6. Azzedine Boukerche Algorithms and protocols for wireless and mobile ad hoc networks // University of Ottawa, Canada, 2009, p. 9.

7. Кулаков М. С. Анализ сценариев развертки мобильных Ad Hoc сетей на базе режима VDL Mode 4 // INTERMATIC – 2013. / Материалы международной научно-практической конференции. Часть 4. М.: МИРЭА, 2013. С. 49–53.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С УЧЕТОМ УПРАВЛЕНИЯ РИСКАМИ

Н.Л. Пиховкин, Д.В. Сахаров

Информационно-вычислительные сети, объединяющие в единую систему все подразделения и филиалы, позволяют одновременно работать с распределенными или централизованными приложениями, базами данных и другими сервисами. Одной из главных задач обеспечения необходимого уровня защищенности таких сетей является процесс управления рисками, который позволяет направить все усилия на защиту от наиболее вероятных угроз. В статье анализируется важность управления рисками в процессе обеспечения информационной безопасности, а также описывается риск-ориентированная методика построения защищенной распределенной сети, разработанная на основе ведущих мировых стандартов и рекомендаций.

Ключевые слова: информационная безопасность, управление рисками, угроза, информационная система, распределенная сеть.

SECURING A DISTRIBUTED INFORMATION NETWORK, TAKING INTO ACCOUNT RISK MANAGEMENT

Pihovkin N., Sakharov D.

Information and computer networks, combining into a single system all departments and branches, can work together in centralized or distributed applications, databases and other services. One of the main tasks of ensuring the necessary level of security of such networks is the risk management process, which allows to make every effort to protect against the most likely threats. The article analyzes the importance of risk management in the process of information security, anddescribes the risk-oriented method of construction of a secure distributed network developed based on leading standards and recommendations.

Keywords: information security, risk management, threat information system, a distributed network.

Построение защищенной территориально распределенной сети – это сложная комплексная задача. При ее решении приходится учитывать множество факторов и рисков, которые могут оказать негативное влияние на деятельность компании, а также поставить под угрозу конфиденциальность, целостность, доступность информации, качество и скорость ее обработки и передачи. Ограниченные ресурсы и постоянно меняющейся ландшафт угроз и уязвимостей делают невозможным полное снижение всех рисков. Специалисты по безопас-

ности должны иметь набор средств, который поможет оценить воздействие рисков на деятельность организации и, если необходимо, снизить их до приемлемого уровня. Для формирования понимания приоритетности мероприятий, направленных на повышение уровня ИБ, разрабатывается механизм управления рисками. В этом случае все усилия направляются на защиту от наиболее вероятных угроз, позволяя снизить возможные потери и минимизировать затраты. Это делается потому, что бессистемное и выборочное внедрение защитных мер не может обеспечить необходимого уровня защищенности. Кроме того, необходимость проведения управления рисками определена в российских и международных стандартах по информационной безопасности (ГОСТ Р ИСО/МЭК 17799:2005, CRAMM, ISO 27001:2013) и нормативных документах государственных органов РФ (например, документах ФСТЭК России по защите персональных данных и ключевых систем информационной инфраструктуры).

Специалист, отвечающий за построение безопасной информационно-вычислительной сети, должен найти баланс как минимум в трех показателях – производительности, безопасности и стоимости. При снижении рисков и повышении уровня безопасности сети, как правило, увеличивается стоимость и снижается производительность. Также конфликтующими свойствами являются надежность и защищенность, с одной стороны, удобство и открытость – с другой. Отсюда следует, что построение безопасной сетевой инфраструктуры – это управление рисками, возникающими вследствие определенных компромиссов.

Рис. 1. Процесс управления рисками

Процесс управления рисками информационной безопасности, подробно описанный на рисунке 1, сводится к получению следующих данных [1, 3]:

1) какие риски существуют в организации;
2) какова вероятность их реализации и масштаб возможных последствий;
3) какие риски руководство организации готово принять;
4) какие средства защиты являются наиболее эффективными (в том числе с экономической точки зрения) для борьбы с той или иной уязвимостью;
5) какой объем средств должен находиться в резерве в случае возникновения инцидента ИБ.

В случае информационно-вычислительных сетей риск-ориентированная методика обеспечения безопасности будет состоять из следующих последовательных шагов:

1) сбор информации о сетевой инфраструктуре;
2) классификация и определение ценности сетевых активов;
3) идентификация и классификация актуальных угроз;
4) анализ существующих защитных мер;
5) анализ рисков сетевой безопасности;
6) проектирование и внедрение системы обеспечения безопасности;
7) документирование результатов;
8) мониторинг эффективности.

На первых этапах проводится анализ документации, интервьюирование работников, отвечающих за функционирование и безопасность сетевой инфраструктуры. Специалисты проводят опрос персонала каждого подразделения с целью выявления используемых активов. Не все активы имеют одинаковую ценность для организации, поэтому после идентификации всех ценных активов они должны быть классифицированы в соответствии с уровнем потенциального ущерба в случае возникновения инцидента. Классификация позволит определить, какие защитные меры и в каком приоритете должны применяться к каждому классу, а также сделать это наиболее экономически эффективным способом.

Далее проводится проверка объектов на наличие уязвимостей и, при необходимости, проведение тестирования на проникновение с использованием выявленных уязвимостей. Как правило, при проведении инструментального сканирования используется программное обеспечение, позволяющее автоматизировать процесс, однако могут быть задействованы и ручные проверки. По завершении всех работ составляется отчетная документация, в которую входит информация об обнаруженных уязвимостях, а также рекомендации по их устранению.

