ЕЛЕНА БАРАНОВА,
национальный исследовательский университет «Высшая школа экономики», *ekbaranova@hse.ru*

АЛЕКСАНДРА МАЛЬЦЕВА,
ООО «Первая международная букмекерская компания», *lebskaya92@mail.ru*

Анализ рисков информационной безопасности для малого и среднего бизнеса

В общем случае под риском понимают возможность наступления некоторого неблагоприятного события, влекущего за собой различного рода потери. Поскольку информация перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности, а приобрела ощутимый стоимостной вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации в случае ее искажения или утраты, проблема обеспечения информационной безопасности (ИБ) приобрела в настоящее время исключительное значение.

В России в последние годы принят ряд стандартов, регламентирующих деятельность в области информационной безопасности – это семейство ГОСТ Р ИСО/МЭК 27 000, основанное и соответствующее семейству международных стандартов на системы управления информационной безопасностью ISO/IEC 27 000. Эти стандарты определяют требования к системам управления информационной безопасностью, управлению рисками, метрики и измерения, а также руководство по внедрению. Это указывает на особое внимание государства к проблемам обеспечения информационной безопасности и подготовки специалистов в этой области. Однако темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Российской Федерации, отсюда возникает необходимость в решении следующих вопросов: в соответствии с какими критериями и показателями производить оценку эффективности системы защиты информации, как обеспечить оценку и мониторинг информационных рисков в организациях, особенно малого и среднего бизнеса (МСБ), поскольку на практике таким организациям необходимо получать не только результаты первоначальной оценки рисков ИБ, рекомендации по их снижению, но и простой в использовании и недорогой инструмент такой оценки.

Методология CORAS для анализа рисков информационной безопасности

Методология *Coras*, предназначенная для анализа рисков безопасности, предоставляет инструмент для моделирования рисков и угроз. Визуализация результатов оценки представляется в виде графа. Программный инструментарий распространяется свободно.

Методология анализа безопасности *Coras* включает в себя семь этапов.

- Вводная встреча. Целью этого этапа является полное понимание того, что подлежит анализу (что будет анализироваться). Во время этой встречи аналитики собирают информацию, основанную на представлениях заказчика.
- Отдельная встреча с представителями заказчика. Аналитики знакомят со своим пониманием полученной на первом этапе информацией и документами, к которым заказчик открыл доступ для аналитиков. На этом этапе идентифицируются первые угрозы, уязвимости, сценарии угроз и нежелательные инциденты.
- Третий этап включает усовершенствованное описание той ситуации, которую необходимо проанализировать, все предположения и другие сделанные предварительные условия. Он заканчивается, как только вся документация была одобрена заказчиком.
- Четвертый этап включает в себя идентификацию всех возможных потенциальных нежелательных инцидентов, а также угроз и уязвимостей.
- На этом этапе оцениваются последствия, которые будут в случае осуществления нежелательных инцидентов, а также вероятность этих инцидентов.
- Первичная полная картина рисков, которую редактируют.
- Обоснование и описание действий, предотвращающих угрозы.

Программный инструментарий, использующий данную методику, распространяется бесплатно, не требует значительных ресурсов для установки и применения. Методика проста в использовании и не требует специальных знаний. Недостатком методики является то, что в ней не предусмотрена периодичность проведения оценки рисков ИБ.

Матричный подход к анализу рисков информационной безопасности

Рассматриваемый метод анализа рисков ИБ связывает активы, уязвимости, угрозы и средства управления и определяет важность различных средств управления, соответствующим активам организации. Активы организации определяются как существенные с точки зрения защиты объекты, они могут быть как материальными, так и нематериальными.

Матричная методология использует три отдельных матрицы: матрицу уязвимостей, матрицу угроз и матрицу контроля, чтобы собрать необходимые данные для анализа рисков.

Матрица уязвимостей содержит связь между активами и уязвимостями в организации, матрица угроз содержит в себе отношения между уязвимостями и угрозами, а матрица контроля содержит связи между угрозами и средствами управления. Значение в каждой ячейке матрицы показывает ценность отношения между элементом строки и столбца. Используется следующая система оценок: низкая, средняя и высокая.

При первоначальном анализе рисков формируются списки активов, уязвимостей, угроз и средств управления. Матрицы заполняются путем добавления данных о связи элемента столбца матрицы с элементом строки. Наконец, данные из матрицы уязвимостей преобразуются и заносятся в матрицу угроз. Таким же образом данные из матрицы угроз переносятся в матрицу контроля, которая содержит относительную важность средств управления.

