УДК 338.242.2

Корпоративное управление информационной безопасностью

Финягина Я.Д.
Студент департамента корпоративных финансов
и корпоративного управления Финансового университета
при Правительстве РФ (Москва)

Юсупов Р.Г.
Студент департамента корпоративных финансов
и корпоративного управления Финансового университета
при Правительстве РФ (Москва)

Эффективное управление информационной безопасностью в настоящее время стало императивом бизнеса. В статье рассматривается система менеджмента информационной безопасности организации как непрерывного процесса управления. Представлены уровни корпоративной информационной системы, подходы к выделению информационных активов, пути формирования эффективной коммуникации в структуре организации в целях информационной безопасности. Рассматриваются задачи формирования бюджета на проведение мероприятий информационной безопасности.

Ключевые слова: информационная безопасность, информационные активы, политика информационной безопасностью.

В настоящее время наблюдается существенное повышение роли информационных активов в деятельности организации, что обусловлено информационными характеристиками современного бизнеса. В то же время информационная сфера является одним из главных источников рисков бизнеса. Обеспечение информационной безопасности является одним из ключевых факторов успеха для всех бизнес-процессов в деятельности организации.

Формирование эффективной системы корпоративного управления информационной безопасностью связано с материальными и трудовыми затратами. Решение задач информационной безопасности не находится в жесткой зависимости от процесса извлечения прибыли, и соответственно, финансирование этого направления, как правило, осуществляется по остаточному принципу. В то же время нарушение целостности информационной системы может привести к потере информации о корпоративных разработках, данных клиентов или стратегических бизнес-планах и в конечном итоге к утрате доверия клиентов, прибыльности деятельности.

Существующие международные технические стандарты доступны в качестве руководящих принципов для управления информационной безопасностью. Однако создание практической модели управления процессами информационной безопасности в системе менеджмента организации вызывает большое количество вопросов.

Международный стандарт по информационной безопасности, разработанный Международной комиссией по стандартизации (International Organization for Standardization, ISO) совместно с Международной электротехнической комиссией (International Electrotechnical Commission, IEC), ISO/IEC 27001 дает определение информационной безопасности как «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность» [1].

В свою очередь Стандарт Банка России СТО БР ИББС-1.0-2014 определяет информационную безопасность как «безопасность, связанную с угрозами в информационной сфере» [2].

Обеспечение информационной безопасности в организации является неотъемлемой частью общей системы управления, включающей в себя организационную структуру, стратегию, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы [3].

Непосредственно система менеджмента информационной безопасности (далее – ИБ) – это часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности. Уровень сложности системы зависит от структурной сложности самой организации.

Непосредственно управление ИБ связано с обеспечением непрерывности бизнеса и минимизацией ущерба для бизнеса путем предотвращения и минимизации последствий инцидентов безопасности, которые угрожают информационным активам организации.

Корпоративную информационную систему можно определить как систему, состоящую из средств автоматизации, информации и персонала. Исходя из этого, структурно в ней можно выделить такие уровни, как технические средства, программное обеспечение, информационные ресурсы и организационные структуры (отделы, сотрудники и т.д.) [4].

Для всех уровней корпоративной информационной системы в целях ИБ должны быть реализованы как минимум три основных компонента:

1. Конфиденциальность – защита уязвимой информации от несанкционированного разглашения или попыток ее раскрытия;
2. Целостность как сохранение точности и полноты информации и программного обеспечения;
3. Доступность, т.е. обеспечение того, чтобы информация и услуги были доступны пользователям [5].

