УДК 004.056

АНАЛИЗ МЕТОДИК ПО СНИЖЕНИЮ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Беребин А.Ю., Юсупова А.Ю.
Кыргызский государственный университет строительства,
транспорта и архитектуры имени Н. Исанова

В статье рассматриваются процедура проведения оценки рисков информационной безопасности для создания эффективной системы управления риска информационной безопасности в предприятии. Приводятся меры безопасности, контрмеры и действия по каждой актуальной угрозе для снижения уровня риска информационной безопасности.

Ключевые слова: риск информационной безопасности, оценка рисков, снижение рисков, анализ рисков, управление информационной безопасности, количественная оценка, качественная оценка.

ИШКАНАДА МААЛЫМАТТЫК КООПСУЗДУК ТОБОКЕЛДИКТЕРИН АЗАЙТУУ БОЮНЧА УСУЛДАРДЫ ТАЛДОО

Беребин А.Ю., Юсупова А.Ю.
Н. Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт
жана архитектура университети

Макалада ишканада маалыматтык коопсуздук тобокелдиктерин башкаруунун сарамжалдуу системасын түзүү үчүн маалыматтык коопсуздук тобокелдиктерин баалоону жүргүзүү процедурасы каралган. Маалыматтык коопсуздук тобокелдигинин деңгээлин азайтуу үчүн коопсуздук чаралары, контрчаралар жана ар бир актуалдуу коркунучтар боюнча иш-аракеттер келтирилген.

Баштапкы сөздөр: маалыматтык коопсуздук тобокелдиги, тобокелдиктерди баалоо, тобокелдиктерди азайтуу, тобокелдиктерди талдоо, маалыматтык коопсуздукту башкаруу, сандык баалоо, сапаттык баалоо.

ANALYSIS OF METHODS TO REDUCE INFORMATION SECURITY RISKS AT ENTERPRISES

Berebin A. Yu., Yusupova A. Yu.
Kyrgyz State University of Construction, Transport and Architecture named after N. Isanov

The article discusses the procedure for conducting an information security risk assessment to create an effective information security risk management system in the enterprise. Security measures, countermeasures and actions for each current threat are given to reduce the level of risk of information security.

Keywords: information security risk, risk assessment, risk mitigation, risk analysis, information security management, quantitative assessment, qualitative assessment.

Современные условия вынуждают предприятия и компании использовать информационные системы для обеспечения эффективного выполнения процессов, значительно ускоряя и облегчая работу сотрудников предприятия.

В настоящее время с развитием информационных систем и их повсеместным внедрением на предприятиях зачастую не уделяется должного внимания вопросам обеспечения информационной безопасности, вследствие чего повышается уязвимость информационных систем, баз данных, а также невыполнение требований по защите персональных данных, что приводит к повышению вероятности санкций за несоблюдение соответствующего законодательства. В целях определения задач защиты информации необходимо оценить возможные риски информационной безопасности на предприятии. Результат проведенной оценки должен стать основой для выработки мер по снижению рисков информационной безопасности на предприятиях.

Оценка рисков осуществляется в трех шагах:

• Планирование. Разработка основы для успешной оценки рисков.

• Координированный сбор данных. Сбор информации о рисках в ходе координированных обсуждений рисков.

• Приоритизация рисков. Ранжирование выявленных рисков на основе непротиворечивого и повторяемого процесса.

Для проведения оценки требуется собрать данные о: активах организации, угрозах безопасности, уязвимостях, текущей среде контроля, предлагаемые элементы контроля.

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определяет следующие качественные классы активов: — высокое, среднее и низкое влияние на бизнес.

Для угроз указывается уровень воздействия в соответствии с концепцией многоуровневой защиты (уровни - физический, сети, хоста, приложения, данных).

Следующий шаг этапа оценки рисков - приоритизация рисков, т.е. создание упорядоченного по приоритетам списка рисков. Формирование данного списка сначала предлагается выполнить на обобщенном уровне, после чего описания наиболее существенных рисков детализируются. Итоговый уровень риска определяется исходя из уровня влияния и оценки частоты возникновения риска.

Формирование перечня рисков на уровне детализации является последней задачей процесса оценки рисков. В этом перечне каждому риску в итоге сопоставляется оценка в числовой (денежной) форме.

Далее определяется уровень подверженности воздействию, а затем производится оценка величины влияния. Каждому уровню подверженности воздействию сопоставляется значение в процентах, отражающее величину ущерба, причиненного активу, и называемое фактором подверженности воздействию. Майкрософт, рекомендует использовать линейную шкалу подверженности воздействию от 100 до 20%, которая может изменяться в соответствии с требованиями организации. Кроме того, каждой величине влияния сопоставляется качественная оценка: высокая, средняя или низкая.

Результирующий уровень вероятности определяется на основании двух значений: вероятности существования уязвимости в текущей среде и вероятности существования уязвимости, исходя из эффективности текущих элементов контроля. Каждое значение изменяется в диапазоне от 1 до 5. Определение оценки проводится на основе ответов на вопросы.

Уровень риска определяется как произведение оценок уровня влияния (от 1 до 10) и уровня вероятности (от 0 до 10). В результате уровень риска может принимать значения от 0 до 100.

