Системный анализ, управление и автоматизация

УДК 681.3

МЕТОД АНАЛИЗА РИСКА ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Ф.Ф. Буканов, В.Н. Ворожейкин

Самарский государственный технический университет
443100, г. Самара, ул. Молодогвардейская, 244

E-mail: esib@samgtu.ru

Предлагается метод анализа риска при обеспечении безопасности промышленного предприятия. Указанный метод базируется на вероятностном подходе при оценке риска и использовании статистических данных по отказам элементов систем и подсистем, как технических, так и физических. Предлагаемый метод использует теорию графов, т. е. построение деревьев отказов и деревьев событий.

Ключевые слова: *метод, анализ, риск, предприятие, угроза, информация, безопасность, система, подсистема, отказ, статистика, данные, преступник, модели, граф, вероятность, эффективность, защита.*

Известные исследования анализа риска охватывают не только вопросы безопасности и надежности технических систем, но и практически все аспекты действий человека во взаимодействии с техническими системами при решении задач обеспечения безопасности сложных объектов.

Данные исследования не потеряли актуальности и в наши дни, так как сохраняется тенденция развития информационных технологий во всех сферах деятельности человека, с которой средства и системы обеспечения безопасности находятся в противоречии. Необходимо учитывать также и то, что для обеспечения безопасности предприятия используется достаточно большая номенклатура технических, программно-аппаратных средств, человеческих ресурсов, которые имеют свою степень надежности функционирования, то есть имеется вероятность отказов, которая может быть определена из статистических данных.

Все вышесказанное требует постоянной оценки эффективности и надежности средств и систем обеспечения безопасности предприятия.

Решение этой задачи может быть осуществлено с помощью методов определения уровня риска совершения для каждой из угроз безопасности предприятия.

Основополагающими работами в области теории анализа риска является работы [1-4], в них системно изложены общие вопросы анализа (идентификация, оценка, прогноз, приемлемость) рисков, а также управления (принятие решения и обоснованность мер) рисками для различных объектов.

Федор Федорович Буканов (к.т.н., доц.), заведующий кафедрой «Электронные системы и информационная безопасность».

Владимир Николаевич Ворожейкин (к.т.н.), доцент кафедры «Электронные системы и информационная безопасность».

В то же время в силу общей направленности данных работ в них вопросы разработки методов и алгоритмов анализа рисков безопасности объектов затрагивались частично.

Анализ известных методов, алгоритмов и моделей, изложенных в работах [5-8], показал, что пока не существует теоретически и практически обоснованных подходов к анализу риска потери промышленными предприятиями материальных и нематериальных активов исходя из отказов элементов и подсистем системы безопасности предприятия.

Учитывая вышесказанное, сформулируем следующую задачу анализа риска безопасности промышленного предприятия.

При заданных:

– модели предприятия, включающей описание объектов его функционирования, схем их расположения, построения и режимов работы;

– модели построения и работы систем безопасности предприятия –

провести анализ риска потери конфиденциальной информации при несанкционированном доступе для случаев отказа элементов и подсистем безопасности предприятия; определить наиболее вероятную модель преступника из числа заданных и наиболее уязвимого места в системе безопасности предприятия.

Предлагаемый в данной работе метод анализа риска для сформулированной выше задачи базируется на вероятностном подходе при оценке риска и использовании статистических данных по отказам элементов систем и подсистем, как технических, так и физических, других элементов технической инфраструктуры, которые могут привести к реализации угрозы безопасности предприятия. Предлагаемый метод базируется на теории графов, т. е. построении деревьев отказов и деревьев событий. Построение дерева отказов начинается с определенного конечного состояния системы безопасности предприятия.

Реализация предлагаемого метода анализа риска обеспечения безопасности предприятия может быть осуществлена с использованием следующего алгоритма:

– шаг 1. Составляется перечень угроз безопасности предприятия с экспертными оценками материальных потерь при реализации этих угроз.
– шаг 2. Проводится экспертная оценка критического уровня материальных потерь предприятия от реализации одиночной угрозы.
– шаг 3. Составляется база данных из угроз безопасности предприятия Ai (i=1÷n), реализация которых может превысить критический уровень материальных потерь предприятия.
– шаг 4. Из базы данных выбирается угроза Ai, которая в дальнейшем будет исследоваться методом анализа риска.
– шаг 5. Составляется модель предприятия (территория, здания, цеха и другие элементы инфраструктуры).
– шаг 6. Определяются рубежи защиты предприятия техническими системами и средствами, человеческими ресурсами от проникновения преступника на территорию, в здание, цеха, комнаты, компьютерные сети с целью реализации A_i угрозы.
– шаг 7. Составляется перечень систем и подсистем безопасности с привязкой к рубежам защиты, других технических систем инфраструктуры с привязкой к территории предприятия, а также человеческих ресурсов, отказ которых может повлиять на реализацию Ai угрозы безопасности предприятия.
– шаг 8. Составляются возможные модели преступника с указанием крайнего ру-

бежа защиты предприятия, до которого он имеет санкционированный доступ.

– шаг 9. Для каждой модели преступника начиная с рубежа защиты, от которого он не имеет санкционированного доступа на объекты предприятия, строится граф – дерево отказов систем и подсистем безопасности, инфраструктуры предприятия, человеческих ресурсов, которые могут привести к реализации A_i угрозы.

– шаг 10. Для каждой ветви дерева отказов на основе статистических данных определяется вероятность реализации угрозы A_{ik}, зависящая от вероятности отказов систем и подсистем, находящихся последовательно в цепочке на конкретной ветви дерева отказов

$$P_{Aik} = P_{B1} \cdot P_{B2} \cdot \ldots \cdot P_{Bj} \cdot \ldots \cdot P_{Bm},$$

где $k = 1 \div r$ – номер конкретной ветви дерева отказов; P_{Aik} – вероятность реализации угрозы A_i для конкретной ветви дерева отказов;
$B_1, B_2, \ldots, B_J, \ldots, B_m$ – событие отказов систем и подсистем, находящихся последовательно в цепочке на конкретной ветви дерева отказов;
$P_{B1}, P_{B2}, \ldots, P_{Bj}, \ldots, P_{Bm}$ – вероятность отказов систем и подсистем, находящихся последовательно в цепочке на конкретной ветви дерева отказов.

– шаг 11. Проводится сравнительный анализ вероятности A_i для различных ветвей $k = 1 \div r$ дерева отказов и определяется наибольшее значение P_{Aik}.

– шаг 12. Для ветвей дерева отказов с наибольшими значениями P_{Aik} проводятся работы по повышению работоспособности и надежности систем и подсистем безопасности, инфраструктуры, человеческих ресурсов предприятия.

– шаг 13. Аналогично проводятся действия предполагаемого алгоритма метода анализа риска для всех угроз безопасности, находящихся в базе данных (см. шаг 3 алгоритма).

Проведем анализ риска угрозы безопасности виртуального промышленного предприятия, используя приведенный выше алгоритм.

В качестве упрощенной модели предприятия примем следующее.

Пусть предприятие состоит из следующих элементов:

– охраняемая территория, проходные, ворота для въезда и выезда транспорта;
– несколько зданий – цеха по изготовлению и выпуску сложной продукции, содержащей элементы ноу-хау и подлежащей информационной защите;
– здание конструкторского бюро с закрытой локальной вычислительной сетью для проектирования новых образцов продукции, содержащей базы данных ноу-хау;
– инженерная инфраструктура промышленного предприятия.

В качестве угрозы безопасности предприятия A_i примем похищение преступником конфиденциальной информации, содержащей ноу-хау о продукции, производимой на предприятии.

Согласно модели предприятия можно выделить следующие рубежи защиты предприятия:

– охраняемая территория, проходные, ворота для въезда и выезда транспорта – рубеж защиты № 1;
– периметры и входы-выходы зданий – цехов, конструкторского бюро – рубеж защиты № 2;
– входы-выходы закрытых помещений – рубеж защиты № 3;

– входы-выходы помещений системы энергоснабжения предприятия – рубеж защиты № 4.

