие требования к соблюдению нормативных требований, предъявляемые к коммерческим организациям. Кроме того, крупный бизнес развил разумное понимание последствий плохой защиты информационных систем. Следовательно, большая часть бизнес-бюджетов была выделена на улучшение защиты корпоративных цифровых активов.

Хотя эти инвестиции и инициативы, безусловно, уменьшат угрозы, исходящие от современного электронного рынка, другие аспекты проблемы остаются в значительной степени нерешенными. Сложность и взаимозависимость проблем безопасности в Интернете серьезно ограничивают эффективность любой инициативы, предпринятой в конкретных организационных или географических контекстах.

Из-за серьезного отсутствия осведомленности о негативных последствиях проблем и угроз информационной безопасности среди малых и средних предприятий (МСП), в дополнение к восприятию менее строгих нормативных требований и очень высоких относительных затрат на защиту цифровой информации, информационные и коммуникационные инфраструктуры этих фирм остаются крайне незащищенными и уязвимыми.

Взаимосвязанность становится все более важным требованием для делового общения. Крупные организации полагаются на услуги, предоставляемые множеством более мелких партнеров и подрядчиков, расположенных за пределами географических границ. Этим более

мелким фирмам следует предоставить определенные уровни доступа к информационным системам крупных организаций для выполнения своих деловых контрактов. Получая доступ к информационным системам организации, партнеры и подрядчики фактически становятся частью корпоративной сети. Учитывая возможность возникновения угроз безопасности и атак с любой машины, подключенной к глобальной сети, малые и средние предприятия выступают в роли «самого слабого звена» в сети. Самое слабое звено в любой сети является привлекательной точкой входа для злоумышленников, желающих взломать систему, и любая сеть так же безопасна, как и ее самое слабое звено. Это означает, что для надлежащей защиты глобальной сети Интернет необходимо применять более целостный подход, уделяя особое внимание самому слабому звену: МСП.

Проблема информационной безопасности в МСП не может быть решена только за счет повышения осведомленности о серьезности ее последствий. Однако многие другие факторы еще больше усложняют ситуацию; и призыв к немедленным действиям жизненно важен. Даже при соответствующей осведомленности и полном понимании вопросов безопасности МСП не обладают необходимыми ресурсами (человеческими, денежными или техническими), которые следует инвестировать для решения проблемы. МСП обычно работают в условиях очень ограниченного бюджета; имеют серьезно ограниченную рабочую силу, и многие потребности конкурируют за очень ограниченный запас ресурсов, что приводит к тому, что информационная безопасность отодвигается на второй план в списке приоритетов. Здесь действует цикл отрицательной обратной связи: меньшая осведомленность о проблеме информационной безопасности отодвигает ее вниз по списку приоритетов, что, в свою очередь, уменьшает выделяемые на нее ресурсы, что приводит к еще более низкой осведомленности (рисунок 1).

Рисунок 1 – Цикл отрицательной обратной связи в отношении осведомленности об информационной безопасности в МСП

Хотя вышеупомянутые проблемы обычно не возникают в контексте крупных организаций, они, безусловно, оказывают существенное влияние на проблему безопасности внутри этих фирм. Взаимосвязанность Интернета подразумевает, что, хотя эти проблемы могут быть связаны с небольшими предприятиями, они также оказывают существенное влияние на другие организации. Большинство инициатив, начатых с целью повышения информационной безопасности в крупных организациях, имели локальный характер, предполагая, что развитие общекорпоративной инфраструктуры безопасности информации и связи повысит статус безопасности во всей организации. Это предположение игнорирует тот важный факт, что электронные атаки и угрозы безопасности могут исходить из любой точки земного шара. Повышенная защита периметра корпоративной сети больше не является эффективным вариантом из-за необходимости трансграничной связи и совместной работы. К безопасности следует подходить с комплексной точки зрения, учитывающей взаимозависимый и взаимосвязанный характер современных глобальных коммуникаций.

Кроме того, из-за серьезной нехватки квалифицированных технических специалистов и опыта информационная безопасность обычно воспринимается как высокая стоимость, которая должна быть достаточно хорошо обоснована, чтобы ее можно было продолжать. Крупные и многонациональные организации и конгломераты изо всех сил пытаются добиться одобрения и распределения своих собственных бюджетов на безопасность, даже несмотря на то, что дело, которое они приводят, весьма привлекательно. При такой предполагаемой высокой стоимости безопасности она будет чрезмерной

Целостный подход к информационной безопасности

Было разработано несколько методологий и стандартов для решения все более важных вопросов информационной безопасности (примеры включают CRAMM [2] и ISO17799 [3]).

Перед разработкой любой системы управления информационной безопасностью необходимо четко определить и сформулировать предполагаемые цели системы. На данном этапе важно признать изменяющуюся бизнес-среду, в которой обычно работают МСП. Это потребует адаптации целей безопасности в соответствии с новыми бизнес-требованиями. Таким образом, гибкость в определении и переопределении целей с минимальными требованиями к ресурсам имеет решающее значение для успеха предлагаемого подхода. Чтобы четко и однозначно определить требования, мы предлагаем использовать методологию мягких систем (SSM). SSM был предложен Питером Чеклендом [4] как «общий подход к решению проблем, подходящий для систем человеческой деятельности» (см. рисунок 2).

