INFORMATION PROTECTION

Shmatko A.V., Fedorchenko V.N., Ivashchenko O.V.

SELECTING THE OPTIMAL INFORMATION PROTECTION SYSTEM FROM DATA LEAKAGE

Shmatko Alexander Vitalievich, Ukraine, National Technical University "Kharkov Polytechic Institute", ass.prof.
Fedorchenko Vladimir Nikolaevich, Ukraine, Simon Kuznets Kharkiv National University of Economics, ass.prof.
Ivashchenko Oksana Vitalievna, Ukraine, National Technical University "Kharkov Polytechic Institute", postgraduate

Abstract
In this article, we consider the problem of organizing the process of selecting the optimal system for protecting information from data leakage. The existing methods of assessing the information risks of an enterprise are analyzed. Information security systems from data leakage represent a complex technical system and have a number of features that complicate the selection process. A promising direction in the development of decision-making methods with expert source information is a linguistic approach based on the theory of fuzzy sets and a linguistic variable.
Keywords: information system, information security system, security audit, risk of information leakage, expert evaluation.

Введение. Информацию без преувеличения можно отнести к одному из важных ресурсов развития. В современном мире она активно влияет на все сферы жизнедеятельности, в том числе в современной экономике.

Каждое предприятие функционирует в условиях рыночной экономики, определяя собственную стратегию развития. У предприятия

есть клиенты, поставщики сырья или услуг, конкуренты. В этих условиях возникает угроза утечки важной для нормальной беспрерывной работы предприятия информации. Такие утечки данных могут привести к потере клиентов, авторитета, снижению конкурентоспособности.

Современная информационная система (ИС) предприятия представляет собой сложную, распределенную систему, которая состоит из множества подсистем, которые имеют собственные программно-технические средства реализации информационных технологий и множество средств для обеспечения взаимодействия этих подсистем с целью предоставления удаленным пользователям набора услуг из сферы информационного обслуживания.

Наличие средств защиты информации является важным фактором любой информационной системы. Эффективность защиты информации в информационных системах достигается с помощью использования систем защиты информации (СЗИ).

Эффективность СЗИ характеризуется эффективностью ее использования в качестве активного средства обеспечения конфиденциальности обработки, хранения и передачи информации предприятия.

В рамках конкретного предприятия, возникает задача внедрения ряда требований по эффективности СЗИ. К ним относят требования к методам защиты, которые должны учитывать особенности организации информационной системы предприятия, количество затраченных ресурсов предприятия на внедрение и сопровождение СЗИ, скрытность способов реализации защиты. Возникает необходимость создания оптимальной СЗИ для предприятия в результате разработки теории, которая связывает ее структуру, логическую организацию, методы и средства деятельности с целью формирования функции выбора множества лучших стратегий защиты информации.

Таким образом, для эффективного функционирования предприятия, нужно постоянно отслеживать появление потенциальных угроз утечки данных и проверять уровень защиты информационной системы предприятия. Определить наибольшие риски появления события утечки данных и оценить уровень надежности системы защиты информации, которая функционирует на предприятии, от утечек данных возможно с помощью проведения аудита информационной безопасности.

Методы исследования. Аудит безопасности информационной системы предприятия представляет собой системный процесс получения объективных качественных и количественных оценок о текущем

состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности.

Целью проведения аудита безопасности являются [1]:

- анализ рисков, связанных с возможностью осуществления угроз безопасности по ресурсам ИС;
- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- внедрение новых или повышение эффективности существующих механизмов безопасности ИС.

Цель оценки рисков заключается в определении характеристик рисков корпоративной информационной системы и ее ресурсов. После оценки рисков можно выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании.

Среди различных методов оценки информационных рисков предприятия, выделяют пять основных:

- табличный метод оценки рисков;
- методика анализа рисков Microsoft;
- модель многоуровневой защиты;
- модель многозвенной защиты;
- LifecycleSecurity.

Табличный метод оценки рисков разделяется на множество табличных методов оценки информационных рисков компании. Важно выбрать для себя подходящий метод, обеспечивающий корректные и достоверные результаты. Существенно, что во всех методах количественные показатели существующих или предлагаемых физических ресурсов предприятия оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса, то есть количественными методами. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть с помощью определения затрат на их приобретение или восстановление количественными методами [2].

Процесс управления рисками безопасности, предложенный Microsoft, включает следующие четыре этапа:

- оценка рисков;
- поддержка принятия решений;
- реализация контроля;
- оценка эффективности программы.

