УДК: 004.056.5

Инструменты выбора метода аудита информационной безопасности предприятия

Вакуленко А.А. nastasi06@yandex.ru
Сорокопудов Н.С. 640kilo@gmail.com
Д-р. экон. наук **Коваленко Б.Б.**
Университет ИТМО
197101, Россия, Санкт-Петербург, Кронверкский пр., д. 49

Для современных предприятий автоматизация бизнес-процессов с использованием средств вычислительной техники и телекоммуникаций являются неотъемлемой частью их развития. Ключевую роль в обеспечении эффективности работы коммерческих и государственных предприятий играют информационные системы. Несвоевременное обнаружение недостатков таких систем влияет на эффективность и надежность систем информационной безопасности. Для обеспечения успешного функционирования и развития информационных систем, аудит информационной безопасности является незаменимым инструментом исследования и оценки их состояния. В данной статье рассматривается проблемавыбора оптимального метода проведения аудита информационной безопасности предприятия. Для решения проблемы предлагается проведениеанализа методик аудита информационной безопасности. Приводятся основные методы проведения аудита информационной безопасности и их особенности. В качестве инструмента для выбора метода аудита информационной безопасности взяты два вида анализа: SWOT-анализ и FMEA-анализ. Описаны поэтапно алгоритмы расчёта количественных показателей этих методов. Сделан вывод о вкладе служб внутреннего аудита в обеспечении информационной безопасности предприятия, его влиянии на принятие управленческих решений, конкурентоспособность. Подведён итог эффективности выбранных для проведения анализа методов аудита информационной безопасности, как по отдельности, так и в совокупности.
Ключевые слова: аудит информационной безопасности, обеспечение информационной безопасности предприятия/методы проведения аудита, SWOT-анализ, анализ FMEA.

DOI: 10.17586/2310-1172-2019-12-3-163-169

The selection tools of information security audit's of the enterprise method

Vakulenko A.A. nastasi06@yandex.ru
Sorokopudov N.S. 640лkilo@gmail.com
D.Sc. **Kovalenko B.B.**
ITMO University
197101, Russia, St. Petersburg, Kronverksky pr., 49

For modern enterprises to automate business processes using computer technology and telecommunications are an integral part of their development. A key role in ensuring the efficiency of commercial and state enterprises play an information system. Late discovery of shortcomings of such systems affects the efficiency and reliability of information security systems. To ensure the successful functioning and development of information systems, information security audit is an indispensable tool of research and evaluation. This article considers the problem of selecting the optimal method of audit of information security of the enterprise. To solve the problem, we propose the analysis of methods of audit of information security. The principal methods of audit of information security and their features.Two types of analysis are taken as a tool for choosing the method of information security audit: SWOT-analysis and FMEA-analysis. Step-by-step algorithms for calculating quantitative indicators of these methods are described. The conclusion is

made about the contribution of internal audit in ensuring the information security of the enterprise, its impact on managerial decision making and competitiveness.The results of the effectiveness of the chosen methods of information security audit both individually and in the aggregate are summarized.
Keywords: information security audit /information security enterprise development business systems enterprise information security/audit methods/SWOT Analysis/FMEA Analysis.

Введение

Достижение целей предприятия в настоящее время все больше зависит от грамотной организации информационного потока предприятия. Связано это с тем, что большой объемстратегически важных для компании данных обрабатываются в корпоративной информационной системе. Тем же объясняются и активное капиталовложение в информационные системы компании. Поэтому, качественное проведение аудита информационной безопасности занимает важное место при получении достоверной информации о функционировании предприятия в целом.[1]

Аудит информационной безопасности является незаменимым инструментом исследования и оценки информационной системы, обеспечения её успешного функционирования и развития. Задача, которую преследует информационный аудит лежит в своевременной и точной оценке состояния безопасности информации в текущий момент конкретного предприятия, а также соответствие поставленной цели и задачи ведения деятельности, с помощью которого должно производиться повышение рентабельности и эффективности экономической деятельности. [2] Иными словами, «аудит информационной безопасности» - системный процесс получения объективных количественных и качественных оценок, характеризующих текущее состояние системы информационной безопасности предприятияпо определенным критериям и показателям безопасности [3].

Объект исследования

Выбор метода проведения аудита информационной безопасности является важнейшим этапом в организации самого аудита информации, от которого зависит дальнейшие результаты его проведения. На сегодняшний день можно выделить следующие три основных метода проведения аудита информационной безопасности[4]:

- Активный аудит. Подразумеваетанализ состояния защищенности информационной системы с точки зрения злоумышленника, который обладает высокой квалификацией в исходной области.
- Экспертный аудит (проведение сравнительного анализа состояния информационной безопасности с «идеальным») [5]
- Аудит на соответствие нормативным документам (исходная системаинформационной безопасности исследуется на соответствие требованиям стандартов)

В процессе научного исследования и подготовки к написанию диссертации была поставлена проблема выбора эффективного метода проведения аудита информационной безопасности на предприятии. В качестве метода нахождения оптимального решения поставленной проблемы был выбран SWOT -анализ (оценка сильных и слабых сторон аудита информационной безопасности предприятия.Данный способ предоставил возможность на основании исходных характеристик компании с участием руководителя и компетентных сотрудниковсделать выводы о рисках, возможностях, необходимости стратегических изменений; выявить оптимальный метод проведения аудита информационной безопасности конкретного предприятия. Были построены SWOT-матрицы и приведены формулы для поиска оптимального метода проведения аудита информационной безопасности предприятия.

Анализ методов аудита информационной безопасности

В настоящее время значительно выросло количество малого бизнеса. Для полноценного стратегического анализа систем у небольших предприятий часто недостаточно компетентных сотрудников и средств. В полном объеме он доступен лишь крупным компаниям. В условиях постоянно изменяющейся информационной среды компаниям становится трудно поддерживать и контролировать состояние всех систем бизнеса. Поэтому, встаёт вопрос об использования оптимальных для размера предприятия, его капитала и преследуемых предприятием целей вариантов стратегий. В то же время, крупные предприятия не могут поставить знак равенства между затраченными на исследование средствами и эффективностью проведения данного исследования. [6]

Метод SWOT-анализа для выбора метода проведения аудита информационной безопасности

В качестве основного инструмента регулярного стратегического управления многие компании используют матрицу «качественного» стратегического анализа - еще SWOT матрица (с английского:Strengths - силы; Weaknesses - слабости; Opportunities - возможности; Threats - угрозы).

Для максимально объективного отражения результатов методов аудита информационной безопасности, информационное поле формируется компетентными лицами. Это могут быть как осведомленные в исходной области (ИБ) сотрудники, так и само руководство компании, с учетом собственного опыта и видения ситуации[7].

При этом исчезает необходимость использования дорогостоящих систем «количественного» анализа и привлечения коммерческихорганизаций по аудиту со стороны. Следует так же учитывать актуальность для выбранного решения во времени. Если оно реализовано слишком поздно, эффективность его может быть равной «нулю». В данной исследовательской работе SWOT-анализ используется для определения сильных и слабых сторон существующих методов аудита информационной безопасности на конкретном предприятии, а так же для определения возможностей выбранных методов и факторов, препятствующих реализации этих методов[8]. Методология SWOT-анализа предполагает сначала выявление сильных и слабых сторон, а также угроз и возможностей методов аудита информационной безопасности предприятия.

Таблица 1

ФакторыSWOT-анализа «Активный аудит»

Сильные стороны	**Слабые стороны**
Автоматизация процесса; Возможность специализированной проверкиконкретного ПО; «Стресс»- тест (создание атак некого злоумышленника при отказе в обслуживании); Исследование информационной системы на производительность и стабильность; Возможность проведения проверки без участия сотрудников компании.	Вероятность необходимости в дополнительном программном обеспечении; Получение результатов аудита по текущему состоянию системы, не отражает уязвимостей при изменении состояния системы; Функционирование системы прекращается на время проведения аудита.
Возможности	**Угрозы**
*(Заполняется руководителем и/или компетентными сотрудниками компании на основании обобщения и согласования существующих возможностей предприятия при использовании метода «активного аудита» информационной безопасности)	Большие капиталовложения в требуемое программное обеспечение, а так же в дополнительное ПО; Узкая направленность программного обеспечения для проведения аудита; Вероятность возникновения ошибок при использовании программного обеспечения для проведения аудита; Отсутствие нормативной базы для проведения аудита.

Таблица 2

Факторы SWOT-анализа «Экспертный аудит»

Сильные стороны	**Слабые стороны**
Не регламентированная частота проведения аудита; Возможность непрерывного функционирования информационной системы при проведении аудита; Отсутствие затрат на дополнительное программное обеспечение; Предыдущие заключения по аудиту учитываются в текущих проверках информационных систем; Распределение компонентов информационной системы по значимости; Покрытие большого количества уязвимостей.	Необходимость привлечения сотрудников предприятия для проведения аудита; Высокие требования к объективности информации, предоставляемой заказчиком; Трудоемкий сбор и анализ данных; Вероятность длительного проведения процедуры аудита.
Возможности	**Угрозы**
*(Заполняется руководителем и/или компетентными сотрудниками компании на основании обобщения и согласования существующих возможностей предприятия при использовании метода экспертного аудита информационной безопасности)	Отсутствие автоматизации процесса; Компетентность экспертов.

Таблица 3

Факторы SWOT-анализа «Аудит на соответствие стандартам»

Сильные стороны	Слабые стороны
Процедура проведения аудита информационной системы регламентируется соответствующими стандартами; Отсутствует необходимость затрат на дополнительное программное обеспечение; Непрерывное функционирование проверяемой информационной системы на момент проведения проверки; Наличие описания отчетных документов в нормативных документах.	Необходимость привлечения сотрудников предприятия для участия в процедуре аудита; При любых изменениях состояния информационной системы требуется проведение повторного аудита; Высокие требования к объективности данных, предоставляемых заказчиком; Вероятность длительного проведения процедуры аудита.
Возможности	**Угрозы**
*(Заполняется руководителем и/или компетентными сотрудниками компании на основании обобщения и согласования существующих возможностей предприятия при использовании метода проведения аудита на соответствие стандартам)	Большая нормативная база; Постоянное обновление правовых документов; Возможность наличия противоречий в нормативных документах; Не односторонний процесс аудита (необходимость привлечения аккредитированной организации).

Определим следующие значения для перехода от качественных к количественным характеристикам:

- коэффициент значимости фактора (K_imp_i);
- наблюдаемое значение влияния фактора (F_inf_i);
- степень неопределенности суждения (F_prob_i);

Значимость каждого фактора вычисляется по формуле:

$$F\_val_i = F\_inf_i * F\_prob_i$$

Тогда **общая сумма значимости** всех факторов для каждого параметра:

$$Val = \sum_{i=1}^{n} K\_imp_i * F\_val_i \quad [9]$$

Технология FMEA-анализа методов аудита информационной безопасности

Для выбора оптимального метода аудита информационной безопасности будет целесообразно рассмотреть все риски, связанные с выбором каждого из вышеперечисленных методов с помощью еще одного инструмента - анализа FMEA.

Анализ видов и последствий отказов - метод FMEA (Failure Modeand Effects Analysis) или Анализ видов и последствий потенциальных дефектов, требования к которому внесены в целый ряд стандартов МЭК (напр. серия МЭК 60300-2003 и МЭК 60812-1985) , национальных стандартов (напр. стандарты серий ГОСТ Р 27.002-89, ГОСТ Р 27.301-95 и ГОСТ Р 27.310-95), отраслевых (напр. стандарты серии ГОСТ Р 51814) и др.[10]

FMEA-анализ позволяет выявить дефекты, обуславливающие наибольший риск потребителя, определить их потенциальные причины, разработать предупреждающие и корректирующие действия, чем фактически предотвратить потенциальные затраты на исправление дефектов. [11]

Исходная технология изображена на схеме 1.

На первом этапе происходит сбор всем полезных для проведения исследования данных о каждом методе для проведения аудита.

Второй этап включает в себя построение 3х моделей. Компонентный анализ проводится для выявления частей (компонентов), из которых состоит данный процесс. В результате этого анализа строится компонентная модель процесса проведения аудита информационной безопасности одним из трёх методов, представляющая собой список элементов процесса. Структурный анализ направлен на выявление взаимодействий между компонентами и их соподчиненности. На основе функционально-структурной модели процесса проведения аудита информационной безопасности исходным методом производства можно определить возможные риски, которые могут возникнуть при нарушении той или иной функции любым из структурных элементов [12].

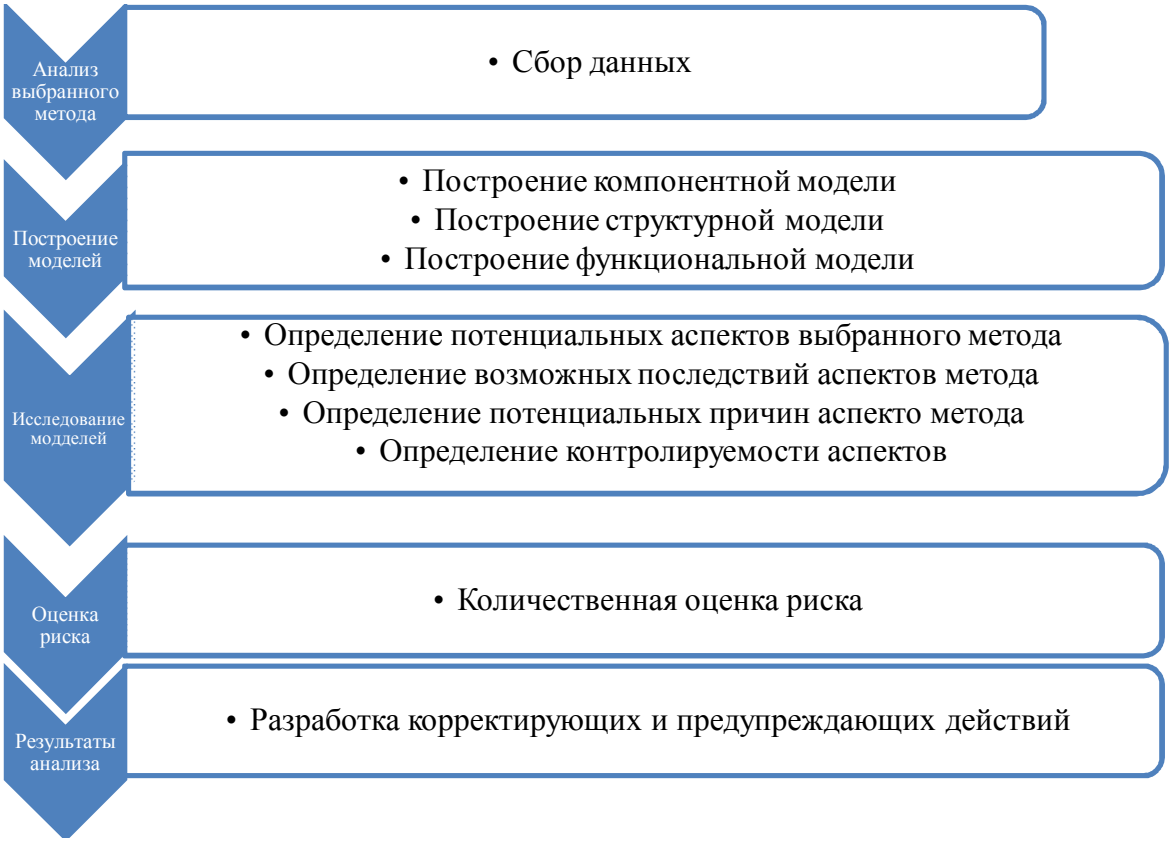

Схема 1. Алгоритм FMEA-анализа метода аудита информационной безопасности

На этапе оценки рисков выбранного метода аудита производится составление таблицы FMEA-анализа по результатам проведенных исследований (табл. 4).

Таблица 4

FMEA-анализ для заполнения

Операция	**Вид потенциального отказа**	**Последствие**	**S**	**Потенциальная причина**	**O**	**Действующие меры по обнаружению**	**D**	**ПЧР**
*(Заполняется на основе построенной компонентной модели)	*(Заполняется на основе построенной функциональной модели)	*(Заполняется на основе построенной структурной модели)	-	*(Заполняется на основе анализа причин отказов, диаграмма Исикавы)	-	-	-	-

Количественную оценку комплексного риска несоответствий проводят на основе вычисления ПЧР (приоритетное число риска), где ПЧР = S × O × D. Эксперты выставляют оценки для составляющих ПЧР (S, O, D) в соответствии со шкалами, приведенными в построенных этими экспертами таблицах специально для выбора метода аудита информационной безопасности с учетом специфики процесса[13].

Значение ПЧР находиться в диапазоне от 1 до 1000. В случае, если фактическое значение ПЧР превосходит ПЧРгр (100–120), по результатам анализа должны разрабатываться и внедряться предупреждающие действия для снижения или устранения риска последствий. Если фактическое значение находится в пределах приемлемого (не более ПЧРгр), то объект анализа не является источником существенного риска и предупреждающих действий не требуются. В любом случае, по результатам анализа необходимо разрабатывать и внедряться предупреждающие действия для снижения или устранения риска последствий[14].

Анализ результатови рекомендации по их применению

По результатам всех 3х вычислений методом FMEA-анализа, метод аудита, чей показатель ПЧР имеет наименьшую величину - наиболее оптимальным для проведения аудита информационной безопасности на текущий момент.

После проведения расчетов методом SWOT-анализа, можно сделать вывод о том, какой метод проведения аудита информационной безопасности является оптимальным для данной организации на данный момент времени.Результаты аудита позволяют построить оптимальную по эффективности и затратам систему менеджмента информационной безопасности, которая соответствует текущим задачам и целям предприятия[15].

Два предложенных метода выбора аудита информационной безопасности можно использовать так же в совокупности. Если по результатам обоих расчётов будет выбран один и тот же метод, это может свидетельствовать об объективности проведенного анализа. В противном случае, есть основания для более детального исследования текущих сильных сторон, слабостей, рисков и уязвимостей информационной системы предприятия.

Литература

1. *Макаренко С.И.* Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. №1 С. 1-29;
2. *Хлестова Д.Р., Байрушин Ф.Т.* Аудит информационной безопасности в организации // Символ науки. 2016. № 11-3 (23). С. 175-177;
3. *Кравчук Д. И., Коркушко Д.А.* Аудит безопасности корпоративных информационных систем // Молодой ученый. 2015. №10. 755 с.
4. *Филяк П.Ю., Шварев В.М.* Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности// Информация и безопасность. 2015. №4. С. 5803-583;
5. *Просянников Р.Е.* Избавиться от заблуждений. Виды аудита информационной безопасности // Connect! Мир связи. 2004. № 12.С. 148–151;
6. *Гапоненко А.Л., Панкрухин А.П.* Стратегическое управление. – М.: Омега-Л, 2008- 464 с.;
7. *Мурзина Н.А., Федоров А.Н., Серов А.А.* Анализ среды функционирования организации с помощью метода SWOT– анализа//Актуальные вопросы экономики региона: анализ, диагностика и прогнозирование. 2016. С. 85-89;
8. *Лившиц И. И., Полещук А. В.* Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации - ИСО 27001 и СТО Газпром // Труды СПИИРАН. 2010. №3 (40). С. 33-44;
9. *Иванова Н.В., Коробулина О.Ю.* Метод аудита информационной безопасности информационных систем // Известия Петербургского университета путей сообщения. – 2017. С. 60 – 66.
10. *Семченко А. А., Засыпкина Е. А.* К вопросу о применении FMEA анализа в промышленности// Материалы IV научного конгресса студентов и аспирантов СПБГЭУ. 2018. №1 С. 1-29;
11. *Петровская Ю.А., Петровская Е.А.* Комплексная оценка рисков методом FMEA//Актуальные проблемы авиации и космонавтики. 2016. №12. С. 194-196;
12. *Розенталь Р.* Методика FMEA - путь повышения качества продукции// электроника: наука, технология, бизнес. 2010. №7 (105). С. 90-95;
13. *Маевская К.Л., Макарочкин В.В., Варепо Л.Г.* FMEA-анализ как основной метод управления рисками на производственных предприятиях // Метрология, стандартизация и управление качеством.Материалы III Всероссийской научно-технической конференции. 2018. С. 84-86;
14. *Приёмак Е.В., Николаева Н.Г.* Применение метода FMEA при анализе экологических рисков фармацевтического предприятия //Методы менеджмента качества. 2011. №11. С. 22-30;
15. *Фомин А.А.* Исследование и оптимизация алгоритмов аудита информационной безопасности организации// Вопросы защиты информации. 2009. №3 (86). С. 57-63.

