ИНФОРМАТИКА
ИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 519.688

Методика оценки рисков реализации угроз при обработке информации в автоматизированных системах Организации

А. Л. Лобков
Пермский государственный национальный исследовательский университет
Россия, 614990, г. Пермь, ул. Букирева, 15
armando.lobkov@yandex.ru; 89026444152

Рассматриваются вопросы, связанные с оценкой рисков информационной безопасности, возникающих в автоматизированных системах, обрабатывающих информационные активы Организации. В качестве оценки рисков предлагается пошаговая математическая модель, сформированная в "Методику оценки рисков реализации угроз при обработке информации в автоматизированных системах Организации" (далее – Методика). Разработанная Методика позволяет оценить величину рисков приводящих к реализации угроз информационным активам Организации при их обработке в автоматизированных системах. Основная решаемая задача Методики заключается в том, чтобы определить численный показатель риска информационной безопасности с целью принятия мер по защите информационных активов при их обработке в автоматизированных системах Организации.

Ключевые слова: *информационный актив; анализ риска; оценивание риска; обработка риска; информационная безопасность.*

DOI: 10.17072/1993-0550-2019-4-72-75

Оценка рисков информационной безопасности представляет собой процесс, состоящий из анализа данного риска и его оценки с заданными критериями. Полученные результаты оценки рисков помогают в определении выбора конкретных мер и приоритетов в области менеджмента рисков информационной безопасности, а также внедрению мер, средств контроля и управления, выбранных для защиты автоматизированной системы Организации от этих рисков.

При проведении оценки каждому риску присваивается реальное процентное значение, в результате которого возможно применение конкретных мер защиты организационного или технического характера структуры автоматизированной системы.

Алгоритм получения значений оценки рисков информационной безопасности при обработке информационных активов должен быть нагляден и понятен, что и подтверждает разработанная Методика. Рассмотрим алгоритм оценки рисков информационной безопасности при обработке информационных активов Организации средствами автоматизации на основе представленной Методики.

Алгоритм оценки рисков информационной безопасности при обработке информационных активов включает в себя следующие этапы:

– Этап № 1. Идентификация информационных активов и средств их обработки.

– Этап № 2. Разработка Модели угроз.

– Этап № 3. Процедура количественной оценки рисков.

– Этап № 4. Определение допустимого уровня риска реализации актуальных угроз.

Этап № 1. Идентификация информационных активов и средств их обработки

На этапе идентификации определяются критически важные информационные активы (метод определения – анкетирование работников подразделений, допущенных к обработке информационных активов в соответствии с их функциональными обязанностями), обрабатываемые с использованием и без использования средств автоматизации в Организации, а также технические средства (активы), предназначенные для их обработки.

К информационным активам относятся:

– информация/данные (электронные файлы, папки и т.п.);

– программное обеспечение, включая прикладные программы;

– документы и т.д.

К средствам (активам), предназначенным для обработки информационных активов относятся:

– аппаратные средства (компьютеры, принтеры и т.п.);

– программно-аппаратные средства (электронные носители);

– электронное оборудование, обеспечивающее необходимые условия работы и т.п.

Этап № 2. Разработка Модели угроз и определение коэффициента уязвимости

Для каждой автоматизированной системы, предназначенной для обработки информационных активов, разрабатывается Модель угроз. На ее основе производится оценка возможных угроз информационным активам при их автоматизированной обработке. Относительно каждой угрозы рассчитывается коэффициент ее реализуемости (*Y*), а также определяется ее актуальность.

Расчет коэффициента реализуемости (Y) производится в соответствии с руководящим документом [4] по формуле

$$\mathrm{Y} = \frac{\mathrm{Y}_1 + \mathrm{Y}_2}{20}, \qquad (1)$$

где: Y_1 – числовой коэффициент исходной защищенности информационной системы, предназначенной для обработки информационных активов (табл. 1 документа [4]).

В соответствии с документом [4] числовой коэффициент Y_1 может принимать следующие значения:

- 0 – высокая степень исходной защищенности;
- 5 – средняя степень исходной защищенности;
- 10 – низкая степень исходной защищенности.

Y_2 – числовой коэффициент вероятности угрозы, возникающей в автоматизированной системе, предназначенной для обработки информационных активов. В соответствии с документом [4] числовой коэффициент вероятности угрозы Y_2 может принимать следующие значения:

- 0 – малая вероятность угрозы;
- 2 – низкая вероятность угрозы;
- 5 – средняя вероятность угрозы;
- 10 – высокая вероятность угрозы.

По значению коэффициента реализуемости угрозы (*Y*) формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если $0 \le \mathrm{Y} \le 0{,}3$, то возможность реализации угрозы признается низкой;

– если $0{,}3 \le \mathrm{Y} \le 0{,}6$, то возможность реализации угрозы признается средней;

– если $0{,}6 \le \mathrm{Y} \le 0{,}8$, то возможность реализации угрозы признается высокой;

– если $\mathrm{Y} > 0{,}8$, то возможность реализации угрозы признается очень высокой.

В соответствии со значениями коэффициента реализуемости угрозы определяем меру разброса случайной величины, т. е. ее отклонения от математического ожидания (дисперсию), по формуле

$$D(\mathrm{Y}) = M(\mathrm{Y}^2) - M^2(\mathrm{Y}), \qquad (2)$$

где: $M(\mathrm{Y}) = \sum_{i=1} \mathrm{Y}_i P_i$ – математическое ожидание; P_i – вероятность возникновения события.

На основании формулы (2) просчитываем риски наступления вероятности данного события по формуле

$$\delta = \sqrt{D(\mathrm{Y})}. \qquad (3)$$

На основании полученных данных в соответствии с формулой (3) оцениваем вербальную интерпретацию реализации угрозы, в соответствии с которой определяем коэффициент

уязвимости K_t (коэффициент уязвимости выбирается в пределах $a_i < \frac{\delta}{4} + \mathrm{Y} < b_i$, где a_i – начало промежутка расчета; b_i – конец промежутка расчета).

Полученные данные расчетов сведены в табл. 1.

Этап № 3. Процедура количественной оценки рисков

Процедура количественной оценки рисков информационной безопасности при обработке информационных активов включает в себя следующие шаги:

Шаг 1. Определение численного коэффициента реализуемости угрозы.

Таблица 1

Коэффициент реализуемости угрозы (Y)	Низкий $0 \le \mathrm{Y} \le 0{,}3$	Средний $0{,}3 \le \mathrm{Y} \le 0{,}6$	Высокий $0{,}6 \le \mathrm{Y} \le 0{,}8$	Очень высокий $\mathrm{Y} > 0{,}8$
Y	1	2	3	4
Y^2	1	4	9	16
Вероятность возникновения события P_i	0,25	0,25	0,25	0,25
Коэффициент уязвимости K_t	0,2	0,3	0,5	0,7

Для каждой угрозы, возникающей в автоматизированной системе, предназначенной для обработки информационных активов, рассчитывается коэффициент ее реализуемости в соответствии с формулой (1).

Шаг 2. Выбор актуальных угроз.

Производится из разработанной Модели угроз для каждой автоматизированной системы, предназначенной для обработки информационных активов (алгоритм выбора актуальных угроз отражен в Модели угроз для конкретной информационной системы).

Шаг 3. Вычисление численного значения риска реализации угрозы информационной безопасности (информационным активам).

Определение риска реализации угрозы с учетом наличия уязвимостей по отношению к информационным активам, обрабатываемым в автоматизированной системе, выражается через следующую формулу:

$$R = \mathrm{Y} * K_t * 100\,\%. \qquad (4)$$

Этап № 4. Определение допустимого уровня риска реализации актуальных угроз

В соответствии с формулой (4) рассчитываются уровни риска реализации актуальных угроз. Полученные значения допустимого уровня риска реализации актуальных угроз сведены в табл. 2.

Таблица 2

Коэффициент реализуемости угрозы (Y)	Низкий $0 \le Y \le 0{,}3$	Средний $0{,}3 \le \mathrm{Y} \le 0{,}6$	Высокий $0{,}6 \le Y \le 0{,}8$	Очень высокий $\mathrm{Y} > 0{,}8$
Коэффициент уязвимости K_t	0,2	0,3	0,5	0,7
Численная величина риска реализации угрозы R в процентном соотношении	0 – 6 %	9 – 18 %	30 – 40 %	Более 60 %

Исходя из полученных значений табл. 2, в соответствии с ценностью информационных активов (уровни значимости) обрабатываемых в автоматизированной системе, а также в соответствии с классом автоматизированной системы (рассчитывается в Модели угроз) принимается решение о принятии организационных или технических мер защиты информации (информационные активы), обрабатываемой в автоматизированной системе.

Список литературы

1. *Национальный* стандарт РФ ГОСТ Р ИСО/МЭК 27002-2012. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. 2012.
2. *Национальный* стандарт РФ ГОСТ Р ИСО/МЭК ТО 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. 2010.
3. *Приказ* ФСТЭК от 11 февраля 2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах". 2013.
4. *Методика* определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России от 14 февраля 2008 г.).
5. *Базовая* модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России от 15 февраля 2008 г.).
6. *Айвазян С.А., Енюков И.С., Мешалкин. Л.Д.* Основы моделирования и первичная обработка данных. М.: Финансы и статистика, 1983. 471 с.
7. *Лазарев И.А.* Информация и безопасность. Композиционная технология информационного моделирования сложных объектов принятия решений. М.: Московский городской центр научно-технической информации, 1997. 336 с.

Technique for assessing the risk of threat materializing when processing data in automated systems of Organization

A. L. Lobkov
Perm State University; 15, Bukireva st., Perm, 614990, Russia
armando.lobkov@yandex.ru; 89026444152

The paper considers issues related to the assessment of risks to information security arising in automated systems that process Organization's information assets. There is proposed a step-by-step mathematical model presented as 'Technique for assessing the risk of threat materializing when processing data in automated systems of Organization'. The developed technique allows one to estimate the extent of risks that result in materializing of threats to Organization's information assets when those are being processed in automated systems. The main problem solved with the help of this technique is determination of the numerical value for the information security risk, which is done in order to take measures to protect information assets.

Keywords: *information asset; risk analysis; risk assessment; risk treatment; information security.*