https://www.modscires.pro/index.php/msr/article/view/msr06-01-010
DOI: 10.30889/2523-4692.2018-06-01-010

УДК 004.2

INFORMATION RISK MANAGEMENT AND PREVENTION OF IT THREATS

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ И ПРЕДОТВРАЩЕНИЕ IT УГРОЗ

Nikonov V.V. / Никонов В.В.
c.t.s., as.prof. / к.т.н., доц.
SPIN: 9981-5659
Gnetova A.I. / Гнетова А.И.
master / магистр.
Federal State Budget Educational Institution of Higher Education ««MIREA – Russian Technological University», Vernadskogo Ave., 78, Moscow, Russia
Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», Москва, Проспект Вернадского, д. 78.

Аннотация. *В работе рассмотрены основные информационные риски, основные этапы проверки ИТ-инфраструктуры и международные стандарты по проверке и защите информационных технологий; представлены модели и схемы алгоритмов, основанные на использовании основного контроля информационных технологий, организационных мероприятиях, разработанной документарной политики для минимизации информационных рисков и снижению компенсаций за ущерб от их наступления; дана классификация в зависимости от типа угроз, от механизма воздействия, которая выявляет риски.*

Ключевые слова: *информационные технологии, управление рисками, IT инфраструктура, диаграммы Венна, круги Эйлера, стандарты безопасности, состояния ИТ.*

На сегодняшний день руководство любых предприятий опасается за конфиденциальность своих данных. Наличие определенной системы защиты информации – это залог успешного развития и существования конкурентоспособной компании.

Чтобы получить данные о текущем состоянии защищенности информации специалисты различных уровней проверяют такую информацию на физическую доступность, конфиденциальность, полноту, а также достоверность. На сегодняшний день не существует специализированной литературы, которая описывает, как именно должны выполняться методики по управлению информационной безопасностью. Отсутствуют определенные алгоритмы, инструменты, предоставляющие возможность оперативно определять проблемные места в системе безопасности. Их наличие на любом предприятии позволило бы достичь определенных результатов по управлению информационными рисками.

Для того, чтобы управлять информационной безопасностью, необходимо знать основные стандарты безопасности, которые используются аудиторскими компаниями при проверке. Информация должна быть защищена по нескольким критериям. Проверку нужно проводить в несколько этапов. На рисунке 1 представлены основные этапы проверки ИТ-инфраструктуры.

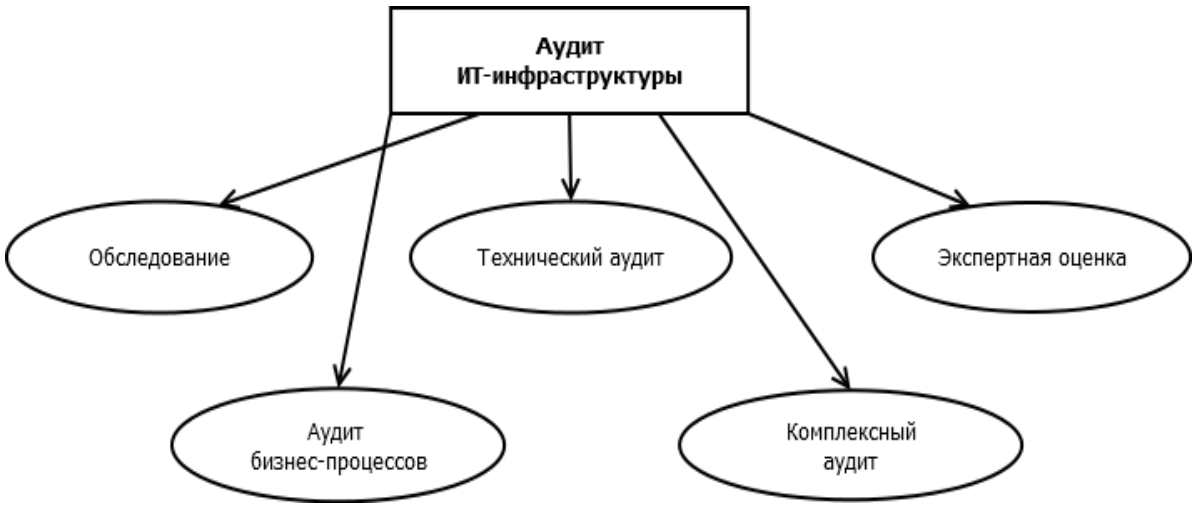

Рис. 1. Основные этапы проверки ИТ-инфраструктуры

За основу предлагается взять следующие стандарты и библиотеки:

– Audit Framework 3rd Edition (ITAF);
– Control Objectives for Information and Related Technologies (CobiT);
– International Professional Practice Framework (IPPF);
– Sarbanes-Oxley Act (SOX);
– Infrastructure Library (ITIL).

