

1 Основы методологии страхования информационных рисков

Хотя страхование рисков, связанных с информационной безопасностью, само по себе не является организационным средством защиты информации (так как факт наличия или отсутствия такой страховки не влияет на вероятность нанесения ущерба информационным ресурсам), все же оно является важным и перспективным инструментом управления информационными рисками на предприятии. С точки зрения риск-менеджмента, страхование является главным инструментом так называемой «передачи рисков». Основным фактором, обуславливающим заинтересованность предприятий в страховании своих информационных ресурсов, является то, что в случае каких-либо серьезных нарушений в работе информационных систем предприятие получает возможность за счет страховых выплат относительно быстро восстановить их (систем) работу, а также основные бизнес-процессы и компенсировать (хотя бы частично) ущерб от вынужденного простоя и потери информационных активов.

Согласно Закону РФ «Об организации страхового дела в Российской Федерации», объектом страхования могут быть не противоречащие законодательству имущественные интересы, связанные с владением, пользованием, распоряжением имуществом, а также связанные с возмещением страхователем причиненного им вреда личности или имуществу физического лица, а также вреда, причиненного юридическому лицу (страхование ответственности). Таким образом, на практике объектами страхования могут быть:

- информационные ресурсы (в любом их виде: базы данных, библиотеки электронных документов и пр.);
- программное обеспечение (как уже используемые программные собственные и покупные продукты, так и находящиеся в разработке);
- аппаратное обеспечение информационных систем (сетевое оборудование, серверы, рабочие станции, телекоммуникационное оборудование, периферия, источники бесперебойного питания и пр.);

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

– финансовые активы (денежные средства, бездокументарные ценные бумаги) в электронной форме (в том числе средства на счетах, управляемых при помощи систем «клиент-банк»).

Договор страхования (страховой полис) может предусматривать возмещение прямых убытков в случае наступления различных страховых случаев, таких как:

– выход из строя (сбои в работе) информационных систем, обусловленные недостаточным качеством используемых программных и аппаратных средств, ошибками при их проектировании, разработке, производстве, установке, настройке, обслуживании или эксплуатации;

– умышленные противоправные действия сотрудников предприятия, совершенные с целью нанести ущерб предприятию либо получить определенную выгоду;

– нападения (атаки) на информационные системы предприятия, которые совершены третьими лицами с целью нанести ущерб информационным ресурсам предприятия и его информационным системам (повредить или уничтожить информацию, хранящуюся в электронном виде, получить конфиденциальные сведения, вывести из строя программные и аппаратные средства с целью прекратить или приостановить функционирование определенных сервисов и пр.);

– воздействия вредоносных программ и макросов (вирусов, червей и пр.), повлекшие нарушения работы информационных систем, потерю информации или разглашение конфиденциальной информации;

– хищение финансовых активов (денежных средств, бездокументарных ценных бумаг), совершенное путем осуществления различных неправомерных действий: кражи паролей и ключей, присвоения личности, внесения изменений в программное обеспечение и пр.

В дополнение к основным рискам, непосредственно связанным с информационными активами, также могут быть застрахованы:

- убытки от приостановки основной хозяйственной деятельности предприятия в результате нарушения работы информационных систем;
- дополнительные расходы, связанные с поддержанием текущей хозяйственной деятельности в период восстановления работы поврежденных информационных систем;
- дополнительные расходы, связанные со срочным восстановлением работы информационных систем, а также срочным восстановлением основной хозяйственной деятельности предприятия;
- дополнительные расходы на восстановление деловой репутации после того, как ей был нанесен ущерб в результате атаки на информационные ресурсы и информационные системы (Public Relations Coverage).

Убытки от приостановки основной хозяйственной деятельности предприятия могут включать в себя упущенную выгоду, обусловленную простоем информационных систем (т.е. ту прибыль, которую предприятие могло бы получить, но не получило по причине выхода из строя информационных систем), а также расходы по поддержанию инфраструктуры предприятия в период вынужденного простоя (как правило, это некоторые постоянные расходы, не зависящие от объема выпуска продукции и интенсивности хозяйственной деятельности). Дополнительные расходы, связанные с поддержанием текущей хозяйственной деятельности в период восстановления работы поврежденных информационных систем, могут возникать в том случае, если существуют некоторые альтернативные способы обработки и хранения информации и осуществления бизнес-процессов (например, на базе программных и аппаратных средств, а также телекоммуникационных каналов, временно арендуемых у специализированных компаний) и предприятие сочтет нужным и возможным воспользоваться этими альтернативными способами. При этом задействование таких резервных ресурсов, как правило, должно быть согласовано со страховой компанией, покрывающей эти расходы. Дополнительные расходы, связанные со срочным

восстановлением работы информационных систем, могут возникать в том случае если, например, у сторонних поставщиков существуют некоторые альтернативные (более оперативные по сравнению с обычными) условия поставок оборудования и программного обеспечения, а также предоставления услуг по вводу в действие информационных систем.

Все эти расходы, очевидно, также могут быть объектами страхования. При этом в каждой ситуации страховщику и страхователю необходимо детально проанализировать различные альтернативы выхода из кризисной ситуации и выбирать наиболее целесообразные варианты. Так, например, страховая компания может отказаться компенсировать дополнительные издержки, связанные со срочным восстановлением информационных систем, если более выгодной является компенсация упущенной выгоды за период более длительного вынужденного простоя.

Процедура страхования (жизненный цикл договора страхования) включает в себя несколько основных этапов (Рисунок 1).

- 1) Предварительное обследование предприятия, анализ существующих рисков для информационной безопасности.
- 2) Формулирование рекомендаций по уменьшению рисков и реализация предприятием соответствующих мероприятий.
- 3) Согласование условий страхования и заключение договора.
- 4) Анализ ущерба и его расчет в денежном выражении в случае реализации застрахованных рисков.
- 5) Согласование и последующее осуществление страховых выплат, покрывающих ущерб.

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

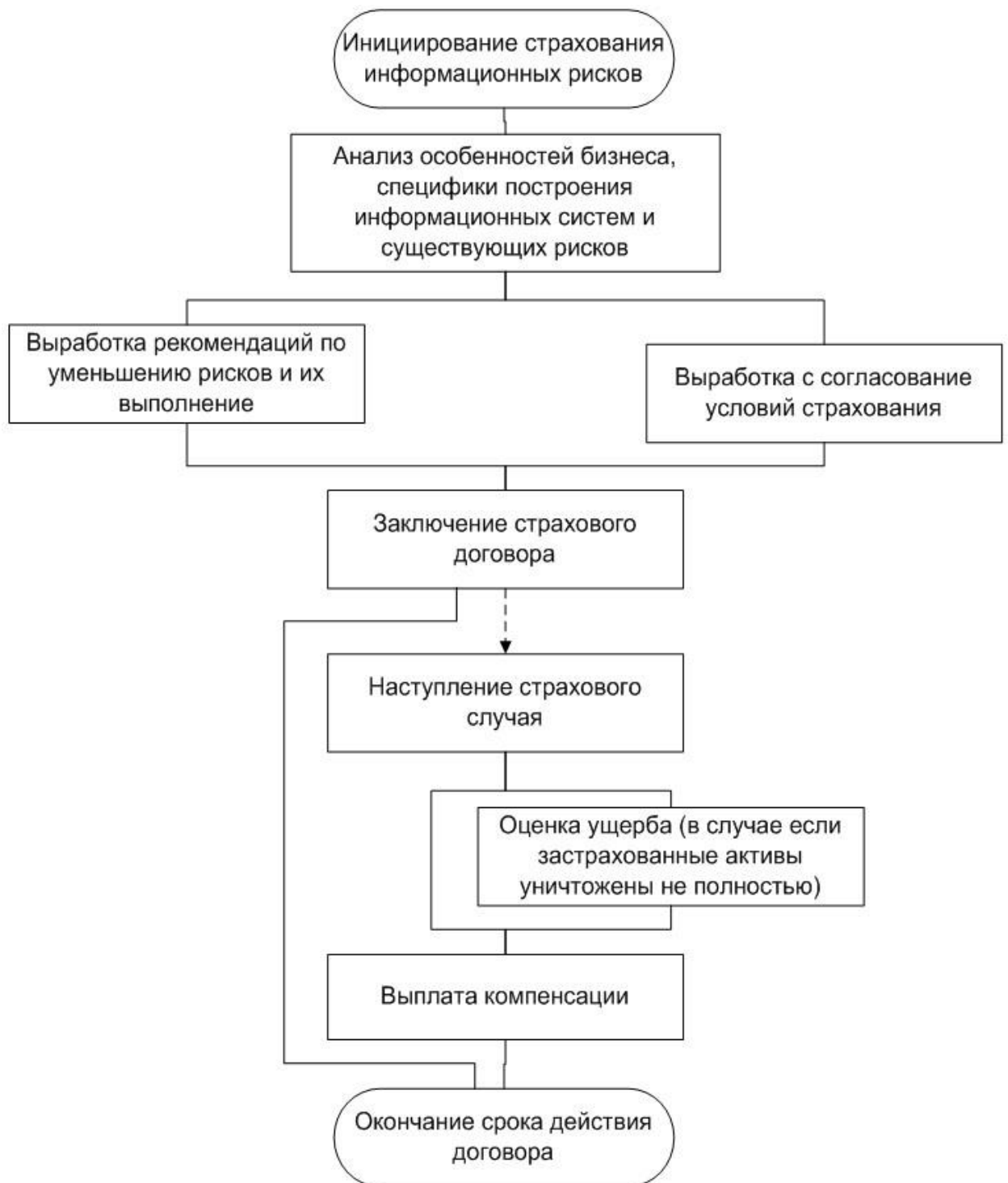


Рисунок 1 – стадии процесса страхования информационных рисков

Предварительное обследование предприятия до заключения договора страхования во многом аналогично проведению внешнего аудита и также может осуществляться независимой специализированной компанией. По окончании такой проверки могут быть сформированы два основных документа:

- отчет (заключение) о состоянии информационной безопасности на предприятии;
- рекомендации по повышению уровня защищенности информационных ресурсов и уменьшению рисков.

Такое обследование в дальнейшем создает предпосылки для принятия решения о возможности и целесообразности страхования информационных рисков данного предприятия, а также для обоснованного количественного анализа рисков и определения основных параметров договора страхования.

На основе оценок рисков (с учетом реализации рекомендованных мероприятий по их уменьшению) определяется одно из наиболее существенных условий договора страхования – ставка страхования. Как правило, ее размер не превышает пяти процентов, однако на практике он может варьироваться в диапазоне от нескольких десятых долей процента до пяти и более процентов. На размер ставки в каждом конкретном случае могут повлиять несколько факторов:

- статистические данные, касающиеся нарушений информационной безопасности на аналогичных предприятиях (в сопоставимых условиях);
- уровень защищенности информационных ресурсов данного предприятия (качество используемых технических средств, уровень организационного обеспечения информационной безопасности на предприятии и пр.);
- интенсивность текущей хозяйственной деятельности (выполнения текущих бизнес-операций);

– страховая сумма – стоимость информационных активов, подлежащих страхованию (как правило, чем больше стоимость страхуемых ресурсов, тем ниже удельная ставка страхования).

Помимо ставки страхования в процессе согласования условий договора также определяется другой важный параметр – лимит ответственности страховой компании (максимальная величина средств, которые могут быть выплачены страховщиком страхователю в течение всего срока действия договора страхования). Как правило, страховая сумма должна быть достаточно большой, чтобы у страховой компании была возможность компенсировать накладные расходы (в частности, расходы на предварительное обследование предприятия), связанные с заключением договора страхования.

В случае реализации риска (возникновения страхового случая) застрахованные информационные ресурсы могут быть полностью утрачены. При этом страховая компания должна будет произвести страховые выплаты в полном объеме (в пределах установленного лимита ответственности). В случае, если повреждена только часть информационных ресурсов, для предприятия и страховой компании начинается сложный процесс определения суммы ущерба, которая должна быть компенсирована. Такая оценка также может быть произведена независимой третьей стороной. Кроме того, предметом анализа в этой ситуации могут быть все обстоятельства, связанные с произошедшим страховым случаем. В частности, договором страхования может быть предусмотрена обязанность предприятия-клиента предпринять ряд мер в рамках определенного плана аварийных мероприятий с целью минимизировать ущерб. Таким образом, страховая компания, прежде чем произвести выплаты, должна будет убедиться в том, что предприятием-клиентом были предприняты определенные меры предосторожности.

То обстоятельство, что взаимодействие страховщика и страхователя при определении размера страховых выплат является одним из наиболее проблемных вопросов, заставляет передовые компании искать новые формы организации процесса страхования. Так, например, для разрешения проблем

при реализации некоторых страховых рисков и уменьшения убытков третьей стороной в договоре страхования может выступать компания – поставщик информационных систем и комплексных решений, которая при наступлении страхового случая может на некоторое время (на период восстановительных работ) предоставить резервные программные и аппаратные средства для обеспечения непрерывности основной деятельности предприятия-страхователя, а также организовать сами восстановительные работы. В этом случае страховая компания может сократить размер страховых выплат на компенсацию упущенной выгоды предприятия-страхователя и избежать некоторых излишних выплат на восстановление утраченных информационных ресурсов.

Помимо страхования собственно информационных рисков, также важное значение имеет страхование гражданской ответственности компаний, оказывающих информационные услуги и услуги по защите информации большому числу пользователей:

- страхование гражданской ответственности удостоверяющих центров, работающих в инфраструктуре публичных ключей;
- страхование ответственности фондовых бирж и других электронных торговых площадок по возмещению имущественного вреда третьим лицам;
- страхование гражданской ответственности разработчиков и поставщиков средств защиты информации.

Необходимость страхования гражданской ответственности компаний-поставщиков продуктов и услуг перед потребителями в этом случае обусловлена тем, что их услугами (продуктами) пользуется большое число клиентов, каждый из которых с использованием этих продуктов и услуг управляет дорогостоящими информационными активами (финансовыми средствами, конфиденциальными сведениями, разглашение которых может привести к огромным убыткам, и пр.). Таким образом, у компаний-поставщиков таких продуктов и услуг возникают риски того, что к ним будут предъявлены иски о возмещении ущерба, понесенного клиентами вследствие

того, что злоумышленники воспользовались уязвимостями в поставляемых продуктах. Очевидно, что собственные активы и доступные средства, имеющиеся у компаний-поставщиков, как правило, гораздо меньше потенциально возможного ущерба, который может возникнуть у их клиентов. В результате этого страхование оказывается единственным средством обеспечения ответственности и, следовательно, построения цивилизованных взаимоотношений на рынке средств защиты информации, а также услуг по защите информации.

2 Рынок страховых услуг

Мировая практика страхования информационных рисков начала складываться в девяностых годах и получила свое развитие после 2000-го года, когда, с одной стороны, риски информационной безопасности стали более серьезными, чем когда-либо, а с другой – в западных странах окончательно сложилась практика не включать информационные риски в универсальные страховые полисы, которыми обычно покрывались основные бизнес-риски.

Таким образом, к настоящему времени крупнейшими мировыми компаниями, оказывающими услуги по страхованию информационных рисков, являются:

- Британская страховая компания «Lloyds of London»;
- американская компания «AIG»;
- Zurich North America («The E-Risk Edge solution»);
- страховая группа «Chubb»;
- страховая компания «Marsh».

Страхование информационных рисков компанией Lloyds of London осуществляется совместно с известной компанией Counterpane, предоставляющей услуги по оценке состояния защищенности информационных ресурсов и по текущей поддержке информационной безопасности. Также в этой работе участвуют компании Frank Crystal & Co. и SafeOnline Ltd. Эти предприятия предлагают два основных совместных страховых продукта:

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

- Internet Asset and Income Protection Coverage («Покрытие рисков, связанных с информационными активами и информационной деятельностью»)
- программа страхования информационных ресурсов отдельных компаний;
- Internet Asset and Income Protection Warranty Plan («План гарантирования информационных активов и информационной деятельности») – основанный на страховании план гарантирования надежности работы поставщиков услуг Интернет.

Американская страховая компания American International Group, Inc. (AIG), действующая в 130 странах мира, в лице своего подразделения AIG eBusiness Risk Solutions (AIG eBRS) предлагает программу страхования информационных рисков netAdvantage (AIG netAdvantage Suite). В рамках своей комплексной программы страхования эта компания предлагает скидки клиентам, пользующимся определенными средствами защиты информации. Для обеспечения эффективности и комплексности услуг по страхованию AIG eBRS организует технологические альянсы с компаниями, поставляющими средства защиты информации, а также проводящими аудиты безопасности.

В рамках программы netAdvantage предлагается несколько вариантов страховой защиты:

- защита от ущерба в случае неправомерного разглашения частных данных;
- защита от уничтожения (утраты) данных или программного обеспечения;
- защита от ущерба в случае нарушения операционной деятельности (упущенная выгода и дополнительные расходы) в случае нарушений информационной безопасности;
- страховая компенсация затрат на нейтрализацию уязвимостей;
- страховая компенсация затрат на восстановление деловой репутации (PR) в случае реализации рисков.

Тема 2.10 – Страхование информационных рисков
(Планирование и управление информационной безопасностью)

В России одной из первых компаний, начавших предоставлять услуги такого рода, стал «Ингосстрах». В 1999 году было подписано «Соглашение о сотрудничестве в области страхования информационных ресурсов» между Министерством РФ по связи и информатизации, с одной стороны, и страховыми компаниями «Ингосстрах» и «Инфистрах» – с другой. Начиная с 2000 года некоторые российские страховые компании получили лицензии на осуществление такой деятельности, однако в целом этот рынок в России остается неразвитым. Деятельность страховых компаний, как правило, ориентирована на страхование банковских рисков и крупных объектов (таких как «Российская торговая система», РТС или система межбанковского процессингового центра электронного документооборота Faktura.Ru), при этом некоторые сегменты этого рынка практически не развиваются.