ПРИНЯТИЕ РЕШЕНИЙ НА ОСНОВЕ ДАННЫХ МОНИТОРИНГА ИНФОРМАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЙ

Витенбург Е.А.[1], Никишова А.В.[1], Оладько В.С.[2], Умницын М.Ю.[1], Омельченко Т.А.[1], Садовникова Н.П.[1]

1. Волгоградский государственный университет,
Россия, г. Волгоград, пр. Университетский д.100
2. Финансовый университет при Правительстве Российской Федерации,
Россия, г. Москва, Ленинградский просп. д. 49
e.vitenburg@ec-rs.ru, nikishova.arina@volsu.ru, vsoladco@fa.ru, umnitsyn@volsu.ru, omelchenko.tatiana@volsu.ru, sadovnikova.natalia@volsu.ru

Аннотация: Из-за функционирования в крупномасштабных системах, система защиты информации также является большой и сложной системой. Поэтому к управлению самой системой следует добавить и управление ее системой защиты информации. