УДК 004.422.81

ПОСТРОЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ НАУЧНО-ПРОИЗВОДСТВЕННОГО ПРЕДПРИЯТИЯ

А.А. Федосеев

ФГУП ГНПРКЦ «ЦСКБ-Прогресс»,
443009, Самара, ул. Земеца, 18

Рассматривается подход к организации комплексного управления безопасностью научно-производственного предприятия на основе обеспечения согласованного взаимодействия пользователей единого информационного пространства.

Ключевые слова: *безопасность, информационные технологии, управление предприятием*

Введение

В условиях высокой динамики развития современных машиностроительных предприятий для сохранения их конкурентоспособности необходимо обеспечить комплексный характер управления безопасностью на основе данных обо всех процессах жизненного цикла изделий. При этом особое внимание следует уделить своевременности и адекватности оценки рисков и выработке мероприятий по обеспечению безопасности за счет проведения всесторонней оценки ситуаций различными экспертами на основе наиболее полных знаний, полученных из единого информационного пространства предприятия.

1. Обеспечение безопасности предприятия в условиях функционирования единого информационного пространства

Проблеме построения функционально полной системы управления комплексной безопасностью сложных организационно-технических систем, к которым также относятся научно-производственные предприятия, в настоящее время уделяется достаточно много внимания. При этом представляются необходимыми выработка достоверных методик оценки рисков и эффективных алгоритмов мониторинга [1], анализ надежности сложных технических систем [2], разработка паспортов и стандартов безопасности [3, 4].

Однако, во-первых, применение этих результатов на практике часто затруднено в связи со сложностью и специфичностью процессов управления, необходимостью адаптации этих результатов, а также высокой динамикой развития современного предприятия. Во-вторых, недостаточно исследован вопрос управления безопасностью в условиях организации единого информационного пространства на предприятии. Требования своевременного информационного обеспечения всех этапов жизненного цикла изделия, процесса, события, содержащих какие-либо угрозы, одновременно свидетельствуют о недостаточной эффективности стандартных методов обеспечения безопасности и необходимости тесной интеграции усилий сотрудников служб безопасности и информационных технологий.

Федосеев Андрей Алексеевич - заместитель генерального директора по безопасности.

В связи с этим весьма актуальной является задача повышения эффективности управления комплексной безопасностью предприятия путем обеспечения согласованного взаимодействия в едином информационном пространстве его подразделений по противодействию угрозам. Для этого необходимо структуру единого информационного пространства дополнить программными средствами анализа рисков, мониторинга угроз, планирования мероприятий по обеспечению безопасности [5]. Функциональность этих средств позволит подразделениям обмениваться данными и их оценками, а руководству предприятия - управлять безопасностью в режиме реального времени.

Кроме этого, необходимо интегрировать в единое информационное пространство предприятия и средства сбора оперативной информации о событиях нарушения безопасности и результатах мониторинга текущей ситуации с точки зрения безопасности. Интеллектуальная обработка этих данных и их привязка к объектам, подлежащим защите, позволит аналитикам оперативно готовить решения по противодействию угрозам.

Такая организация работ по управлению безопасностью требует дополнительных усилий по обеспечению безопасности самого единого информационного пространства, так как с момента начала его использования подразделениями безопасности в нем появляются сведения о результатах их работы, которые подлежат защите.

2. Обеспечение согласованного противодействия угрозам

Организация согласованного взаимодействия подразделений по обеспечению безопасности и служб информационных технологий является отдельной задачей, сложность которой обусловлена различием бизнес-процессов, регламентов работы и квалификации сотрудников. Создание жестко определенного процесса по взаимодействию в этом случае невозможно, так как нельзя предусмотреть все возникающие угрозы и процедуры противодействия им. В данном случае видится целесообразным обеспечение возможности лицам, принимающим решения, свободно взаимодействовать в едином информационном пространстве, а руководству - координировать их взаимодействие и управлять его динамикой.

Отметим, что поскольку это взаимодействие отражается в результате регистрации сведений обо всех событиях и их обработке, у руководителя появляется возможность анализа этих данных и выработки управляющих воздействий. В качестве инструментария такого анализа можно предложить различные алгоритмы математической статистики; в частности, для обоснования применения мероприятий предлагается использовать алгоритмы анализа рисков, а для исследования динамики согласованного взаимодействия служб безопасности с другими подразделениями целесообразно применять алгоритмы взаимного интервально-корреляционного анализа.

При условии, что известна эффективность мероприятия по снижению риска (по результатам статистической обработки исторических данных, на основании экспертных оценок или данных, полученных в ходе имитационного моделирования), задача поддержки принятия решений будет состоять в выборе необходимых мероприятий на основе данных об изменении риска.

Для оценки рисков можно использовать модель взаимодействия с противником в игре с неизвестными платежами. При этом необходимо учитывать возможность появления неконтролируемых искажающих воздействий. Задачу управления безопасностью следует отнести к классу задач, связанных с неравноправием партнеров, когда противник располагает неизвестными возможностями.

Включение инструментария по согласованному управлению рисками и противодействию угрозам в состав компонентов единого информационного пространства в части управления безопасностью предприятия позволяет обеспечить функциональную полноту профиля интегрированной системы обеспечения комплексной безопасности научно-производственного предприятия [6].

3. Моделирование и анализ деятельности подразделений предприятия по обеспечению безопасности

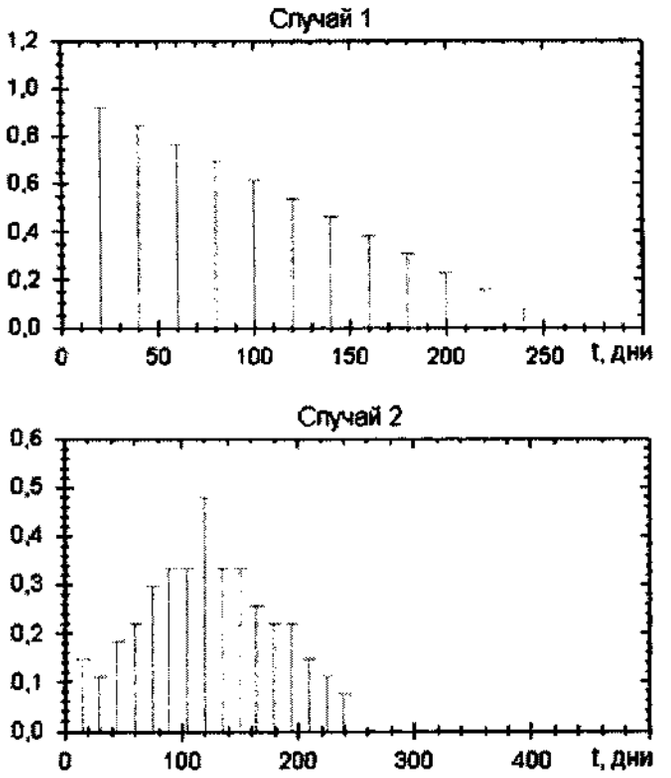
Рассмотрим более подробно аспекты применения интервально-корреляционного анализа для решения задачи управления согласованным противодействием угрозам. Анализ своевременности проведения мероприятий можно проводить на основе информации о потоках событий, связанных с обеспечением безопасности. В частности, для автоматизированного исследования процессов обеспечения безопасности предприятия предлагается использовать имитационную модель противодействия угрозам, в основе которой лежит анализ потоков событий по нарушению безопасности и экспертных оценок. Применение этой модели целесообразно в случае высокой вероятности атак, когда высока важность своевременной и безошибочной оценки риска.

Представить последовательность событий, приводящих к нарушению безопасности предприятия, можно при помощи случайного потока. На основе сведений о типовых процессах по обеспечению безопасности можно сделать вывод, что для построения модели в данном случае подходит поток с аддитивной случайной дискретизацией. Оценки угроз, производимые экспертами, также можно представить при помощи случайного потока с «дрожанием» и пропусками наблюдений. Эксперты, как правило, производят оценки достаточно регулярно, однако возможны задержки, связанные с необходимостью обработки дополнительной информации, а также пропуски оценок, которые в данном контексте отражают отсутствие решение или решение об отсутствии необходимости выставления преграды. В имитационной модели случаи пропуска оценки или неправильной оценки описываются суммарной вероятностью пропуска в потоке экспертных оценок угроз.