В качестве приближенной модели системы информационной безопасности рассматриваемого выше промышленного предприятия будем рассматривать следующий ее состав:

– подсистема № 1 охраны периметра;
– подсистема № 2 режима пропуска людей и техники на территорию предприятия и с нее;
– подсистема № 3 режима пропуска людей в здание конструкторского бюро;
– подсистема № 4 режима пропуска людей в цеха предприятия;
– подсистема № 5 охраны помещений, имеющих элементы локальной вычислительной сети;
– подсистема № 6 защиты закрытых помещений от утечки конфиденциальной информации по техническим каналам;
– подсистема № 7 защиты локальной вычислительной сети, защищающей обрабатываемую конфиденциальную информацию от несанкционированного доступа;
– подсистема № 8 охраны помещений с конфиденциальной информацией;
– подсистема № 9 защиты системы электроснабжения предприятия от выхода ее из строя.

На базе изложенных упрощенных моделей предприятия, системы обеспечения информационной безопасности, а также выделенных рубежей защиты строим дерево возможных отказов систем и подсистем безопасности предприятия. Под отказами будем понимать не только полные отказы систем и подсистем безопасности предприятия, но и сбои в работе этих средств. На рисунке изображено дерево отказов систем и подсистем безопасности предприятия для следующих моделей преступника – похитителя информации:

– преступник – не работник предприятия (модель № 1);
– преступник – не работник предприятия, но имеет доступ на территорию предприятия, в конструкторское бюро (представитель заказчика или соисполнитель) и не имеет доступа в закрытые помещения (модель № 2);
– преступник – работник предприятия, имеющий доступ в цеха, конструкторское бюро, но не имеющий доступа в закрытые помещения (модель № 3);
– преступник – работник предприятия, имеющий доступ в цеха, конструкторское бюро, закрытые помещения, к закрытой локальной вычислительной сети.

Проведем анализ дерева отказов на предмет выявления возможных путей движения преступника к конфиденциальной информации, учитывая при этом, какие системы и подсистемы безопасности должны выйти из строя, чтобы он решил свою задачу.

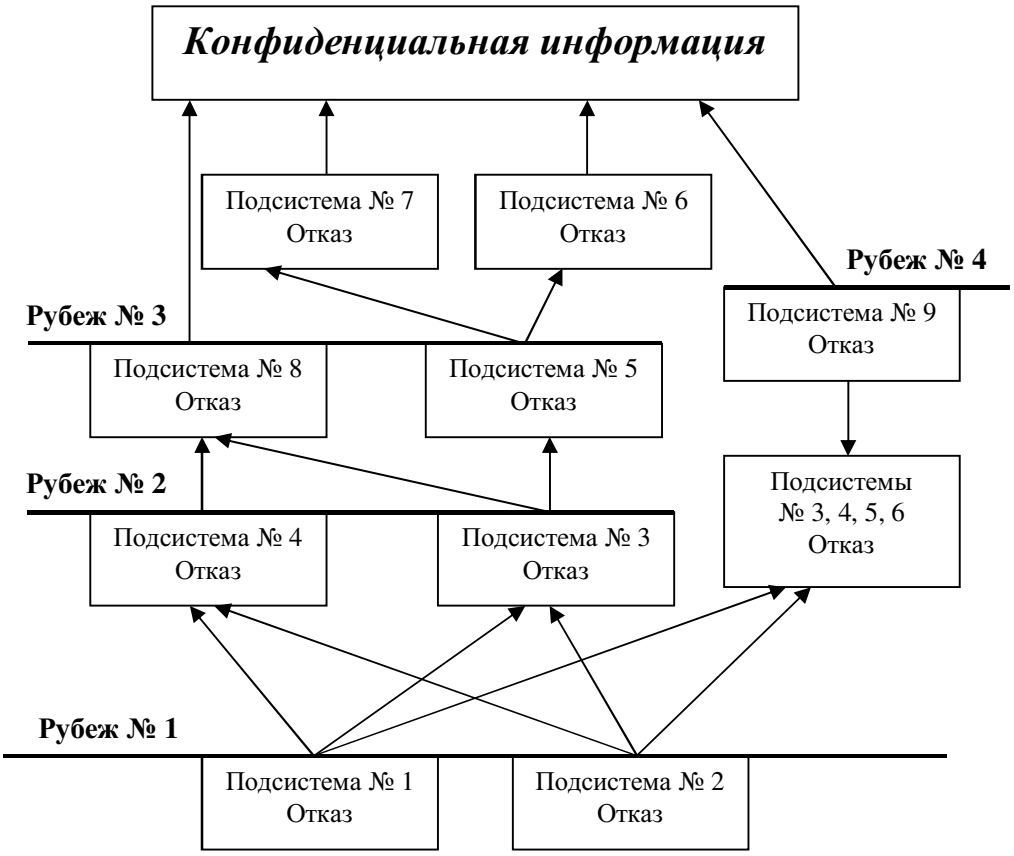
Для модели преступника № 1 возможны следующие варианты цепочек отказов систем и подсистем безопасности, которые могут обеспечить ему получение конфиденциальной информации, т. е. привести к реализации рассматриваемой угрозы:

– вариант 1 (модель № 1): подсистема № 1 (P_1) → подсистема № 4 (P_4) → подсистема № 8 (P_8);

– вариант 2 (модель № 1): подсистема № 1 (P_1) → подсистема № 3 (P_3) → подсистема № 8 (P_8);

– вариант 3 (модель № 1): подсистема № 1 (P_1) → подсистема № 9 (P_9);

– вариант 4 (модель № 1): подсистема № 1 (P_1) → подсистема № 3 (P_3);



Дерево отказов систем и подсистем безопасности предприятия

– вариант 5 (модель № 1): подсистема № 1 (P_1) → подсистема № 3 (P_3) → подсистема № 5 (P_5) → подсистема № 7 (P_7);

– вариант 6 (модель № 1): подсистема № 2 (P_2) → подсистема № 4 (P_4) → подсистема № 8 (P_8);

– вариант 7 (модель № 1): подсистема № 2 (P_2) → подсистема № 3 (P_3) → подсистема № 8 (P_8);

– вариант 8 (модель № 1): подсистема № 2 (P_2) → подсистема № 9 (P_9);

– вариант 9 (модель № 1): подсистема № 2 (P_2) → подсистема № 3 (P_3) → подсистема № 5 (P_5) → подсистема № 6 (P_6);

– вариант 10 (модель № 1): подсистема № 2 (P_2) → подсистема № 3 (P_3) → подсистема № 7 (P_7),

где P_i, $i = 1 \div 9$ – вероятности отказов рассматриваемых систем и подсистем безопасности.

Для модели преступника № 2 возможны следующие варианты цепочек отказов систем и подсистем безопасности, которые могут привести к реализации рассматриваемой угрозы:

– вариант 1 (модель № 2): подсистема № 4 (P_4) → подсистема № 8 (P_8);

– вариант 2 (модель № 2): подсистема № 3 (P_3) → подсистема № 8 (P_8);

– вариант 3 (модель № 2): подсистема № 3 (P_3) → подсистема № 5 (P_5) → подсистема № 6 (P_6);

– вариант 4 (модель № 2): подсистема № 3 (P_3) → подсистема № 5 (P_5) → подси-

стема № 7 (P_7);

– вариант 5 (модель № 2): подсистема № 9 (P_9).

Для модели преступника № 3 варианты цепочек отказов аналогичны таковым для модели преступника № 2.

Для получения преступником конфиденциальной информации при использовании модели преступника № 4 отказы систем и подсистем безопасности не требуются.

