АНАЛИЗ И ОПРЕДЕЛЕНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Харченко А.Ю.[1], Харченко Ю.А.[2]
Email: Kharchenko684@scientifictext.ru

[1]Харченко Александр Юрьевич - магистр,
кафедра прикладной информатики,
Белгородский государственный аграрный университет им. В.Я. Горина;
[2]Харченко Юрий Алексеевич - кандидат биологических наук, старший преподаватель,
кафедра факультетской хирургии,
Белгородский государственный национальный исследовательский университет,
г. Белгород

Аннотация: *актуальность данной темы обусловлена тем, что в течение последних нескольких лет информация стала играть важнейшую роль во всех сферах человеческой жизни, что связано с постепенным становлением информационного общества. В статье уделено внимание информационным рискам как основной составляющей рисков применения различных информационных технологий в бизнесе. Информационная безопасность является обеспечением устойчивого развития и функционирования объекта. Защита информации требует определенных затрат, поэтому задача нахождения соответствующего уровня защиты при допустимых затратах является одним из условий обеспечения информационной безопасности. Возможность выявления рисков в различных областях имеет ключевое значение для развития и стабильности предприятий, поскольку позволяет понять и оценить предполагаемые опасные события, выявить их причины и последствия, вероятности возникновения и принятия решений, что является одной из сложных задач. Для оценки существующего уровня защищенности ресурсов любой организации требуется проведение анализа рисков информационной безопасности в целях их последующего сокращения, утилизации или передачи.*
Ключевые слова: *информационные риски, информационная безопасность, анализ рисков, определение рисков.*

ANALYSIS AND DETERMINATION OF INFORMATION SECURITY RISKS

Kharchenko A.Yu.[1], Kharchenko Yu.A.[2]

[1]Kharchenko Alexander Yuryevich - Master,
DEPARTMENT OF APPLIED INFORMATICS,
BELGOROD STATE AGRARIAN UNIVERSITY NAMED AFTER V.YA. GORIN;
[2]Kharchenko Yuri Alekseevich - Candidate of Biological Sciences, Senior Lecturer,
DEPARTMENT OF FACULTY SURGERY,
BELGOROD STATE NATIONAL RESEARCH UNIVERSITY,
BELGOROD

Abstract: *the relevance of this topic is due to the fact that over the past few years, information has begun to play a crucial role in all areas of human life, which is associated with the gradual formation of the information society. The article focuses on information risks as the main component of the risks of using various information technologies in business. Information security is ensuring the sustainable development and operation of the facility. Information protection requires certain costs, therefore, the task of finding the appropriate level of protection at an acceptable cost is one of the conditions for ensuring information security. The ability to identify risks in various fields is key to the development and stability of enterprises, since it allows you to understand and evaluate the alleged hazardous events, identify their causes and consequences, the likelihood of occurrence and decision-making, which is one of the difficult tasks. To assess the existing level of security of the resources of any organization, an analysis of information security risks is required with a view to their subsequent reduction, disposal or transfer.,*
Keywords: *information risks, information security, risk analysis, risk definition.*

УДК 004.056

В настоящий момент еще не сложилось однозначного понятия о том, что же из себя представляет информационный риск. Некоторые специалисты рассматривают информационный риск в качестве события, которое оказывает непосредственное влияние на информацию: ее удаление, искажение, нарушение ее конфиденциальности или доступности [6].

Риски подразделяются по характеру на внешние и внутренние; по времени возникновения на прошлые или ретроспективные и будущие или перспективные; по фактору возникновения такие, как проектные, операционные риски, процессные, организационные; по последствиям на чистые и спекулятивные.

Так же выделяется подклассификация рисков по степени последствий возникновения и состоит из: допустимого риска, критического риска и катастрофического риска. Эта классификации является важной при принятии решений по осуществлению какой-либо деятельности, связанной с рисками.

Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков [2].

Важным этапом является идентификация риска - это одна из стадий анализа рисков позволяющая выявить, оценить и понять предпосылки, которые ведут к появлению риска и которую необходимо проводить перед осуществлением классификации рисков. От правильности ее проведения и будет зависеть результат выбранного метода для устранения ущерба.

Факторы риска - это те основные параметры, которыми оперируют при оценке рисков, а именно:

- Актив (Asset).
- Угроза (Threat).
- Ущерб (Loss).
- Уязвимость (Vulnerability).
- Возврат инвестиций (ROI).

- Механизм контроля (Control).
- Размер среднегодовых потерь (ALE).

Способы анализа и оценки этих параметров определяются используемой в организации методологией оценки рисков [1,5].

Информационный риск является опасным для объекта или субъекта информатизации событием, при реализации которого возможно нанести ущерб, как для информационной сферы, так и для информационного обслуживаемого объекта в целом. Информационные риски связаны с информационной безопасностью (ИБ) с помощью современных методик анализа и управления рисками.