References

1. Makarenko S.I. Audit informacionnoj bezopasnosti: osnovnye etapy, konceptual'nye osnovy, klassifikaciya meropriyatij // *Sistemy upravleniya, svyazi i bezopasnosti*. 2018. №1 S. 1-29;
2. Hlestova D.R., Bajrushin F.T. Audit informacionnoj bezopasnosti v organizacii // *Simvol nauki.* 2016. № 11-3 (23). S. 175-177;
3. Kravchuk D. I., Korkushko D.A. Audit bezopasnosti korporativnyh informacionnyh sistem // *Molodoj uchenyj.* 2015. №10. 755 s.
4. Filyak P.YU., SHvarev V.M. Obespechenie informacionnoj bezopasnosti organizacii na osnove sistemy menedzhmenta informacionnoj bezopasnosti// *Informaciya i bezopasnost'.* 2015. №4. S. 5803-583;

5. Prosyannikov R.E. Izbavit'sya ot zabluzhdenij. Vidy audita informacionnoj bezopasnosti // *Connect! Mir svyazi.* 2004. № 12.S. 148–151;
6. Gaponenko A.L., Pankruhin A.P. Strategicheskoe upravlenie. – M.: Omega-L, 2008- 464 s.;
7. Murzina N.A., Fedorov A.N., Serov A.A. Analiz sredy funkcionirovaniya organizacii s pomoshch'yu metoda SWOT– analiza//*Aktual'nye voprosy ekonomiki regiona: analiz, diagnostika i prognozirovanie.* 2016. S. 85-89;
8. Livshic I. I., Poleshchuk A. V. Prakticheskaya ocenka rezul'tativnosti SMIB v sootvetstvii s trebovaniyami razlichnyh sistem standartizacii - ISO 27001 i STO Gazprom // *Trudy SPIIRAN.* 2010. №3 (40). S. 33-44;
9. Ivanova N.V., Korobulina O.YU. Metod audita informacionnoj bezopasnosti informacionnyh sistem // Izvestiya Peterburgskogo universiteta putej soobshcheniya. – 2017. S. 60 – 66.
10. Semchenko A. A., Zasypkina E. A. K voprosu o primenenii FMEA analiza v promyshlennosti // *Materialy IV nauchnogo kongressa studentov i aspirantov SPBGEU.* 2018. №1 S. 1-29;
11. Petrovskaya YU.A., Petrovskaya E.A. Kompleksnaya ocenka riskov metodom FMEA // *Aktual'nye problemy aviacii i kosmonavtiki.* 2016. №12. S. 194-196;
12. Rozental' R. Metodika FMEA - put' povysheniya kachestva produkcii// *Elektronika: nauka, tekhnologiya, biznes*. 2010. №7 (105). S. 90-95;
13. Maevskaya K.L., Makarochkin V.V., Varepo L.G. FMEA-analiz kak osnovnoj metod upravleniya riskami na proizvodstvennyh predpriyatiyah // *Metrologiya, standartizaciya i upravlenie kachestvom.Materialy III Vserossijskoj nauchno-tekhnicheskoj konferencii.* 2018. S. 84-86;
14. Priyomak E.V., Nikolaeva N.G. Primenenie metoda FMEA pri analize ekologicheskih riskov farmacevticheskogo predpriyatiya //*Metody menedzhmenta kachestva.* 2011. №11. S. 22-30;
15. Fomin A.A. Issledovanie i optimizaciya algoritmov audita informacionnoj bezopasnosti organizacii// *Voprosy zashchity informacii.* 2009. №3 (86). S. 57-63.

Статья поступила в редакцию 29.06.2019 г.