В руководстве этой методологии особо отмечается, что термины управление рисками и оценка рисков не являются взаимозаменяемыми. Под управлением рисками понимаются общие меры по снижению риска в рамках организации до приемлемого уровня. Управление рисками представляет собой непрерывный процесс, но произведенные оценки чаще всего делаются для годового интервала. Под оценкой рисков понимается процесс выявления рисков для бизнеса, который является составной частью управления рисками.

С точки зрения информационной безопасности, модель многоуровневой защиты определяет набор уровней защиты информационной системы. Модель часто используется корпорацией Microsoft в пособиях по безопасности. Корректная организация защиты на каждом из выделенных уровней, позволяет уберечь систему от реализации угроз информационной безопасности [3].

На практике в ряде случаев защитный контур любого уровня может состоять из нескольких «соединенных» между собой преград с разной прочностью. Такая модель защиты называется многозвенной моделью защиты. Информация, которая хранится и обрабатывается в ИС, и контур защиты должны включать еще и другие звенья, которые обеспечивают контроль доступа к аппаратуре, защиту от подслушивания, дистанционное видеонаблюдение, перехват побочного электромагнитного излучения и др. Каждое из звеньев должно обеспечивать замкнутое препятствие для соответствующего канала несанкционированного доступа к данному предмету защиты. В этом случае между звеньями не образуются так называемые «щели», позволяющие осуществлять "обход" соответствующих препятствий [4].

LifecycleSecurity- это обобщенная схема построения комплексной защиты компьютерной сети предприятия. Выполнение описываемого в ней набора процедур позволяет системно решать задачи, связанные с защитой информации, и дает возможность оценить эффект от затраченных средств и ресурсов. С этой точки зрения, идеология LifecycleSecurity может быть противопоставлена тактике "точечных решений", заключающейся в том, что все усилия сосредоточиваются на внедрении отдельных частных решений - например, межсетевых экранов или систем аутентификации пользователей по старт-картах. Без предварительного анализа и планирования, подобная тактика может привести к появлению в компьютерной системе набора разрозненных продуктов, которые не стыкуются друг с другом и не позволяют решить проблемы предприятия в сфере информационной безопасности [3].

Системы защиты информации от утечки данных представляют сложную техническую систему. Решение задач анализа и синтеза СЗИ от утечек данных осложняется рядом их особенностей, основными из которых являются [1]:

– – сложная взаимосвязь показателей качества DLP-систем с показателями качества информационной системы;

– – необходимость учета большого количества показателей (требований) DLP-систем при оценке и выборе их рационального варианта;

– – преимущественно качественный характер показателей, учитываемых при анализе и синтезе СЗИ;

– – существенная взаимосвязь и взаимозависимость этих показателей имеют противоречивый характер;

– – сложность получения исходных данных, необходимых для решения заданий анализа и синтеза DLP-систем, особенно на ранних этапах их проектирования.

Перечисленные особенности делают практически невозможным применение традиционных математических методов.

Результаты и обсуждение. Сложность процесса принятия решений приводит к тому, что при оценке и выборе альтернатив необходимо использовать и обрабатывать качественную экспертную информацию. Перспективным направлением разработки методов принятия решений при экспертной исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистической переменной.

Нами предлагается методология исследования уровня безопасности ИС предприятия и выбора оптимальной системы защиты данных от утечек, которая состоит из следующих этапов:

– проведение аудита ИС;

– определение рисков утечки данных;

– определение критериев и альтернатив выбора оптимальной DLP-системы.

Сначала проводится аудит системы с целью определения уровня защиты ИС предприятия.

Проводится определение априорной вероятности принадлежности ИС к каждому из заданных уровней надежности ИС и априорной вероятности надежности ИС по типовым признакам - реакции системы на известные уязвимости. Эти вероятности определяются с помощью общей статистики уровня безопасности подобных предприятий. Для получения апостериорной вероятности принадлежности ИС к каждой из заданных

групп, необходимо собрать фактические значения реализации определенных уязвимостей. Для этого проводится тест на проникновение**.**

Следующим этапом системный аналитик вместе с руководителем предприятия, формируют множество возможных рисков утечки данных на предприятии. После этого, эксперты оценивают важность каждого риска и в результате риски ранжируются и избираются самые важные.

Важнейшие риски переходят в критерии выбора оптимальной DLP-системы, также, аналитик формирует дополнительно необходимые критерии, опираясь на общую статистику требований к DLP-систем на предприятиях, занимающихся аналогичной деятельностью. Выполнив экспертную оценку критериев, определяется множество альтернативных DLP-систем, которые соответствуют заданным требованиям.

