электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056

РИСК-МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Миков Д.А., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Информационная безопасность»

Научный руководитель: Булдакова Т.И..,д.т.н., профессор
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
bauman@bmstu.ru

Риском информационной безопасности называется риск, связанный с информационными технологиями. Этот относительно новый термин появился в связи с повышением осознания того факта, что информационная безопасность является лишь одной из составляющих множества рисков, которые имеют отношение к информационным технологиям и реальным мировым процессам, связанным с ними. В общем случае, риск – это произведение вероятности происходящего события и влияния этого события, оказываемого на активы информационных технологий [1]. Влияние события на информационные активы обычно рассчитывается как произведение уязвимости актива и ценности актива для заинтересованных сторон. Таким образом, величина риска информационной безопасности (R) может быть определена как произведение значений угроз (T), уязвимостей (V) и активов (A) [2]:

$$R = T \times V \times A$$

На первом этапе риск-менеджмента информационной безопасности необходимо определить внешний и внутренний контекст, что предполагает установление основных критериев, необходимых для управления информационными рисками, определение масштабов и границ, а также создание соответствующего организационного подразделения для оперативного управления рисками информационной безопасности. В зависимости от масштаба и задач управления рисками, могут быть применены различные подходы. Подходы также могут различаться для каждой итерации. Соответствующий подход к управлению рисками выбирается или разрабатывается в зависимости от таких основных критериев, как критерий оценки риска, критерий воздействия и критерий допустимости риска.

1. Критерий оценки риска должен быть разработан для оценки рисков информационной безопасности организации с учётом следующих факторов:

1) стратегическое значение информационных бизнес-процессов;

2) критичность задействованных информационных активов;

3) законодательные и нормативные требования, а также договорные обязательства;

4) важность доступности, конфиденциальности и целостности для бизнес-операций;

5) ожидания и восприятие от заинтересованных сторон и отрицательные последствия для репутации.

Кроме того, критерий оценки риска может быть использован для определения приоритетов при обработке рисков.

2. Критерий воздействия должен быть разработан и конкретизирован в зависимости от степени ущерба или расходов в организации вследствие события информационной безопасности с учётом следующих факторов:

1) уровень воздействия на информационные активы;

2) нарушения информационной безопасности (например, потеря конфиденциальности, целостности и доступности);

3) нарушение деятельности (как внутренней, так и третьих лиц);

4) экономические и финансовые потери;

5) нарушение планов и сроков;

6) ущерб репутации;

7) нарушение правовых, нормативных или договорных требований.

3. Организация должна определить свою собственную шкалу для уровня допустимости риска. Следует принимать во внимание во время разработки следующие факторы:

1) критерий допустимости риска может включать в себя несколько порогов с желаемым целевым уровнем рисков, но при этом возможно дать распоряжение руководителям высшего звена допускать риски выше этого уровня при определённых обстоятельствах;

2) критерий допустимости риска может быть выражена как отношение рассчитанной прибыли (или другой выгоды) к оценённым рискам;

3) различные критерии допустимости риска могут относиться к различным классам рисков, например, риски, которые могут привести к несоблюдению правил или законов, не могут быть допущены, в то время как принятие высоких рисков может быть разрешено, если это указано в требованиях контракта;

4) критерий допустимости риска может включать в себя требования к будущей дополнительной обработке, например, риски могут быть допущены, если есть согласие и

готовность принять меры для их снижения до допустимого уровня в течение определённого периода времени;

5) критерий допустимости риска может различаться в зависимости от ожидаемого времени существования рисков, например, риски могут быть связаны с временной или краткосрочной деятельностью.

Критерий допустимости риска должны быть установлен с учётом бизнес-критериев, правовых и нормативных аспектов, операций, технологий, финансов, социальных и гуманитарных факторов.

Следующим этапом риск-менеджмента информационной безопасности является идентификация активов, угроз, существующих и планируемых контрмер, уязвимостей и последствий.

1. Необходимо идентифицировать активы в установленных рамках. Активами является всё, что имеет ценность для организации и, следовательно, нуждается в защите. Для идентификации активов следует иметь в виду, что информационная система состоит не только из аппаратных средств и программного обеспечения.

2. Необходимо идентифицировать угрозы и их источники. Угроза потенциально вредит таким активам, как информация, процессы и системы, и, следовательно, организациям. Угрозы могут быть природного или человеческого происхождения, случайными или преднамеренными. Все случайные и преднамеренные источники угроз должны быть идентифицированы. Угроза может возникнуть в пределах или за пределами организации. Угрозы должны быть идентифицированы как в общем, так и по типу (например, несанкционированные действия, физические повреждения, технические сбои), а затем, в случае необходимости, определяются отдельные угрозы в универсальном классе.