Отношения между компонентов можно представить с помощью кругов Эйлера (диаграммы Венна), которые представлены на рисунке 2.

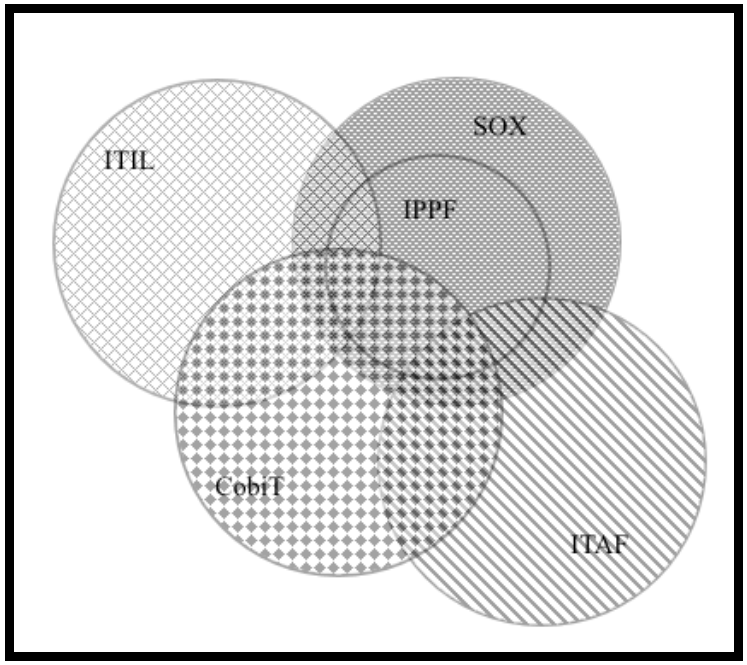

Рис. 2. Модель взаимосвязи компонентов

Из рисунка 2 видно, что все стандарты и методологии информационной безопасности имеют общие компоненты, следовательно совместное их использование поможет наилучшим образом разработать систему управления информационными рисками и предотвращения ИТ угроз.

Систему по управлению информационными рисками и предотвращению ИТ угроз представим в виде схемы связей и отношений на рисунке 3.

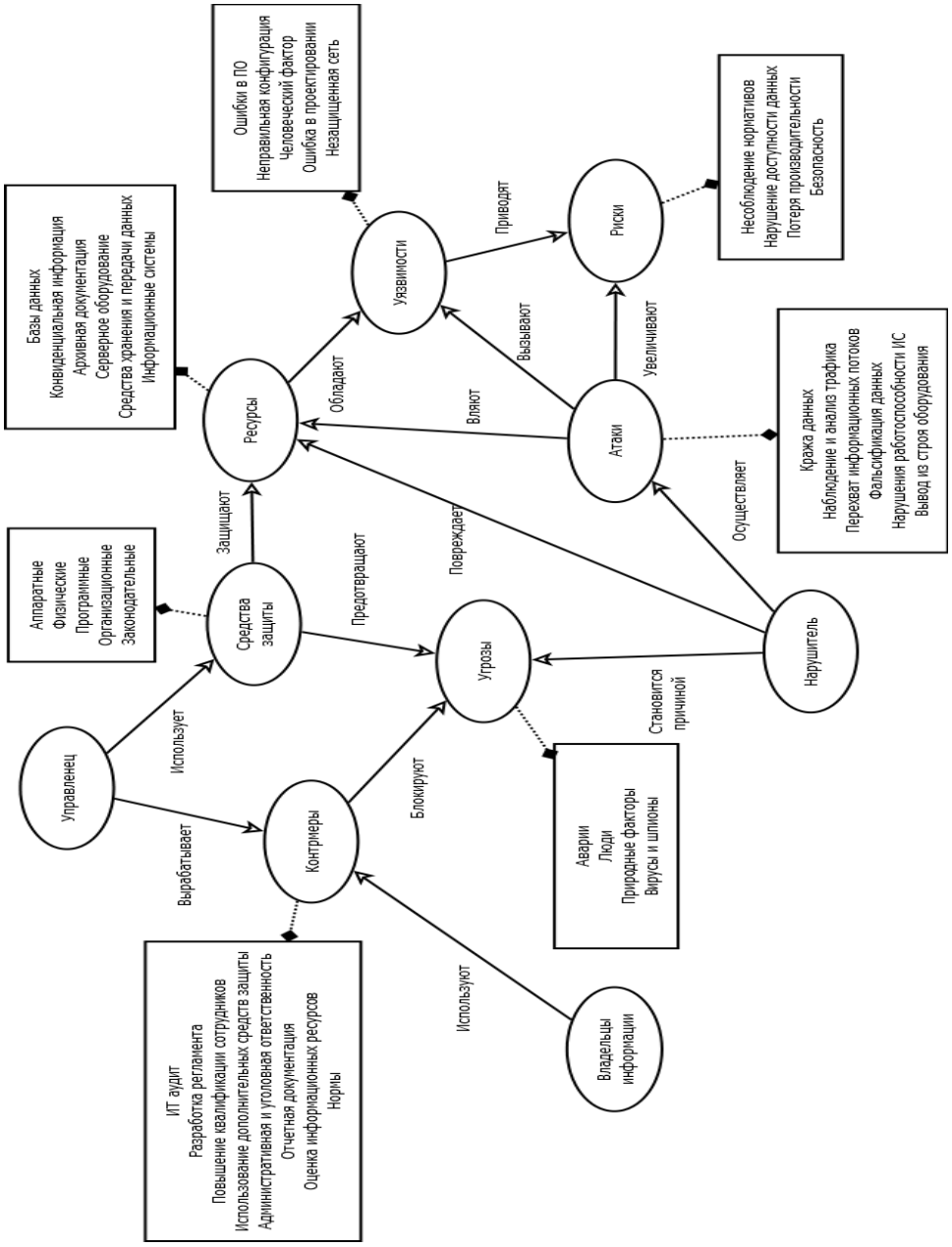

Рис. 3. Схема связей и отношений в системе управления информационными рисками и предотвращения ИТ угроз

Основываясь на выше представленных данных, введем общий алгоритм методики (рисунок 4). Он включает основные этапы работ, которые направлены на выявление уязвимостей. Сама методика может быть описана в текстовой форме, используя контрольные точки. Каждой точке необходимо обозначить основные параметры:

- название контрольной точки;
- описание (текущее состояние);
- норма контрольной точки;
- нарушения или отклонения, имеющиеся у контрольной точки;

– предложения по улучшению состояния контрольной точки.

Нормы контрольных точек, предложения по улучшения состояния складываются из международных стандартов и правил, а также лучших средств защиты, описанных ранее.

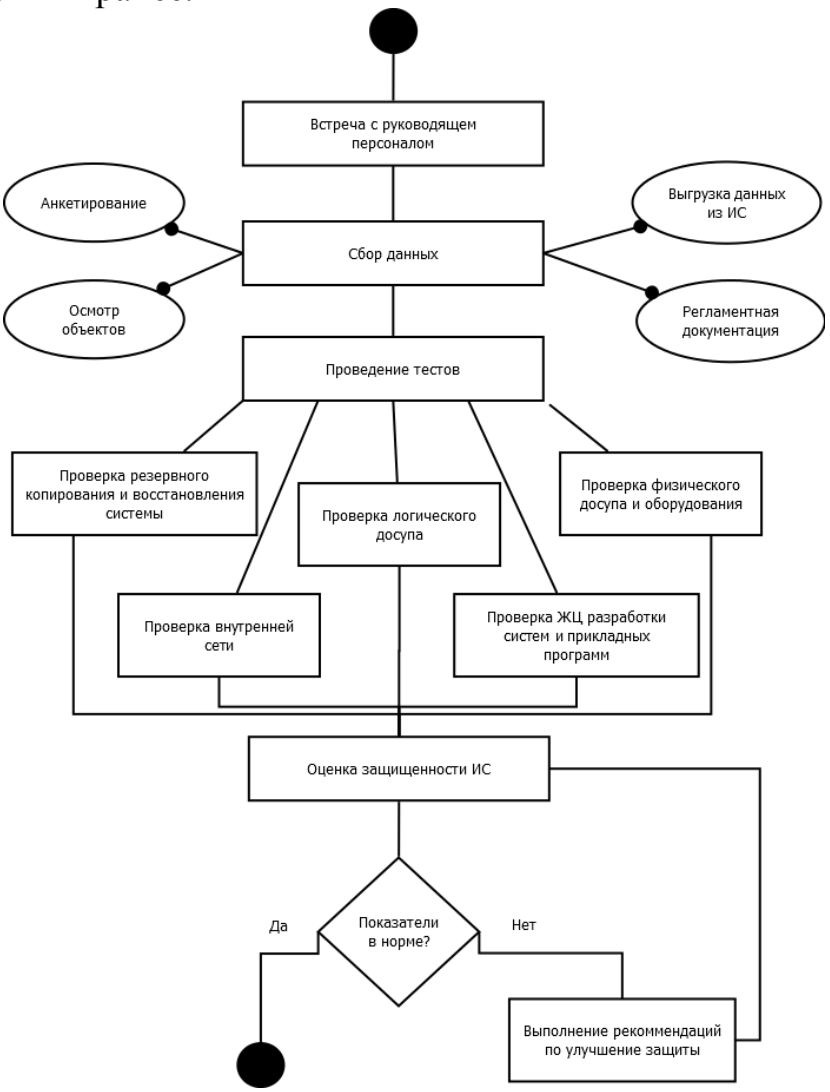

Рис. 4. Модель системы управления

Полученная модель связывает между собой показатели со всех средств защиты.

Используя формулу расчета (формулы 1 и 2) общего состояния ИТ компонент организации установим общую эффективность контрольных точек, которая наблюдается на данный момент.

$$ITstatus = \frac{\sum_{i=1}^{n} R_i}{\sum_{i=1}^{n} Rpoint_i}, \quad (1)$$

$$R = Rpoint_i \times Reffect_i, \quad (2)$$

где $ITstatus$ – общее состояние ИТ компонент организации,

$Rpoint_i$ – оценка важности контрольной точки,

$Reffect_i$ – оценка текущего состояния контрольной точки.

Введем классификацию общего состояния ИТ компонент:

– $ITstatus < 0{,}4$ – высокая подверженность ИТ рискам и угрозам;

– $0{,}4 \leq ITstatus \leq 0{,}75$ – существует вероятность ИТ рисков и угроз;

– $ITstatus > 0{,}75$ – низкая вероятность возникновения ИТ рисков и угроз.

При показателе $ITstatus < 0{,}4$ руководству предприятия необходимо пересмотреть политику видения бизнеса в сфере ИТ и использовать разработанную систему управления информационными рисками и предотвращения ИТ угроз как внутреннюю политику по организации и защите ИТ.

После ряда мероприятий необходимо произвести повторную оценку, чтобы установить насколько совершенные действия были эффективны.

Если же у руководства организации не хватит самостоятельных сил для решения сложившейся ситуации, рекомендуется пригласить квалифицированных специалистов, чтобы они помогли установить высокий уровень защищенность ИТ объектов организации с помощью разработанной системы управления информационными рисками и предотвращения ИТ угроз в качестве универсальной модели, как должна соблюдаться политика информационной безопасности.

Литература:

1. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – М.: Издательство Юрайт, 2017. – 309 с.

2. Черняк, В.З., Эриашвили Н.Д., Барикаев Е.Н. Управление предпринимательскими рисками в системе экономической безопасности. Теоретический аспект: монография. – М.: ЮНИТИ-ДАНА, 2015. – 159 с.

3. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. – М.: Издательский дом Высшей школы экономики, 2015. – 574 с.

4. BS ISO\IEC 27001:2005. BS 7799-2:2005. Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасность – Требования.

5. ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems (Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности).

6. Морозова Т.Ю., Никонов В.В., Сумкин К.С. Методы управления доступом к информационным ресурсам асу на основе канонических мо-делей // Приборы и системы. Управление, контроль, диагностика. 2008. № 10. С. 12-14.

7. Сумкин К.С., Никонов В.В., Иванова И.А. Использование беспроводных систем при мониторинге объектов, находящихся под воздействием сетевых угроз // Естественные и технические науки. 2014. № 3 (71). С. 155-157.

8. Nikonov V.V., Los' V.P., Ross G.V. Development of automated system for identifying abnormal network activity and detecting threats // Automatic Control and Computer Sciences. 2016. Т. 50. № 8. С. 693-702.

References:

1. Shcheglov, A. Yu. Zashchita informatsii: osnovy teorii: uchebnik dlya bakalavriata i magistratury [Information security: basic theory: a textbook for undergraduate and graduate programs] / A. Yu. Shcheglov, K. A. Shcheglov. – M.: Izdatelstvo Yurayt [Moscow: Publishing house «Jurait»], 2017. – 309 s.

2. Chernyak, V.Z., Eriashvili N.D., Barikaev Ye.N. Upravlenie predprini-matelskimi riskami v sisteme ekonomicheskoy bezopasnosti. Teoreticheskiy aspekt: monografiya [Management of business risks in the system of economic security. Theoretical aspect: monograph]. – M.: YuNITI-DANA, [Moscow: Publishing house « YuNITI-DANA »] 2015. – 159 s.

3. Serdyuk, V. A. Organizatsiya i tekhnologii zashchity informatsii: obna-ruzhenie i predotvrashchenie informatsionnykh atak v avtomatizirovannykh sistemakh predpriyatiy: uchebnoe posobie [Organization and technology of information protection: detection and prevention of information attacks in automated systems of enterprises: a tutorial]. – M.: Izdatelskiy dom Vysshey shkoly ekonomiki [Moscow: Publishing house « Higher School of Economics »], 2015. – 574 s.

4. BS ISO\IEC 27001:2005. BS 7799-2:2005. Informatsionnye tekh-nologii – Metody obespecheniya bezopasnosti – Sistemy upravleniya informatsionnoy bezopasnost – Trebovaniya [BS ISO \ IEC 27001: 2005. BS 7799-2: 2005. Information technology - Security methods - Information security management systems - Requirements.].

5. ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems (Trebovaniya dlya organov, obespechivayushchikh audit i sertifikatsiyu sistem menedzhmenta informatsionnoy bezopasnosti) [ISO / IEC 27006: 2007, Requirements for bodies providing audit and certification of information security management systems].

6. Morozova T.Yu., Nikonov V.V., Sumkin K.S. Metody upravleniya do-stupom k informatsionnym resursam asu na osnove kanonicheskikh mo-deley [Methods to control access to information resources of the ACS based on canonical models] // Pribory i sistemy. Upravlenie, kontrol, diagnostika [Instruments and systems. Management, control, diagnostics]. 2008. № 10. S. 12-14.

7. Sumkin K.S., Nikonov V.V., Ivanova I.A. Ispolzovanie besprovodnykh sistem pri monitoringe obektov, nakhodyashchikhsya pod vozdeystviem setevykh ugroz [The use of wireless systems in the monitoring of objects under the influence of network threats]// Yestestvennye i tekhnicheskie nauki [Natural and Technical Sciences]. 2014. № 3 (71). S. 155-157.

8. Nikonov V.V., Los' V.P., Ross G.V. Development of automated system for identifying abnormal network activity and detecting threats // Automatic Control and Computer Sciences. 2016. Т. 50. № 8. С. 693-702.

Abstract. *The paper discusses the main information risks, the main stages of testing IT infrastructure and international standards for the verification and protection of information technology; models and schemes of algorithms based on the use of basic control of information technologies, organizational measures, developed documentary policies to minimize information risks and reduce compensation for damage from their occurrence; a classification is given depending on the type of threats, on the mechanism of influence, which reveals risks.*

Key words: *information technologies, risk management, IT infrastructure, Venn diagrams, Euler circles, security standards, IT states.*

Статья отправлена: 29.11.2018 г.