Положительная оценка эксперта приводит к выполнению некоторого мероприятия, в результате которого формируется преграда. В описываемой модели учитывается время, требуемое на выполнение мероприятия, и время существования преграды, которое отражает изменение стратегии действий по ее преодолению, актуальность угрозы и стоимость поддержки преграды.

Оценивание взаимной интервальной корреляционной функции (ВИКФ) (см. рисунок) при исследовании эффективности противодействия угрозам в системе обеспечения комплексной безопасности предприятия позволяет определить проблемы, связанные с несвоевременностью оценок и отсутствием согласованности действий экспертов.

Анализ интервальной корреляции в системе противодействию угрозам представляет возможность определить пути совершенствования системы обеспечения комплексной безопасности, а именно с учетом возможности по установлению преград для заданной группы угроз определить необходимую частоту оценок рисков и временные характеристики основных бизнес-процессов служб безопасности. Разработанная с использованием данной модели автоматизированная система позволяет обрабатывать данные о потоках оценок и угроз и проводить анализ этих данных с помощью определения взаимных интервальных корреляционных функций.



Правая часть ВИКФ для соизмеримой частоты событий и оценок (случай 1) и при частоте событий, в два раза большей частоты оценок (случай 2)

Заключение

При построении комплексной системы управления безопасностью современного научно-производственного предприятия наряду с использованием современных технологий защиты необходимо осуществить проведение двух организационно-технических мероприятий:

1) организовать работу служб безопасности в едином информационном пространстве, что, во-первых, приведет к их тесному взаимодействию с другими подразделениями в рамках современных процессов управления жизненными циклом изделия, а во-вторых, предоставит им актуальные знания об использовании и изменении сведений, подлежащих защите;
2) по результатам работы служб безопасности в едином информационном пространстве необходимо провести анализ динамики противодействия угрозам и обеспечить согласованное взаимодействие подразделений в этом направлении, руководствуясь результатами взаимного интервально-корреляционного анализа.

В этом случае создаваемая комплексная система будет своевременно и эффективно реагировать на возникающие угрозы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Габричидзе Т.Г., Янников И.М., Зозуля В.Г.* Локальные системы оповещения в районах размещения потенциально опасных объектов в Удмуртской Республике // Вестник Самар. гос. техн. ун-та. – 2008. – №2 (22). – С. 73-79.
2. *Викторова В.С., Степанянц А.С.* Программные комплексы по анализу надежности, безопасности и эффективности систем // 3-я Международная конференция по проблемам управления. Пленарные доклады и избранные труды. – М.: ИПУ РАН. – 2006. – С. 738-740.
3. *Юсупова Н.И., Митакович С.А., Еникеева К.Р.* Системное моделирование процесса информационной поддержки разработки паспортов безопасности опасных производственных объектов // Вестник УГАТУ. Сер. Управление, вычислительная техника и информатика. – 2008. – Т. 10. – №2 (27). – С. 80-87.
4. *Резников Г.Я., Бабин С.А., Костогрызов А.И., Родионов В.Н.* Количественная оценка защищенности автоматизированных систем от несанкционированного доступа // Информационные технологии в проектировании и производстве. – 2004. – №1. – С. 11-22.
5. *Федосеев А.А., Прохоров С.А., Иващенко А.В.* Комплексное управление безопасностью в едином информационном пространстве предприятия // Программные продукты и системы. – 2008. – №4. – С. 132-135.
6. Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения / С.А. Прохоров, А.А. Федосеев, В.Ф. Денисов, А.В. Иващенко. – Самара: СНЦ РАН, 2008. – 199 с.

Статья поступила в редакцию 16 сентября 2009 г.

UDC 004.422.81

DEVELOPMENT OF SECURITY COMPLEX MANAGEMENT SYSTEM AT RESEARCH AND PRODUCTION ENTERPRISE

A.A. Fedoseev

Samara Space Centre, 1
8, Zemets Street, Samara, 443009 Russia

The approach is described of complex management of research and production enterprise security based on organization of interactive cooperation of solid information space users.

Key words: *security, information science, enterprise management.*