В Британском стандарте норм поведения для информационной безопасности системы управления (BS 7799) выделены десять ключевых элементов управления, которые определяют минимальные требования для любой организации. К ним относятся:

1. Политика информационной безопасности, указывающая цели ИБ.
2. Распределение обязанностей в области ИБ.
3. Программы обучения и подготовки в области ИБ для всего персонала.
4. Отчетность об инцидентах, связанных с ИБ, обеспечивающая осведомленность сотрудников.
5. Средства контроля, используемые для обнаружения и предотвращения угроз.
6. Планирование непрерывности бизнеса, выявление рисков для бизнес-операций и разработка планов по обеспечению непрерывности критически важных бизнес-процессов в случае катастрофы.
7. Управление копированием программного обеспечения.
8. Охрана организационных документов для защиты их от утраты, разрушения и фальсификация.
9. Защита данных.
10. Соблюдение политики безопасности.

Важным элементом управления ИБ является политика информационной безопасности. К главной цели политики информационной безопасности относится обеспечение устойчивого функционирования организации и защита информационных ресурсов от случайных и направленных противоправных действий.

В свою очередь, к задачам информационной политики относится:

– формирование целостного представления об ИБ и взаимосвязь ее с другими элементами системы безопасности организации;

– определение путей реализации мероприятий, обеспечивающих необходимый уровень ИБ.

В организации должны быть выделены информационные активы, существенные для обеспечения непрерывности бизнеса.

Непосредственно к объектам ИБ, подлежащим защите, относятся:

– информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, а также акустическая (речевая) информация;

– сведения, ставшие известными сотрудникам организации в процессе исполнения ими своих должностных обязанностей;

– средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телефонной, факсимильной, радиосвязи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

– технические средства и системы защиты информационных ресурсов и служебные помещения, в которых хранится и обрабатывается информация ограниченного доступа.

В конкретной организации состав информационных активов определяется в соответствии с принятыми в организации подходами к их классификации и уровнем детализации типов информационных активов. При этом права доступа работников и клиентов к информационным активам организации должны быть зафиксированы документально. Кроме того, в документах организации должны быть определены, утверждены и прописаны процедуры идентификации, аутентификации и авторизации.

Защита каждой части данных является громоздкой и, по сути, неэффективной. Организация должна классифицировать свои данные на основе важности, создавать архитектуру безопасности и устанавливать политику безопасности и меры защиты для каждого из этих уровней. Это связано не только с оценкой типа данных и содержимого, но также с тем, кто имеет доступ к данным и типу проверки подлинности, необходимой для просмотра данных.

Классификация и защита данных также требует понимания типа и источника угроз, с которыми сталкиваются организации. Типичные атаки нацелены почти на все данные организации и являются обычным явлением, от большинства этих атак обычно существующие меры безопасности организации обладают достаточно высоким уровнем защиты. С другой стороны, целенаправленные атаки обладают персонифицированной избирательностью и зачастую направлены на определенный тип данных. И в случае успешности такие нападения могут повлечь негативные последствия для деятельности организации. Здесь важно понять мотивы таких атак, чтобы их можно было предотвратить и также не допустить нарушения ИБ в будущем.

Для реализации мер по эффективной защите информации в организации необходимо полное взаимодействие между подразделениями организации. В свою очередь, все функции, связанные с безопасностью ИБ, должны находиться под руководством подразделения ИБ в целях обеспечения надлежащего мониторинга вопросов безопасности и управления рисками в соответствии с бизнес-целями. Подразделение ИБ должно выступать в роли координационного центра по вопросам ИБ и вместе с исполнительными органами организации обеспечивать достижение целей безопасности для бизнеса. Подразделение ИБ несет ответственность за программу ИБ и обеспечивает фокусность и стратегическое присутствие для достижения ее видения и миссии.

Наиболее успешная форма внутреннего корпоративного взаимодействия в части ИБ, когда подразделение ИБ отчитывается напрямую члену исполнительного органа компании. ИБ должна рассматриваться как приоритетная по отношению к другим направлениям корпоративного управления.

Подразделение ИБ, по сути, является внутренним поставщиком услуг. Подобно управлению услугами подразделением информационных технологий, отдел ИБ может создать каталог услуг, который отвечает потребностям отдельных бизнес-подразделений.