Определение рисков в сфере ИБ - это вероятность того, что предприятие или организация могут понести убытки из-за нарушения безопасности информационной системы (ИС). При этом часто понятие риска рассматривается с понятием угрозы, где угроза ИБ - это потенциально возможное происшествие, которое может быть совершено преднамеренно или случайно, но при этом оказывает нежелательное воздействие как на компьютерную систему, так и на информацию, которая находится и обрабатывается в ней. Основное отличие риска от угрозы состоит в том, что риск имеет как количественную оценку возможных потерь, так и оценку вероятности реализации угрозы [3]

На первом этапе эксперт собирает данные об информационной системе. Основные шаги первого этапа анализа информационных рисков показаны на рис. 1.

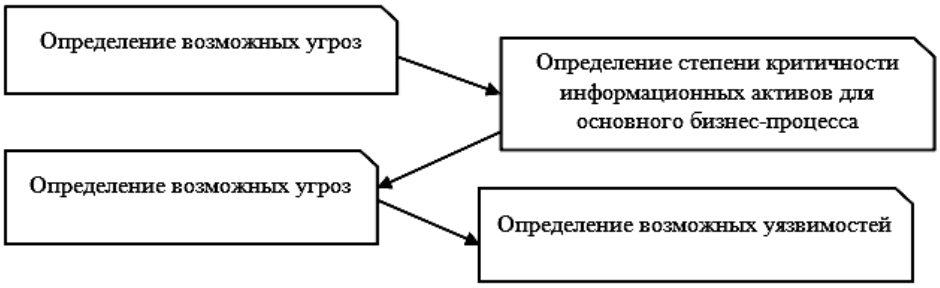

Рис. 1. Подготовка к проведению анализа рисков информационной безопасности

На втором этапе эксперт составляет сценарии возможных инцидентов информационной безопасности и анализирует их. Основные шаги второго этапа анализа рисков информационной безопасности показаны на рис. 2.

Рис. 2. Анализ сценариев возможных инцидентов информационной безопасности

После проведения анализа возможных инцидентов информационной безопасности требуется приобрести некоторое средство защиты информации (далее - СЗИ), а определить, какое именно СЗИ подойдет лучше всего - сложно. Еще сложнее ситуация, когда целесообразность внедрения СЗИ как таковых приходится объяснять руководству. Обычно это дело сопровождается запугиванием руководства всевозможными вирусами и хакерами, злобными конкурентами и регуляторами, страшными рассказами о недовольных сотрудниках, которые навредили в такой-то организации перед собственным увольнением и т.д. Такой подход вполне действенный, но несколько... не научный. Чтобы подойти с научной точки зрения, придется вспомнить о таком методе как оценка рисков информационной безопасности.

Рекомендации по оценке рисков приведены в нескольких документах: *ГОСТ ИСО/МЭК 27005, РС БР ИББС-2.2-2009, NIST SP 800-30.*

Исходя из данных документов, предполагается, что для некоторых существующих в организации активов характерен ряд уязвимостей, через которые на эти активы могут воздействовать угрозы. Задача средств защиты информации - эти уязвимости в той или иной мере закрыть, тем самым уменьшая вероятность воздействия угрозы на актив [4].

Заключение.

С переходом к рыночной экономике и ростом значения прогнозирования экономического развития существенно возросла роль информации. Информация стала залогом успешного функционирования фирмы, поддержанием ее конкурентоспособности и нормального развития. Однако широкое использование информации породило новый вид рисков, которые могут составлять серьезную угрозу развитию и функционированию компаний - это информационные риски, требующие незамедлительного выявления, анализа и оценки в целях последующего сокращения, утилизации или передачи.

Так как анализ рисков - это достаточно трудоемкая процедура, то в её процессе должны применяться различные методические материалы и инструментальные средства.

Однако уже разработано множество систем и методик по расчету и анализу возможных информационных рисков, которые позволяют оперативно информировать о них бизнес и впоследствии соблюдать главные требования рынка - непрерывность и безопасность экономической деятельности компании.

Список литературы / References

1. *Тенетко М.И., Пескова О.Ю.* Анализ рисков информационной безопасности // Известия ЮФУ. Технические науки, 2011. № 12.
2. *Маслова М.А.* Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. Т. 4. № 1, 2019.
3. *Герасименко В.А., Малюк А.А.* Основы защиты информации. М.: Инкомбук, 1997.
4. Анализ рисков информационной безопасности // securitylab.ru. [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/blog/personal/aguryanov/30007.php/ (дата обращения: 21.02.2020).
5. Анализ рисков в управлении информационной безопасностью // bytemag.ru. [Электронный ресурс]. Режим доступа: https://www.bytemag.ru/articles/detail.php?ID=13265/ (дата обращения: 21.02.2020).
6. Информационные риски: методы оценки и анализа // itportal.ru. [Электронный ресурс]. Режим доступа: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/ (дата обращения: 21.02.2020).