В таблице 1 представлен пример матрицы активов.

Таблица 1. Матрица активов

Шкала 0 – нет воздействия 1 – слабое воздействие 3 – умеренное воздействие 9 – сильное воздействие **Уязвимость**	**Активы и затраты**	**Торговые секреты**	**Конфиденциальная информация**	**Репутация**	**Потерянный доход**	**Затраты на восстановление**	**Информация**	**Аппаратные средства**	**Программное обеспечение**	**Обслуживание**	**Коммуникации**
Веб-сервер											
Вычислительный сервер											
Брандмауэр											
Маршрутизатор											
Клиентские узлы											
Базы данных											

Пусть есть m активов, относительная стоимость актива a_j Є$_j$ (j=1, n).
Также пусть c_{ij} – это воздействие уязвимости v_i на актив a_j.
Тогда совокупное воздействие уязвимости v_i на активы организации вычисляются по формуле:

$$V_i = \sum_{(j=1)}^{n} v_{ij} \times C_j$$

Таблица 2. Матрица угроз

Шкала 0 – нет воздействия 1 – слабое воздействие 3 – умеренное воздействие 9 – сильное воздействие **Уязвимость**	**Угроза**	**Отказ в обслуживании**	**Вредоносный код**	**Ошибки пользователя**	**Внутренние атаки**	**Спам**	**Физическое повреждение аппаратных средств**
Веб-сервер							
Вычислительный сервер							
Брандмауэр							
Маршрутизатор							
Клиентские узлы							
Базы данных							

В таблице 2 представлен пример матрицы угроз.
Пусть имеется p угроз, которые воздействуют на V уязвимостей, а d_{ki} – это потенциал воздействия угрозы t_k уязвимости v_i. Тогда относительное совокупное воздействие угрозы T_k определяется по формуле:

$$T_k = \sum_{(i=1)}^{m} d_{ki} \times V_i$$

Таблица 3. Матрица контроля

Шкала 0 – нет воздействия 1 – слабое воздействие 3 – умеренное воздействие 9 – сильное воздействие **Средства контроля**	**Угроза**	**Отказ в обслуживании**	**Вредоносный код**	**Ошибки пользователя**	**Внутренние атаки**	**Спам**	**Физическое повреждение аппаратных средств**
Брандмауэр							
Система обнаружения вторжений							
Обучение персонала							
Политика безопасности							
Конфигурация архитектуры сети							

В таблице 3 представлен пример матрицы контроля.
Пусть есть q средств управления, которые могут смягчить p угроз, а e_{lk} – воздействие средства контроля z_0 на угрозу t_k. Тогда относительное совокупное воздействие средств контроля Z_0 определяется по формуле:

$$Z_0 = \sum_{(l=1)}^{p} e_{0l} \times T_l$$

Матричный подход к определению рисков ИБ может легко использовать внутри любой организации. Методология обеспечивает удобные шаблоны, которые могут совершенствоваться со временем с увеличением количества доступной для анализа информации. Методология обеспечивает прозрачность процесса анализа и легко адаптируется к постоянно изменяющимся угрозам, уязвимостям и активам. Она полезна организациям для того, чтобы самостоятельно провести оценки риска ИБ.

Расчетная методика оценки рисков информационной безопасности

Данная методика предназначена для проведения оценки рисков ИБ в рамках построения или совершенствования системы ИБ в организациях малого и среднего бизнеса.

Основная задача методики заключается в том, чтобы определить численный показатель риска ИБ с целью принятия эффективных мер по защите информации. Предлагаемая методика оценки рисков позволяет выполнить полноценный анализ и оценку рисков без привлечения высококвалифицированных специалистов.

Обобщенный алгоритм проведения оценки рисков ИБ может быть представлен следующим образом.

Этап 1. Идентификация активов.
Этап 2. Определение риска несоответствия требований законодательства.
Этап 3. Разработка модели угроз.
Этап 4. Процедура количественного определения рисков.
Этап 5. Определение допустимого риска.

Процедуры оценки рисков ИБ как комплексного подхода выполняются сотрудниками предприятия совместно с руководящим звеном.

На первом этапе происходит идентификация активов. Эксперты проводят интервью с персоналом каждого подразделения или отдела с целью выявления используемых активов. При идентификации активов следует иметь в виду, что всякая система ИТ включает

в себя не только аппаратные средства, но и программное обеспечение. Описание информационных активов проводится путем построения бинарных отношений.

На втором этапе определяется риск несоответствия законодательству в области ИБ. Любая организация, имеющая ИС или работа которой связана с использованием ИТ для ведения бизнеса, должна соблюдать федеральные законы, действующие в этой отрасли. Невыполнение данных требований может повлечь за собой гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством РФ, ответственность. Риск невыполнения требований законодательства влияет на общий риск ИБ. Алгоритм определения риска несоответствия требованиям законодательства в области ИБ включает в себя проведение всестороннего анализа состояния системы защиты с целью выявления выполнения требований в соответствии с требованиями законодательства. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение 1, в противном случае – значение 0. Все требования, которым присвоено значение 1, суммируются, остальные значения не учитываются. После чего необходимо определить уровень риска несоответствия требованиям по ИБ (R_n) по соответствию значений, представленных в таблице 4.

На третьем этапе разрабатывается модель угроз. Определение вероятности наступления неблагоприятных событий определяется экспертом или группой экспертов, занимающихся разработкой модели угроз. Также экспертным методом определяется и актуальность угроз ИБ.

После завершения оценки угроз составляется перечень актуальных идентифицированных угроз на каждый идентифицированный актив или группу активов, подверженных этим угрозам. Весь процесс составления перечня актуальных угроз проводится с использованием теории графов, с помощью которой описывается методика актуализации угроз.

Таблица 4. Значения риска несоответствия требованиям законодательства

Сумма выполненных требований	Риск несоответствия требованиям законодательства
13-14	0,01
8-12	0,25
Менее или равно 7	0,5
Не выполняются	0,9

На четвертом этапе проводится количественная оценка рисков ИБ. Процедура количественной оценки рисков ИБ включает в себя следующие шаги.

- Выбор актуальных угроз частной модели угроз. При помощи частной модели угроз формируется перечень актуальных угроз ИБ. Идентифицированные активы сопоставляются с направленными на них угрозами.
- Определение вероятности наступления угрозы. Так как на один актив могут воздействовать одновременно несколько угроз, необходимо определить вероятность того, что хотя бы одна угроза реализуется по отношению к выбранному активу. Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз $y_1, y_2, \ldots, y_n$, где n – количество угроз, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.
- Определение ценности актива. Ценность актива определяется его стоимостью. В связи с тем, что зачастую нельзя определить точные стоимости активов и предприятия в целом, рекомендуется ценность актива задавать в диапазоне от 0 до 1, которая будет показывать отношение цены актива к стоимости всего бизнеса. В данной методике оценка стоимости активов осуществляется владельцем организации совместно с экспертом (группой экспертов).
- Определение возможности использования организационных и технических уязвимостей. Возможность использования организационных уязвимостей проводится экспертным методом. При этом анализируются применяемые организационные меры защиты информации. В ходе проведения анализа всем организационным мерам, которые выполняются, присваивается значение 1. Всем мерам, которые не выполняются, присваивается значение 0. Все значения 1 для организационных мер, которые выполняются, суммируются, и по полученному значению определяется коэффициент уязвимости организационных мер защиты информации ($К_О$). Соответствие значения суммы выполняемых организационных мер защиты информации и значения коэффициента уязвимости организационных мер защиты информации представлено в таблице 5.

Таблица 5. Соответствие значений суммы выполняемых организационных мер защиты информации и коэффициента уязвимости организационных мер защиты информации

Сумма выполняемых мер защиты	Коэффициент уязвимости организационных мер защиты
14-17	0,01
8-13	0,25
Менее 8	0,5
Не выполняются	0,9

Таблица 6. Соответствие значений суммы выполняемых технических мер защиты информации и коэффициента уязвимости технических мер защиты информации

Сумма выполняемых мер защиты	Коэффициент уязвимости технических мер защиты
15-19	0,01
9-14	0,25
Менее 9	0,5
Не выполняются	0,9

Возможность использования технических уязвимостей проводится экспертным методом, в ходе которого анализируются выполняемые технические меры защиты информации. В ходе проведения анализа всем техническим мерам, которые выполняются, присваивается значение 1, всем мерам, которые не выполняются, присваивается значение 0. Все значения 1 для технических мер, которые выполняются, суммируются, и по полученному значению определяется коэффициент уязвимости технических мер защиты информации (K_t). Соответствие значения суммы выполняемых технических мер защиты информации и значения коэффициента уязвимости технических мер защиты информации представлено в таблице 6.

● Вычисление численного значения риска. В данной методике оценка рисков реализации хотя бы одной угрозы ИБ основывается на взаимности нескольких факторов: вероятности реализации хотя бы одной актуальной угрозы, коэффициента ценности актива, среднеарифметического значения коэффициента возможностей использования технических и организационных уязвимостей и риска несоответствия требованиям законодательства. Под коэффициентом ценности актива понимается ценность или критичность актива по отношению к стоимости всего бизнеса.

В данной методике процедура количественной оценки рисков реализации хотя бы одной угрозы из всего перечня актуальных угроз по отношению к конкурентному активу определяется относительно каждого типа актива, на который воздействует совокупность угроз ИБ, что позволяет дискретно определить риск наступления неблагоприятных событий на каждый тип актива.

Риск реализации хотя бы одной угрозы из всего перечня актуальных угроз с учетом наличия уязвимостей по отношению к конкурентному активу определяется по общей формуле:

$$R = R_{угр} \times R_n \times C \times \frac{K_o + K_t}{2} \times 100\ \%$$

где R – численная величина риска реализации угроз ИБ;

$R_{угр}$ – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз;

R_n – риск несоответствия требованиям законодательства;

C – ценность актива;

K_o – вероятность использования организационных уязвимостей;

K_t – вероятность использования технических уязвимостей.

Далее определяется допустимый уровень риска. Для организаций малого и среднего бизнеса рекомендованное значение риска не должно превышать 5 %.

© DEPOSITPHOTOS.COM/DEYWEB

Таблица 7. Сравнение методик анализа рисков для организаций МСБ

Критерии сравнения	CORAS	Матричный подход	Расчетная методика
Методика рассчитана на организации МСБ	1	1	1
Методика рассчитана на организации различных областей деятельности	1	1	1
Простота использования	1	1	1
Бесплатное использование	1	1	1
Количественная оценка	0	1	1
Качественная оценка	1	1	1
Повышение информированности сотрудников	1	1	1
Пригодность к регулярному использованию	0	1	1
Использование независимой оценки	1	0	0
ИТОГО:	7	8	8
Ресурсы	1	1	1
Ценность ресурсов	1	1	1
Угрозы	1	1	1
Уязвимости	1	1	1
Выбор контрмер	1	1	0
Базовые требования в области безопасности	0	0	0
Потери	0	0	0
Меры защиты информации	0	0	1
Частота возникновения угроз	0	0	0
Сетевое оборудование	0	0	0
Виды информации	0	0	0
Группы пользователей	0	0	0
СЗИ	0	1	1
ИТОГО:	5	6	6

Для управления рисками ИБ в организациях малого и среднего бизнеса приемлемыми являются все рассмотренные методики

Выполнение всех этапов оценки рисков ИБ повторяется для каждого типа актива. Полученное значение риска ИБ необходимо для выработки рекомендаций по снижению уровня риска и принятия эффективных мер по обеспечению ИБ в организации.

Методика разработана для использования в организациях без привлечения сторонних специалистов, проста в использовании и не требует использования программного инструментария.

Сравнение эффективности рассмотренных методик для организаций малого и среднего бизнеса приводится в таблице 7.

Для управления рисками ИБ на базе периодических оценок в организациях малого и среднего бизнеса наиболее приемлемыми являются все рассмотренные методики, поскольку на практике таким организациям необходимо получать не только результаты первоначальной оценки рисков ИБ, рекомендации по их снижению, но и простой в использовании и недорогой инструмент такой оценки. ●

Источники:

Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. 2015 № 1 (9). С. 73–79.
Баранова Е.К., Зубровский Г.Б. Управление инцидентами информационной безопасности. Проблемы информационной безопасности / Труды I Международной научно-практической конференции «Проблемы информационной безопасности» Гурзуф, Крымский федеральный университет им. В. И. Вернадского, 26–28 февраля 2015 г. С.27–33.
Баранова Е.К., Чернова М. Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 160–168.
Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: РИОР:ИНФРА-М, 2014.
Баранова Е.К., Бабаш А.В. Практикум по моделированию систем защиты информации: учебное пособие. – М.:РИОР:ИНФРА-М, 2014.
Белов В.М., Плетнев П.В. Методика оценки рисков информационной безопасности на предприятиях малого бизнеса. Доклады ТУСУРа. 2012. № 1. С. 83–86
Goel S., Chen V. Information security risk assessment – a matrix-based approach. University at Albany, SUNY. 2005