УДК 338.27

СОВРЕМЕННЫЕ ПОДХОДЫ К УПРАВЛЕНИЮ ИНФОРМАЦИОННЫМИ РИСКАМИ

Николаева А. А., Неизвестный А.А.,
научный руководитель доцент Данилова Л.В.
Сибирский федеральный университет

Процесс принятия решений в экономике на всех уровнях управления происходит в условиях постоянно присутствующей неопределенности состояния внешней и внутренней среды, которая обуславливает частичную или полную неопределенность конечных результатов деятельности. В экономике под неопределенностью понимается неполнота или неточность информации об условиях хозяйственной деятельности, в том числе о связанных с ней затратах и полученных результатах. Причинами неопределенности являются три основных фактора: незнание, случайность и противодействие.

Существование риска непосредственно связано с неопределенностью. Риск является одним из способов снятия неопределенности, которая представляет собой незнание достоверного, отсутствие однозначности. Акцентировать внимание на этом свойстве риска важно в связи с тем, что оптимизировать на практике управление и регулирование, игнорируя объективные и субъективные источники неопределенности, бесперспективно.

Управление рисками − процесс принятия и выполнения управленческих решений, направленных на снижение вероятности возникновения неблагоприятного результата и минимизацию возможных потерь, вызванных его реализацией.

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации.

На данный момент, российскими компаниями значительное внимание в управлении информационными рисками уделяется анализу преимуществ и недостатков, известных аппаратных и программных средств и технологий защиты информации. В меньшей степени внимание затрагивает вопросы и меры организационного обеспечения информационной безопасности компаний, такие как концепция и политика безопасности, стратегия и тактика защиты информации, планы защиты информационных ресурсов компании в штатных и внештатных условиях функционирования информационных систем.

Информационные риски − это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий. IT-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи.

Информационные риски можно разделить на следующие категории:

1. Внешнее мошенничество: незаконное проникновение в информационные системы, посредством сети интернет (хакерские атаки); причинение ущерба информационным системам; кража информации, повлекшая денежные потери.
2. Внутреннее мошенничество: несанкционированное использование информационных систем; преднамеренное искажение (сокрытие или раскрытие) важной информации, повлекшее денежные потери.
3. Клиенты, продукты и ведение бизнеса: связанное с недостаточностью систем; неправомерное раскрытие конфиденциальной информации.

4. Ущерб материальным активам: ущерб информационным системам в результате воздействия внешних неконтролируемых событий; ущерб в результате актов вандализма, терроризма.

5. Остановка бизнеса и сбои в системах: выход из строя информационных систем, отдельных модулей и элементов функционала; сбои в работе каналов связи; поломка оборудования.

6. Проблемы с управлением и исполнением операций: отсутствие или несовершенство системы защиты или порядка контроля доступа к информации; неправильная организация информационных потоков внутри организации; невыполнение обязательств перед организацией поставщиками, провайдерами; ошибки при вводе и обработке данных; ошибки в работе информационных систем.

Оценка рисков − первый этап в управлении системы информационной безопасности, предназначенный для идентификации источников рисков и определения его уровня значимости. Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом:

1. Идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса.
2. Оценивание возможных угроз.
3. Оценивание существующих уязвимостей.
4. Оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для бизнеса уязвимые информационные ресурсы компании подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризуют опасность, которая может угрожать компонентам корпоративной информационной системы. При этом информационные риски компании зависят от:

– показателей ценности информационных ресурсов;
– вероятности реализации угроз для ресурсов;
– эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. После оценки рисков можно выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть установлены как количественными методами (например, при нахождении стоимостных характеристик), так и качественными, скажем, с учетом штатных или чрезвычайно опасных нештатных воздействий внешней среды.

Возможность реализации угрозы для некоторого ресурса компании оценивается вероятностью ее реализации в течение заданного отрезка времени. При этом вероятность того, что угроза реализуется, определяется следующими основными факторами:

– привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);
– возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);
– техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;
– степенью легкости, с которой уязвимость может быть использована.

На этапе управления рисками разрабатывается некоторая стратегия, в рамках которой возможны следующие подходы к управлению информационными рисками компании:

1. Уменьшение риска – значительное число рисков удается уменьшить за счет простых и дешевых действий (корректное управление паролями снижает риск несанкционированного доступа).
2. Уклонение от риска – от некоторых рисков можно уклониться (вынесение публичных серверов организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны интернет-клиентов).
3. Изменение характера риска – если от риска не удается уклониться или эффективно его уменьшить, можно принять меры страховки или переложить риск на стороннюю организацию, отдавая отдельные функции на аутсорсинг (страхование оборудования от внештатных ситуаций, договор о сопровождении и компенсации ущерба).
4. Принятие риска – некоторые риски невозможно уменьшить до желаемой величины, либо затраты на их уменьшение неоправданно высоки. В таких случаях организация признает потенциальные потери приемлемыми для себя и не реализует специальные меры по снижению риска.

Указанные подходы не являются взаимоисключающими и часто применяются в комплексе. Основная цель ограничения риска – это его снижение до приемлемого для организации уровня, но поскольку риск при этом не устраняется полностью, то его часть, оставшаяся после ограничения, должна быть принята организацией.

Минимизировать IT-риски возможно путем предупреждения несанкционированного доступа к данным, а также аварий и сбоев оборудования. Процесс минимизации следует рассматривать комплексно: сначала выявляются возможные проблемы, затем эти проблемы классифицируются по выше приведенной системе подходов к управлению рисками. Далее необходимо разделить все выявленные IT-риски на подконтрольные и неподконтрольные для организации. Организация не может воздействовать на неподконтрольные ей риски (такие, как природные угрозы и некоторые угрозы технологической среды), и, следовательно, организация может либо принять эти риски, либо передать их путем страхования. Если для подконтрольных рисков сравнить денежную оценку каждого элемента набора рисков с порогом принятия риска, определяемым на основе важности риска, установленного высшим руководством или акционерами компании, то это позволит выделить приемлемые риски, то есть риски, которые могут быть полностью приняты организацией. Таким образом, остаются подконтрольные, но неприемлемые для организации риски, которые следует минимизировать наиболее подходящими средствами и способами.

Управление информационными рисками – это системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативно-правовой базы в области защиты информации и собственной корпоративной политики безопасности. Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании.

Таким образом, мы выявили, что основная задача системы управления рисками − объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании.