УДК 005.511
DOI 10.21685/2587-7704-2020-5-2-5

Open Access RESEARCH ARTICLE

Страхование киберрисков в системе менеджмента информационной безопасности

А. Г. Фатеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

И. Ю. Ульянкина
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Рассматривается место страхования киберрисков в системе менеджмента информационной безопасности, в связи с возрастающим интересом организаций к киберстрахованию и ростом предложений по страхованию киберрисков. Описаны этапы функционирования системы менеджмента информационной безопасности и их соответствие модели PDCA. Определяется, на каком этапе функционирования системы менеджмента информационной безопасности следует рассматривать покупку полиса киберстрахования.

Ключевые слова: информационная безопасность, кибериски, страхование киберрисков, средние и крупные предприятия, модель PDCA.

Cyber risk insurance in the information security management system

A. G. Fateev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

I. Yu. Ul'yankina
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. This article examines cyber risk insurance in the information security management system in terms of organizational growing interest in cyber insurance and the increase in cyber risk insurance proposals. The article also discusses the stages of information security management system operation and their compliance with the PDCA model. The appropriate stage of the information security management system operation for the purchase of a cyber insurance policy is considered.

Keywords: information security, cyber risks, cyber risk insurance, medium-sized and large enterprises, PDCA model.

По данным страховой компании «Росгосстрах» [1], в России наблюдается рост интереса к страхованию киберрисков, что приводит к росту предложений данной услуги со стороны страховщиков. По данным отчета «Cyber Insurance Market Size, Share & Trends Analysis Report By Organization (SMB, Large Enterprise), By Application (BFS, Healthcare, IT & Telecom), And Segment Forecasts, 2019–2025» [2], крупные организации составляют большую часть потребителей услуги киберстрахования, и эта тенденция будет сохраняться в ближайшие несколько лет. В связи с появлением предложений по страхованию киберрисков возникает проблема введения страхования информационных рисков в систему менеджмента информационной безопасности организации, которая реализована в большинстве крупных организаций.

Система менеджмента информационной безопасности (СМИБ) – часть общей системы менеджмента, основанная на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению информационной безопасности [3]. Согласно стандарту ГОСТ Р ИСО/МЭК 27000-2012 [3] внедрение системы менеджмента информационной безопасности следует модели «План (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA) для непрерывного совершенствования процессов системы менеджмента информационной безопасности:

– планирование включает в себя определение проблемы, сбор полезной информации для оценки риска безопасности, определение политик и процессов, которые можно использовать для устранения причин проблемы, разработку методов для обеспечения постоянного улучшения возможностей управления информационной безопасностью;

– осуществление включает в себя реализацию разработанных политик и процедур безопасности;

– проверка включает в себя отслеживание эффективности политик и средств контроля информационной безопасности;

– действие включает в себя корректировку и улучшение работы.

В соответствии с международным стандартом ISO/IEC 27001:2013 [4] выделяются следующие этапы функционирования системы менеджмента информационной безопасности:

– контекст организации. На данном этапе необходимо проанализировать внешнюю и внутреннюю среду для определения факторов, которые могут повлиять на функционирование СМИБ;

– руководство. На данном этапе руководство организации определяет лиц, которые контролируют формирование и функционирование СМИБ, но даже при передаче своих полномочий другим лицам руководство по-прежнему будет нести полную ответственность за деятельность, связанную с информационной безопасностью и СМИБ. Руководство устанавливает политику информационной безопасности, которая описывает стратегическую важность СМИБ для организации. Политика информационной безопасности должна содержать деловую ситуацию организации, корпоративную культуру, факторы и цели организации, связанные с информационной безопасностью. Руководство также должно обеспечить распределение обязанностей и полномочий ролей, относящихся к информационной безопасности, которые должны быть распределены и доведены до сведения лиц по всей организации;

– планирование. Данный этап включает в себя оценку риска и планирование обработки риска, определение и внедрение процесса оценки рисков информационной безопасности, выбор вариантов обработки риска и определение соответствующих мер обеспечения информационной безопасности для осуществления выбранных вариантов обработки риска;

– поддержка. На данном этапе необходимо определить и предоставить ресурсы для создания, внедрения, обслуживания и постоянного улучшения СМИБ. Также необходимо определить необходимую квалификацию для лиц, выполняющих работу, связанную с обеспечением информационной безопасности, и убедиться, что квалификация этих лиц базируется на их приемлемом образовании, профессиональной подготовке (стажировке) или опыте работы;

– функционирование. На данном этапе должны проводится контроль и реализация процессов, требуемых для безопасности информации. Должны осуществляться планы по выполнению целей обеспечения информационной безопасности, установленные на этапе планирования. При запланированных изменениях необходимо контролировать их выполнение, распределять обязанности, установить сроки и выделять ресурсы для введения изменений. При непреднамеренных изменениях необходимо проводить анализ последствий от них, в случае негативных последствий принимать меры по их снижению или устранению. В случае передачи части функций на аутсорсинг должна проводится проверка и мониторинг услуг поставщиков, при необходимости можно управлять изменениями в услугах поставщика;

– оценка деятельности. На данном этапе необходимо собирать данные о функционировании мер защиты информации. Для сбора дополнительных сведений об эффективности СМИБ необходимо проводить внутренние аудиты. При необходимости для проведения внутреннего аудита может привлекаться третья сторона. При оценке обеспечения безопасности информации могут быть идентифицированы новые риски безопасности информации или скорректированы выявленные ранее;

– совершенствование. На данном этапе могут быть рассмотрены идентифицированные несоответствия и сферы, требующие постоянного совершенствования. Шаги, предпринятые при реагировании на идентифицированные несоответствия, могут способствовать обработке рисков безопасности информации.

На рис. 1 показано соответствие этапов СМИБ модели PDCA.

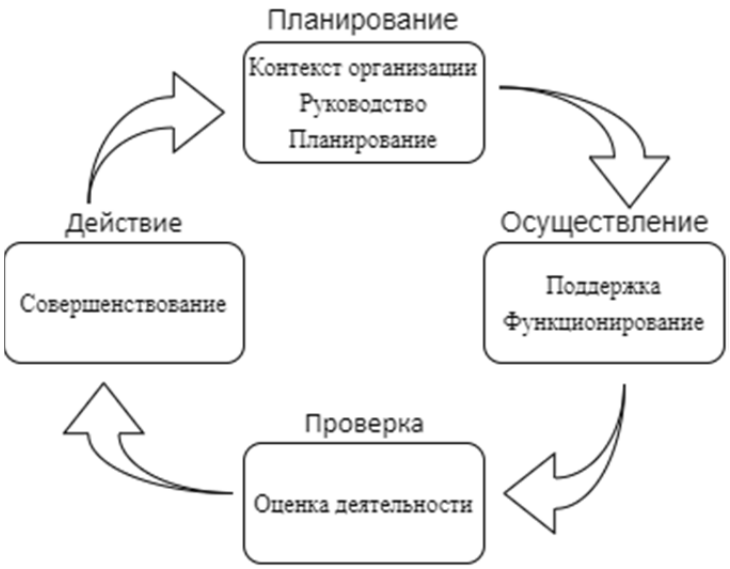

Рис. 1. Соответствие этапов СМИБ модели PDCA

Исходя из утверждения международного стандарта ISO/IEC 27102:2019 [4], что киберстрахование является вариантом обработки риска, рассматривать его необходимо на стадии «Планирование». Существует четыре варианта обработки риска: модификация риска, сохранение риска, предотвращение риска и перенос риска. Варианты обработки риска следует выбирать на основе результатов оценки риска, предполагаемой стоимости реализации этих вариантов и ожидаемых от этих вариантов выгод. Не обязательно выбирать только один вариант обработки риска.

Модификация риска осуществляется путем введения, устранения или изменения мер защиты информации, так, чтобы остаточные риски могли быть вновь оценены как приемлемые. Если уровень риска соответствует критериям принятия риска, нет необходимости в реализации дополнительных мер защиты информации и риск может быть сохранен.

Когда идентифицированные риски считаются слишком высокими или когда стоимость реализации других вариантов обработки риска превышает выгоды, может быть принято решение о полном предотвращении риска путем отказа от планируемого или существующего вида деятельности или совокупности видов деятельности или изменения условий, в которых осуществляется этот вид деятельности.

Риски также можно разделить с внешними сторонами, то есть переложить риск на другие субъекты, следовательно, киберстрахование следует рассматривать при принятии решения о переносе риска. При передаче риска страховой компании руководство организации страхователя должно быть уверено в том, что их страхование эффективно передает риск с учетом актуальных угроз и нормативно-правовой базы. Страховым компаниям, в свою очередь, необходимо всестороннее представление о состоянии информационной безопасности организации.

Поскольку киберстрахование – один из вариантов переноса рисков, который является частью СМИБ организации-страховщика, то есть смысл в том, чтобы застрахованное лицо регулярно предоставляло страховщику соответствующую информацию о кибербезопасности. Подобный обмен информацией должен быть согласован между страхователем и страховой компанией**.**

В стандарте ISO/IEC 27102:2019 [5] отмечается, что в процессе страхования рисков кибербезопасности страховая компания и страхователь должны обмениваться информацией для того, чтобы:

– страхователь мог продемонстрировать свои усилия по защите от угроз кибербезопасности;

– страховая компания могла определить, какие риски страхователь хочет разделить;

– страховая компания могла оценить принимаемый им риск, а затем создать полис страхования и определить расценки, включая применимые франшизы или исключения.

Следует отметить, что страхование киберрисков для уменьшения влияния негативных последствий должно использоваться в дополнение к организационным и техническим мерам защиты информации. Страхование рисков информационной безопасности не может быть заменой надежных планов обеспечения кибербезопасности и планов по эффективному реагированию на инциденты. Страхование следует рассматривать в качестве важного компонента общего плана по управлению рисками организации и повышению устойчивости к ним.

Библиографический список

1. Интерес к киберстрахованию в РФ со стороны потребителей растет – «Росгосстрах». – URL: https://mfd.ru/news/view/?id=2254524, (свободный).
2. Cyber Insurance Market Size, Share & Trends Analysis Report By Organization (SMB, Large Enterprise) / by Application (BFS, Healthcare, IT & Telecom), And Segment Forecasts, 2019 – 2025. – URL: https://www.grandviewresearch.com/industry-analysis/cyber-insurance-market
3. ГОСТ Р ИСО/МЭК 27000–2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. – URL: http://docs.cntd.ru/document/1200102762
4. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.
5. ISO/IEC 27102:2019. Information security management — Guidelines for cyber-insurance.

Образец цитирования:

Фатеев, А. Г. Страхование киберрисков в системе менеджмента информационной безопасности / А. Г. Фатеев, И. Ю. Ульянкина // Инжиниринг и технологии. – 2020. – Vol. 5(2). – С. 1–4. – DOI 10.21685/2587-7704-2020-5-2-5.