Примерный список таких услуг может включать:

- обеспечение безопасной среды для бизнес-приложений, управляющих строго конфиденциальными данными;
- аудит безопасности третьей стороны;
- консультации по вопросам безопасности и поддержки бизнес-проектов;
- выполнение цикла ежегодных систем управления информационной безопасностью: анализ риска, мер и планирования внедрения;
- обеспечение доступа к публичным сервисам;
- анализ проникновения и анализ влияния на бизнес;
- кампании по повышению информированности и обучение персонала.

По своей сути, ИБ является расширением бизнеса, а отдел ИБ должен предоставлять услуги безопасности, относящиеся к бизнесу. Одним из способов достижения этого является работа в качестве интегратора услуг.

Настройка ИБ в качестве центра организации означает, что затраты на ИБ должны распределяться отдельно, а не совмещаться с корпоративными накладными расходами. Когда эти услуги появятся в бюджете каждого бизнес-отдела, то, помимо прозрачности, будут более эффективно использоваться ресурсы организации.

Такой подход к формированию затрат особенно важен при рассмотрении вопроса о стоимости, основанной на уровне риска и ограничении ответственности.

Для создания системы ИБ организации необходимо согласовать цели своей ИБ со своей бизнес-стратегией, целями и ценностью в условиях риска, а затем создать прочную и целостную стратегию ИБ с четкой и общей дорожной картой. Эта стратегическая дорожная карта и поддерживающий ее бюджет должны регулярно обновляться в ответ на угрозы и изменения в бизнес-среде. Когда потребности в ИБ сформированы в формате финансовых затрат, исполнительные органы организации и бизнес-подразделения более склонны обращать на это внимание.

Создание бюджета для поддержания и улучшения возможностей ИБ является достаточной сложной задачей. Большинство отделов ИБ работают в условиях жестких финансовых ограничений. Будущие потребности в финансовых ресурсах неопределенны: каждый год появляются новые угрозы и уязвимости, новые технологии и часто новые нормативные требования. Организациям необходимо здесь искать баланс между перерасходом и недорасходованием в контексте потенциальных угроз нарушения целостности ИБ.

При планировании бюджета затрат для поддержания системы ИБ необходимо сформировать разделы бюджета по трем направлениям:

1. Бюджет текущих затрат, который должен быть рассчитан непосредственно на цели отдела ИБ и для решения задач в различных областях: от оперативной деятельности до управления рисками.

2. Бюджет для отдела информационных технологий либо для одного из бизнес-подразделений, где должны быть отражены дополнительные затраты на реализацию мероприятий по развитию ИБ. Например, для разработки новых приложений или затраты на средства управления ИБ в бизнес-процессах.

3. Бюджет для минимизации последствий в случае нарушения ИБ.

Также важно отделить бюджет внутренней ИБ от бюджетов, связанных с защитой информации о продукте организации. Как правило, многие организации определяют на эти цели примерно 5 % бюджета от бюджета на информационные технологии, что не совсем корректно. Когда бюджеты отделены, появляется более ясная информация о ролях информационных технологий и ИБ.

Планируемый бюджет дополнительно должен разделяться на меры по подготовке, профилактике, выявлению и реагированию, при этом больший упор необходимо делать на раннее выявление и смягчение последствий. Бюджет должен обновляться ежегодно с возможными корректировками в середине года, обусловленными непредвиденными событиями, а не просто прогнозируемыми, а также с учетом финансового воздействия прошлых инцидентов и предыдущих инвестиций в систему безопасности, изменений потенциальных угроз и мер новой защиты.

Для расчета объема бюджета целесообразно использовать модель Гордона–Лоэба (*Gordon–Loeb model*), представляющую собой обобщенную модель оценки уменьшения уязвимости системы как результат увеличения инвестиций в информационную безопасность [6].

Данная модель показывает, что в целом экономически нецелесообразно инвестировать в мероприятия по ИБ более 37 % ожидаемого ущерба, который может возникнуть в результате нарушения безопасности. Ожидаемый убыток рассчитывается исходя из ценности риска и вероятности материализации риска.