3. Необходимо идентифицировать существующие и планируемые контрмеры. Это делается для того, чтобы избежать ненужных работ или затрат, например, при дублировании функций контрмер. Кроме того, при идентификации существующих контрмер следует убедиться, что они работают корректно – ссылка на уже существующие отчёты аудита СМИБ (системы менеджмента информационной безопасности) должны ограничить время, затраченное на эту задачу. Если контрмеры работают некорректно, это может привести к уязвимостям. Следует обратить внимание на ситуацию, когда выбранная контрмера (или стратегия) не действует и, следовательно, необходимы дополнительные контрмеры для эффективного устранения выявленных рисков. В СМИБ это осуществляется путём оценки эффективности контрмер. Оценка эффективности

контрмер показывает, как та или иная контрмера снижает вероятность угрозы, возможность использования уязвимости или воздействие инцидента.

4. Необходимо идентифицировать уязвимости, которые могут быть использованы угрозами для причинения ущерба активам или организации. Уязвимости могут быть идентифицированы для организации, процессов и процедур, этапов управления, персонала, физической среды, конфигурации информационной системы, аппаратных средств, программного обеспечения или средств связи, зависимости от внешних сторон.

5. Должны быть идентифицированы последствия, которые приводят к потере конфиденциальности, целостности и доступности и могут оказать воздействие на активы. Последствием может быть потеря эффективности, неблагоприятные условия работы, бизнес-потери, репутационный и иной ущерб и т.д. Это действие идентифицирует ущерб или последствия для организации, которые могут произойти по сценарию инцидентов. Сценарий инцидентов представляет собой описание угроз, использующих определённые уязвимости или группу уязвимостей при инциденте информационной безопасности. Последствия сценариев инцидентов должны быть установлены с учётом критерия воздействия, разработанного в процессе деятельности по определению контекста. Воздействие может быть оказано на один или несколько активов либо часть актива. Таким образом, активам можно присвоить значения как для их финансовой стоимости, так и для последствий для бизнеса в случае их повреждения или компрометации. Последствия могут носить временный или постоянный характер, как в случае уничтожения актива. Организации должны идентифицировать оперативные последствия сценариев инцидентов с точки зрения времени расследования и восстановления, потери рабочего времени, упущенных возможностей, здоровья и безопасности, финансовой стоимости конкретных навыков для возмещения ущерба, репутации и имиджа и т.д.

После идентификации основных критериев риска и вышеперечисленных элементов СМИБ необходимо провести оценку рисков.

Риск информационной безопасности – это вероятность того, что данная угроза сможет использовать уязвимости актива или группы активов и тем самым причинить вред организации. Он измеряется как сочетание вероятности события и его последствий [3].

OWASP (Open Web Application Security Project) предлагает практическую методологию оценки рисков на основе следующих этапов [4].

1. Оценка вероятности как среднее арифметическое различных характеристик по шкале от 0 до 9:

1) характеристики злоумышленников: уровень квалификации, мотивированность, возможности, количество;

2) характеристики уязвимостей (данная группа характеристик связана с существующими уязвимостями, цель заключается в оценке вероятности обнаружения и использования отдельной существующей уязвимости, с учётом характеристик злоумышленников, оценённых выше): вероятность обнаружения, вероятность использования, осведомлённость, обнаружение вторжения.

2. Оценка воздействия как среднее арифметическое различных факторов по шкале от 0 до 9:

1) факторы технического воздействия (техническое воздействие можно разделить на факторы, связанные с традиционными областями безопасности: конфиденциальностью, целостностью, доступностью и подотчётностью – цель заключается в оценке степени воздействия на систему, если уязвимость была использована): потеря конфиденциальности, потеря целостности, потеря доступности, потеря подотчётности;

2) факторы воздействия на бизнес (воздействие на бизнес связано с техническим воздействием, но требует глубинного понимания важности тех или иных аспектов для компании, в общем, необходимо стремиться поддерживать риски воздействия на бизнес, особенно на уровне исполнителей, так как бизнес-риски оправдывают вложение средств в безопасность): финансовый ущерб, ущерб репутации, несоблюдение юридических и договорных требований; нарушение конфиденциальности персональных данных.