При наличии статистических данных по отказам систем и подсистем безопасности можно количественно оценить вероятность отказа всей цепочки любого варианта для любой модели преступника. Например, для варианта № 1 модели преступника № 1 вероятность потери конфиденциальной информации будет составлять

$$P_{\substack{вариант1 \\ модель№1}} = P_1 P_4 P_8 ,$$

а для варианта № 1 модели преступника № 2

$$P_{\substack{вариант1 \\ модель№2}} = P_4 P_8 .$$

Сравнивая вероятности отказов возможных цепочек систем и подсистем безопасности для различных моделей преступников, мы можем определить наиболее вероятную модель действий преступника, наиболее уязвимые места в системе безопасности предприятия и исходя из этого выбрать варианты решений задачи повышения эффективности защиты конфиденциальной информации.

Предлагаемый метод анализа риска обеспечения безопасности предприятия универсален и может быть использован для различных угроз безопасности при любой сложности моделей предприятия, моделей систем безопасности, моделей преступников.

Таким образом, в результате данной работы:

- сформулирована в новой постановке задача анализа риска безопасности предприятия, отличающаяся от ранее известных в решении проблемы анализа совместного влияния модели преступника и отказа элементов, подсистем системы безопасности на вероятность потери конфиденциальной информации;
- предложен метод решения данной задачи, который базируется на вероятностном подходе при оценке риска и теории графов с использованием статистических данных по отказам элементов и подсистем системы безопасности предприятия;
- предложен алгоритм реализации данного метода;
- проведена апробация предложенного алгоритма в целях анализа риска потери конфиденциальной информации для виртуального промышленного предприятия;
- в результате апробации алгоритма получены зависимости вероятности потери конфиденциальной информации от вероятностей отказов элементов, подсистем системы безопасности для заданных моделей действия преступника.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Катулев А.Н., Северцев Н.А, Соломаха Г.М.* Исследование операций и обеспечение безопасности: прикладные задачи: Учеб. пособие. – М.: Физматлит, 2005. – 240 с.
2. *Костогрызов А.И., Степанов П.В.* Инновационное управление качеством и рисками в жизненном цикле систем. – М.: Изд-во ВПК, 2008. – 404 с.
3. *Шоломицкий А.Г.* Теория риска. Выбор при неопределенности и моделирование риска. – М.: Изд-во ГУ ВШЭ, 2005. – 121 с.
4. *Прохоров С.А., Федосеев А.А., Иващенко А.В.* Автоматизация комплексного управления безопасностью предприятия. – Самара: СНЦ РАН, 2008. – 55 с., ил.
5. *Васильева Т.Н., Львова А.В., Хорьков С.Н.* Применение оценок рисков при защите от реальных

угроз информационной безопасности // Современные технологии в задачах управления, автоматики и обработки информации: Труды XVII Международного научно-технического семинара, Алушта, 2008. – Спб.: ГУАП, 2008.
6. *Платонов А.П.* Разработка имитационных систем для анализа рисков на производственных предприятиях // Вестник Челябинского государственного университета. Вып. Экономика. – 2010. – № 3 (184). – С. 101-105.
7. *Плетев П.В., Белов В.М.* Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа, № 1 (25). Ч. 2, 2012.
8. *Семенов А.К.* Мониторинг системы рисков промышленного предприятия // Материалы V Международной научно-практической конференции «Актуальные проблемы развития территорий и систем регионального и муниципального управления». Вып. 3 / Под ред. Ю.В. Вертакова. – Курск: КГТУ, 2010. – С. 98-102.

Статья поступила в редакцию 13 июня 2013 г.

RISK ANALYSIS METHOD FOR ENSURING THE SAFETY OF INDUSTRIAL ENTERPRISES

F.F. Bukanov, V.N. Vorozheikin

Samara State Technical University
244, Molodogvardeyskaya st., Samara, 443100

A method of risk analysis while ensuring the safety of an industrial enterprise is offered. The method in question is based on the probabilistic approach in risk assessment, and the use of statistical data on failures of system and sub-system components, both technical and physical. The proposed method uses the graph theory, i. e. drawing fault and event trees.

Keywords: *method, analyze, risk, enterprise, threat information, security, system, subsystem, refusal, statistics, data, criminal, model, graph, probability, efficiency, protection.*

Fedor F. Bukanov (Ph.D. (Techn.)), Associate Professor.
Vladimir N. Vorozheikin (Ph.D. (Techn.)), Associate Professor.