В заключение процедуры оценки рисков, проводится количественный анализ.

Количественную оценку предлагается начать с активов, соответствующих описанию класса высокого влияния на бизнес. Для каждого актива определяется денежная стоимость с точки зрения его материальной и нематериальной ценности для организации. Для определения степени ущерба, которая может быть причинен активу, предлагается использовать ранее определенный уровень подверженности воздействию, на основе которого определяется одноименный фактор.

Как отмечал Шиляев С., что количественная оценка рисков применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями, выраженными в деньгах, процентах, времени, человекоресурсах и прочее. Метод позволяет получить конкретные значения объектов оценки риска при реализации угроз информационной безопасности.

При количественном подходе всем элементам оценки рисков присваивают конкретные и реальные количественные значения. Алгоритм получения данных значений должен быть нагляден и понятен. Объектом оценки может являться ценность актива в денежном выражении, вероятность реализации угрозы, ущерб от реализации угрозы, стоимость защитных мер и прочее.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Принять риск - значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск - значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск - значит переложить последствия от реализации риска на третье лицо, например с помощью страхования.

В результате количественной оценки рисков должны быть определены:

- ценность активов в денежном выражении;
- полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;
- частота реализации каждой угрозы;
- потенциальный ущерб от каждой угрозы;
- рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе.

К сожалению, не всегда удается получить конкретное выражение объекта оценки из-за большой неопределенности. В таком случае применяется качественный метод.

При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной

(низкий, средний, высокий), пятибалльной или десятибалльной шкале (0…10). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи.

Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

Как провести качественную оценку рисков:

1. Определить ценность информационных активов.

Ценность актива можно определить по уровню критичности (последствиям) при нарушении характеристик безопасности (конфиденциальность, целостность, доступность) информационного актива.

2. Определить вероятность реализации угрозы по отношению к информационному активу.

Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала (низкая, средняя, высокая).

3. Определить уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты.

Для оценки уровня возможности реализации угрозы также может использоваться трехуровневая качественная шкала (низкая, средняя, высокая). Значение возможности реализации угрозы показывает, насколько выполнимо успешное осуществление угрозы.

4. Сделать вывод об уровне риска на основании ценности информационного актива, вероятности реализации угрозы, возможности реализации угрозы.

Для определения уровня риска можно использовать пятибалльную или десятибалльную шкалу. При определении уровня риска можно использовать эталонные таблицы, дающие понимание, какие комбинации

показателей (ценность, вероятность, возможность) к какому уровню риска приводят.

5. Провести анализ полученных данных по каждой угрозе и полученному для нее уровню риска.

Часто группа анализа рисков оперирует понятием «приемлемый уровень риска». Это уровень риска, который компания готова принять (если угроза обладает уровнем риска меньшим или равным приемлемому, то она не считается актуальной). Глобальная задача при качественной оценке — снизить риски до приемлемого уровня.

6. Разработать меры безопасности, контрмеры и действия по каждой актуальной угрозе для снижения уровня риска.

Целью обоих методов является понимание реальных рисков ИБ компании, определение перечня актуальных угроз, а также выбор эффективных контрмер и средств защиты. Каждый метод оценки рисков имеет свои преимущества и недостатки.

Количественный метод дает наглядное представление в деньгах по объектам оценки (ущербу, затратам), однако он более трудоемок и в некоторых случаях неприменим.

Качественный метод позволяет выполнить оценку рисков быстрее, однако оценки и результаты носят более субъективный характер и не дают наглядного понимания ущерба, затрат и выгод от внедрения СЗИ.

Выбор метода следует делать исходя из специфики конкретной организации и задач, поставленных перед специалистом.

Для выполнения более специфических требований к безопасности необходимо разрабатывать индивидуальный, повышенный режим безопасности. Этот режим предусматривает стратегии работы с рисками разных классов, в которых реализуются следующие подходы:

- снижение рисков: многие риски могут быть снижены за счет использования простых и дешевых контрмер;

- неприятие риска: некоторые классы риска можно избежать с помощью выведения веб–сервера организации за пределы локальной сети;
- изменение характера риска: если невозможно уклониться от риска или уменьшить его, то лучше застраховать уязвимый объект;
- принятие риска: специалист должен знать остаточную ценность риска из–за невозможности сведения его к малой величине.

В результате, принимая во внимание все вышеперечисленные моменты, возможно создать достаточно эффективную систему управления риска информационной безопасности для предприятия.

В заключение отметим, что обязательным условием успешного управления информационными рисками является его непрерывность. Поэтому оценка информационных рисков, а также разработка и обновление планов по их минимизации должны производиться в организациях с определенной периодичностью, например раз в квартал. Периодический аудит системы управления рисками, проводимый независимыми экспертами, будет дополнительно способствовать минимизации рисков.

ЛИТЕРАТУРА

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.:ИД «Форум»: Инфра-М, 2012. - 416 с.
2. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность [Текст] / Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.: ил.
3. Симонов С. Технологии и инструментарий для управления рисками // Jet Info. – 2003. – № 2 (117). – С. 3–32.