Если воздействие на бизнес рассчитывается точно, можно использовать его оценку далее, в противном случае следует использовать оценку технического воздействия:

1) распределение оценок вероятности и воздействия по трёхуровневой шкале {НИЗКИЙ, СРЕДНИЙ, ВЫСОКИЙ}, где низкий уровень – менее 3, средний – от 3 до 5, высокий – от 6 до 9;

2) расчёт уровня рисков с помощью сводной таблицы.

Итоговая оценка риска

Воздействие	ВЫСОКОЕ	Средний	Высокий	Критический
	СРЕДНЕЕ	Низкий	Средний	Высокий
	НИЗКОЕ	Отсутствует	Низкий	Средний
		НИЗКАЯ	СРЕДНЯЯ	ВЫСОКАЯ
	Вероятность			

Заключительным этапом риск-менеджмента информационной безопасности является обработка рисков. Существует четыре метода обработки рисков: уменьшение рисков, принятие рисков, отказ от рисков и передача рисков.

1. Необходимо выбрать надлежащие и оправданные контрмеры в соответствии с требованиями оценки и обработки рисков. Выбор уменьшения рисков должен учитывать как критерий допустимости риска, так и правовые, нормативные и договорные требования. Этот выбор должен учитывать также стоимость и сроки осуществления контрмер или технические, экологические и культурные аспекты. Очень часто при правильно подобранных контрмерах можно снизить общую стоимость владения системой.

В общем, контрмеры могут обеспечить один или несколько из следующих видов защиты: коррекция, ликвидация, профилактика, минимизация воздействия, сдерживание, обнаружение, восстановление, мониторинг и осознание. При выборе контрмер важно сравнить стоимость приобретения, осуществления, управления, эксплуатации, мониторинга и поддержания контрмер со стоимостью защищаемых активов. Кроме того, должна быть рассмотрена окупаемость инвестиций с точки зрения уменьшения риска и потенциала использования новых возможностей бизнеса, предоставляемых определёнными контрмерами. Вдобавок необходимо уделять внимание специализированным навыкам, которые могут потребоваться для определения и реализации новых контрмер или изменения существующих.

Существует множество ограничений, которые могут повлиять на выбор контрмер. Технические ограничения, такие как требования производительности, вопросы управляемости (эксплуатационные требования поддержки) и совместимости, могут помешать использованию некоторых контрмер или привести к человеческим ошибкам либо аннулировать контрмеру, вызвать ложное чувство безопасности или даже увеличить риски при отсутствии контрмер (например, сложная парольная защита без надлежащей подготовки приводит к тому, что пользователи записывают пароли). Кроме того, может случиться так, что контрмера будет влиять на производительность. Менеджеры должны попытаться найти решение, удовлетворяющее требованиям производительности при обеспечении достаточного уровня информационной безопасности. Результатом этого этапа является перечень возможных контрмер с их стоимостью, выгодой и приоритетом выполнения.

2. Решение о принятии рисков без дополнительных действий должно быть принято в зависимости от оценки рисков. Если уровень рисков соответствует критерию допустимости риска, нет необходимости реализовывать дополнительные контрмеры, и риски могут быть приняты.

3. Когда выявленные риски слишком высоки, или расходы на реализацию других вариантов обработки превышают выгоду, может быть принято решение отказаться от рисков полностью, путём отказа от запланированного или осуществляемого действия или

группы действий или изменения условий, в соответствии с которыми выполняются действия. Например, для рисков, связанных с природными факторами, наиболее экономически эффективной альтернативой может быть физическое перемещение средств обработки информации в место, где риски отсутствуют или находятся под контролем.

4. Передача рисков включает решение разделить определённые риски с внешней стороны. Передача рисков может создать новые риски или изменить существующие, выявленные риски. Таким образом, может быть необходима дополнительная обработка риска. Передача может быть сделана путём страхования, которое защитит от последствий, или путём заключения контракта с партнёром, роль которого будет заключаться в мониторинге информационной системы и осуществлении немедленных действий для нейтрализации атаки, прежде чем будет причинён определённый уровень ущерба. Следует отметить, что можно передать ответственность за управление рисками, но обычно невозможно передать ответственность за воздействия. В таких случаях, как правило, негативные воздействия списываются на вину самой организации.

Список литературы

1. OHSAS 18001: 2007. Occupational health and safety management systems – Requirements.
2. Caballero, Albert. Chapter 14. Computer and Information Security Handbook. Morgan Kaufmann Publications, Elsevier Inc., 2009. 232 c.
3. ISO/IEC FIDIS 27005: 2008. Information technology – Security techniques – Information security risk management.
4. Open Web Application Security Project risk rating Methodology. URL.https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (дата обращения:10.04.2013).