Управление безопасностью всегда следует воспринимать как непрерывный процесс. В условиях современного динамичного рынка уже недостаточно внедрять отличные меры безопасности без оценки изменений в бизнес-среде и требованиях. Особенно это касается малых и средних предприятий. Небольшие организации гораздо более гибкие, чем их более крупные коллеги, и они обычно извлекают выгоду из этой гибкости, чтобы выходить на различные рынки и адаптировать методы ведения своего бизнеса.

Последний этап связан с изменением характера деловой среды. Он направлен на адаптацию реализации СМИБ [5] для реагирования на изменения бизнес-требований. Когда какое-либо серьезное изменение требует значительного изменения в СУИБ компании, можно использовать тот же процесс, описанный выше, чтобы адаптировать решение для удовлетворения новых потребностей.

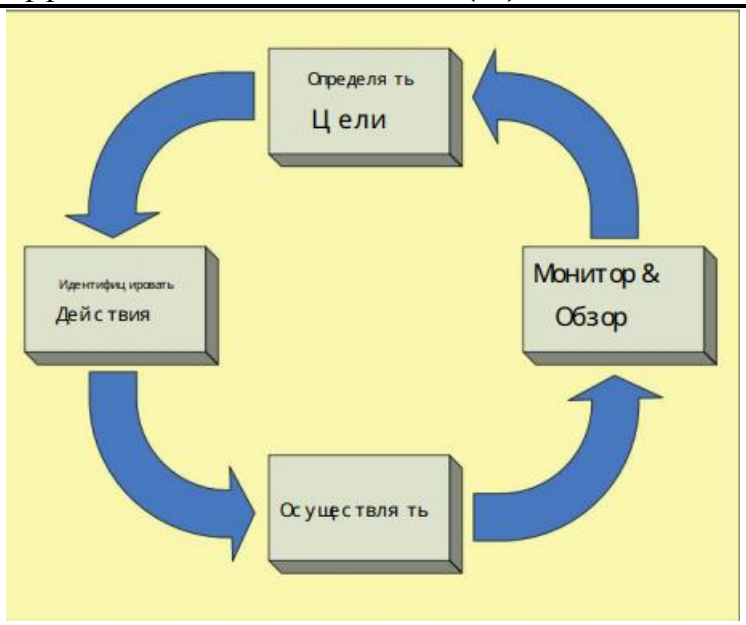

Рисунок 2 – Четыре этапа процесса управления безопасностью малого и среднего бизнеса

Выводы

Большое внимание уделяется проблеме защиты цифровой информации на современном технологическом рынке. Информация, собираемая, хранящаяся, обрабатываемая и передаваемая организациями, может быть очень конфиденциальной и повлечь за собой серьезные негативные последствия, если ее целостность, конфиденциальность или доступность будут нарушены. Организации любого размера должны проявлять должное усердие в защите информации, которой они располагают. В то время как крупные организации вложили разумные средства в повышение стандартов информационной безопасности в своей деятельности, малые и средние предприятия сталкиваются со многими проблемами в достижении повышенных уровней безопасности.

В этой статье представлены некоторые проблемы, препятствующие развитию информационной безопасности в МСП. Эти проблемы включают, но не ограничиваются ограниченными бюджетами, ограниченными человеческими ресурсами и постоянно меняющейся бизнес-средой. Был предложен целостный подход к управлению информационной безопасностью на малых и средних предприятиях, основанный на методологии мягких систем, который признает и решает эти проблемы. Этот структурированный подход включает четыре этапа: определение целей безопасности предприятия, определение действий, осуществление действий, а также мониторинг и анализ реализации безопасности.

Список литературы

1. Бэйси фон Солмс, «Управление информационной безопасностью и соответствием требованиям по сравнению с операционным управлением», Компьютеры и безопасность, 24, Elsevier, стр. 443-447, 2005.
2. Инструментарий управления рисками CRAMM. http://www.cramm.com
3. ISO17799 Информационные технологии. Методы обеспечения безопасности. Свод практических правил по обеспечению информационной безопасности

4. Checkland, P. (1999) Системное мышление, системная практика. Уайли, Западный Суссекс, ВЕЛИКОБРИТАНИЯ.
5. Институт защиты информационной инфраструктуры (I3P) (2003 г.), Программа исследований и разработок в области кибербезопасности.

References

1. Basie von Solms, "Information Security and Compliance Management Versus Operational Management", Computers and Security, 24, Elsevier, pp. 443-447, 2005.
2. CRAMM risk management tools. http://www.cramm.com
3. ISO17799 Information technology. Security methods. Code of Practice for Information Security
4. Checkland, P. (1999) Systems thinking, systems practice. Wylie, West Sussex, UK.
5. Institute for Information Infrastructure Protection (I3P) (2003), Cybersecurity Research and Development Program..