Модель Гордона-Лоэба является одной из наиболее общепринятых аналитических моделей в экономике ИБ.

Также в целях оценки готовности системы ИБ к отражению угроз организации необходимо проводить стресс-тестирование для оценки их потенциального воздействия. Такие тесты могут помочь выявить пробелы в возможностях ИБ и послужить основой для плана восстановления, включая изменения в политике, технологиях или даже командных ролях и обязанностях.

Конкретный способ стресс-тестирования инфраструктуры ИБ – это тестирование на проникновение, в котором используются реалистичные сценарии атак и уязвимости, как технические, так и нетехнические. Результаты дают четкое представление о том, где инвестиции могут оказать немедленное воздействие. Оптимальное количество тестов на проникновение варьируется в зависимости от таких факторов, как сфера деятельности организации, ее размер, количество и тип обрабатываемой информации. Это позволяет организациям выявлять недостатки ИБ в разных функциональных областях и исправлять их, оценивать состояние всей системы ИБ в целом.

Но наиболее уязвимый аспект управления информационной безопасностью в организации – это человеческий ресурс. Человеческие отношения и поведение, которые являются отражением организационной культуры, являются критическим элементом корпоративной ИБ.

Процессы ИБ часто могут непреднамеренно вмешиваться в бизнес-процессы, что в свою очередь влияет на анализ угроз и анализ рабочего процесса. Чтобы привлекать сотрудников как активных участников ИБ, организации необходимо изменить восприятие мер безопасности с позиции препятствия бизнеса. Кроме того, осведомленность отдельных сотрудников, которые вовлечены в обработку конфиденциальной корпоративной информации, является основополагающей для управления ИБ. Организации необходимо обеспечить регулярное образование для всех сотрудников относительно важности конфиденциального управления корпоративной информацией.

Изменение восприятия сотрудников способствует повышению приверженности к культуре ИБ на оперативном уровне и, следовательно, повышению эффективности ИБ.

Таким образом, поддержание на высоком уровне ИБ является непрерывным процессом. Система менеджмента информационной безопасности ставит задачи комплексного подхода к формированию мероприятий по обеспечению организации информационной безопасности. Налаженная система управления ИБ позволяет организациям легко реагировать на постоянно меняющуюся операционную среду. Контроль за ИБ должен быть экономичным и сосредоточен на соответствующих процессах. Хорошо внедренная система ИБ также позволяет организации контролировать состояние ключевых элементов управления и тем самым повышать уровень безопасности.

Литература:

1. Стандарт ISO/IEC 27001. – URL: http://www.rusregister.ru (Дата обращения: 15.05.2017).
2. Распоряжение Банка России от 17.05. 2014 г. № Р-399 «Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности банковской системы Российской Федерации. Общие Положения» – URL: http://www.cbr.ru (Дата обращения: 14.05.2017).
3. Приказ Ростехрегулирования от 27.12.2006 г. № 375-ст ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // СКС «КонсультантПлюс».
4. Нечунаев В.М. Методика описания корпоративной информационной системы для процедуры управления рисками информационной безопасности. // Технические науки. Доклады ТУСУР. – 2008. – № 2-1. – С. 116-117.
5. BS 7799 Part 1 // Code of Practice for Information Security Management («Практические правила управления информационной безопасностью)». – URL: http://www./iso-management.com (Дата обращения: 15.05.2017).
6. Собакин И.Б. Анализ подходов к определению оптимального объема инвестиций в информационную безопасность. // Труды Института системного анализа РАН. – 2012. – № 3 (Т. 62). – С. 63-38.

Corporate Management of Information Security

Ya.D. Finyagina, R.G. Yusupov
Financial University under the Government of the Russian Federation

Effective management of information security nowadays has become a business imperative. The article discusses the management system of information security of the organization as a continuous management process. It presents levels of the corporate information system, approaches to the allocation of information assets, formation of effective communication within the organization for information security purposes. The authors consider the problems of budgeting for information security operations.

Key words: information security, information assets, information security policy.

◆