Экспертная оценка представляет лингвистические значения, в соответствие которым проставляются числа на шкале [0, 1], используя теорию нечетких множеств. В результате, оценки рисков, критериев и альтернатив определяются в виде нечетких чисел, которые нечетко характеризуют лингвистические оценки. Используя теорию нечетких множеств, нечеткое число разлагается на нечеткое множество.

Используя методы построения функций принадлежности, полученное нечеткое множество отображается в виде треугольной функции принадлежности. Таким образом, на выходе аналитик получает нечеткие оценки рисков, критериев и альтернативных DLP-систем.

Далее производится расчет оптимальной DLP-системы.

Используя полученные на выходе нечеткие оценки критериев и альтернатив, проводится определение взвешенной оценки альтернатив с помощью бинарных операций над нечеткими числами. Полученные взвешенные оценки альтернативных вариантов DLP-систем строят в виде треугольных функций принадлежности. Используя метод выбора альтернатив при аддитивности критериев, системный аналитик проводит ранжирование полученных оценок и на основе полученных результатов определяет лучшую DLP-систему, по отношению к заданным критериям.

Для решения задачи определения уровня безопасности информационной системы предприятия и выбора оптимальной DLP - системы предлагается следующее алгоритмическое обеспечение. Общая схема (методология) решения представлена на рисунке 1.

Выводы. В данной статье была рассмотрена задача выбора оптимальной системы защиты информации от утечки данных. Особенности систем защиты информации делают сложным выбор оптимальной СЗИ. Сложность процесса принятия решений приводит к тому, что при оценке и выборе альтернатив необходимо использовать и

обрабатывать качественную экспертную информацию. В данной статье предложено при разработке методов принятия решений при экспертной исходной информации использовать лингвистический подход на базе теории нечетких множеств и лингвистической переменной.

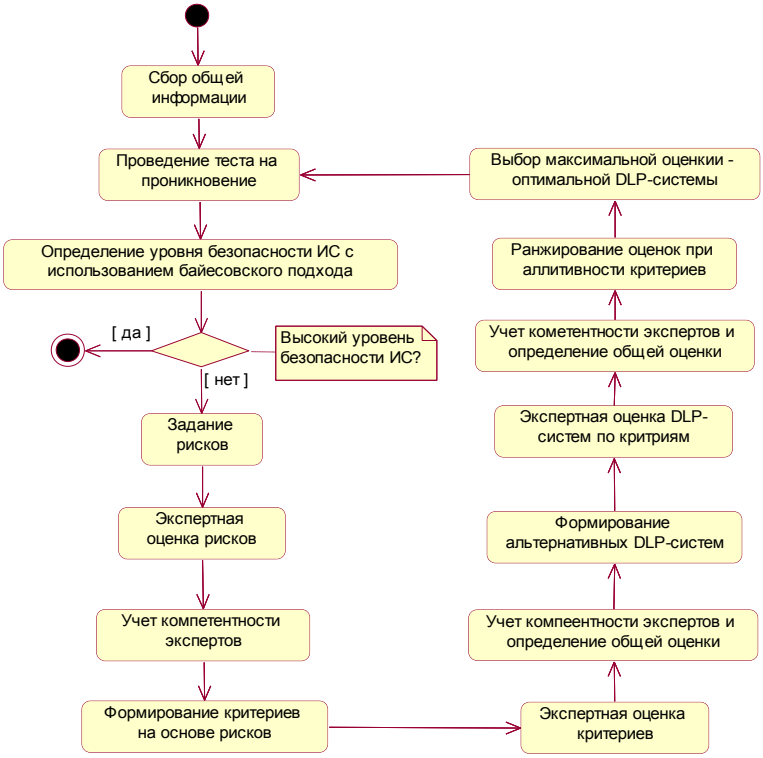

Рис. 1. Общая схема решения

References:

[1] Barmen S. Development of information security rules / S. Barmen - M .: "Vilyams", 2002. - 208 p.

[2] Petrenko S.A. Information Risk Management. Economically justified safety / S.A. Petrenko, S.V. Simonov - Moscow: DMK Press, 2004. - 392 p.

[3] Nesterov S.A. Analysis and management of risks in information systems based on Microsoft operating systems / S.A. Nesterov - "INTUIT", 2007. - 136 p.
[4] J. McDonald The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities / J. McDonald, M.Dowd, J. Schuh – Addison-Wesley Professional, 2006.– 1200 p.