После всестороннего изучения сетевой инфраструктуры проводится анализ рисков, связанных с нарушением безопасности сетевых активов. В настоящее время существует множество инструментов и программных инструментов, позволяющих автоматизировать этот процесс – ГРИФ, RiskWatch, Risk Advisor, FRAP, CRAMM, Microsoft Security Assessment Tool, Symantec Lifecycle Security (основные сравнительные характеристики приведены в таблице). Не-

смотря на большое разнообразие, все они так или иначе основаны на двух фундаментальных к оценке рисков – на количественном или на качественном [2].

ТАБЛИЦА 1. Основные сравнительные характеристики инструментов анализа рисков

	ГРИФ	**RiskWatch**	**Risk Advisor**	**FRAP**	**CRAMM**	**MSAT**	**Symantec LS**
Способы измерения величины риска							
Качественный метод	+	+	+	+	+	+	+
Количественный метод	+	+	–	–	+	+	–
Подход к анализу и оценке риска							
Модель анализа угроз и уязвимостей	+	+	–	+	+	–	+
Метод информационных потоков	+	+	+	–	+	+	+
Элементы риска							
Материальные активы	+	+	+	+	+	+	+
Нематериальные активы	+	+	+	+	+	+	+
Ценность активов	+	+	+	+	+	+	+
Угрозы	+	+	+	+	+	+	+
Уязвимости	+	+	+	+	+	+	+
Средства защиты	+	+	+	+	+	+	-
Потенциальный ущерб	+	+	+	+	+	+	+
Вероятность реализации угрозы	+	+	+	+	+	+	+
Финансовые показатели							
Расчет возврата инвестиций (ROI)	+	+	–	–	–	–	–
Расчет ожидаемых годовых потерь (ALE)	–	+	–	–	–	–	–

Для определения очередности обработки рисков выполняется операция их ранжирования. Один из самых простых способов – это ранжирование по вероятности реализации угрозы и по степени критичности информации, исходя из которого составляется многоуровневая шкала или матрица рисков, показывающая степень воздействия выявленных угроз на сетевую инфраструктуру. Пример матрицы рисков приведен на рисунке 2.

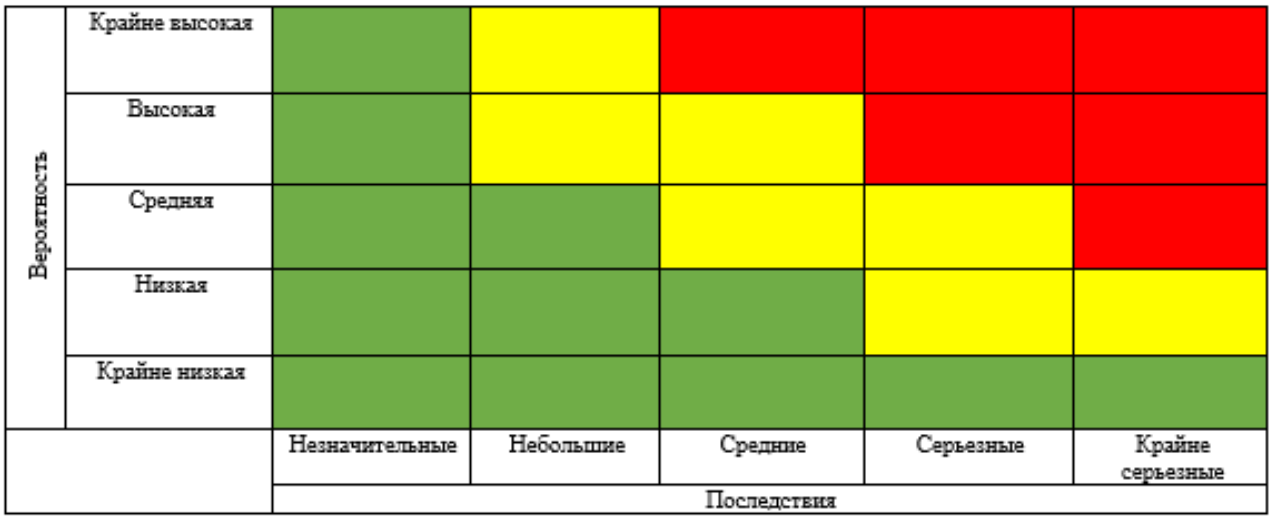

Рис. 2. Процесс управления рисками

На основе данных, полученных на предыдущих этапах, проектируется подходящий дизайн сетевой инфраструктуры и разрабатываются политики информационной безопасности. Написание и строгое соблюдение политик определяет работу всей системы защиты. После этого начинается непосредственное внедрение средств защиты.

Еще одной важной составляющей обеспечения безопасности и непрерывной работы сетевых сервисов является осуществление мониторинга сети, который позволяет своевременно реагировать на возникающие угрозы и значительно упрощает работу сетевых администраторов.

Таким образом, можно сказать, что применение риск-ориентированного подхода позволяет выбрать состав системы защиты сети, который полностью отвечает заданным условиям и требованиям. Это максимально повышает эффективность внедренных мер защиты, а также позволяет снизить затраты на обеспечение и поддерживание необходимого уровня информационной безопасности. Управление рисками в сфере информационной безопасности информационно-вычислительных сетей играет такую же важную роль, как и во всех других областях человеческой деятельности.

Список используемых источников

1. Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н. Организационно-правовое и методическое обеспечение информационной безопасности. СПб.: Университет ИТМО, 2016. 168 с.

2. Steven Hernandez. Official (ISC)^2 Guide to the CISSP CBK, Third Edition. ISC2 Press, 2012. 968 с.

3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М.: Издательство стандартов, 2010. 51 с.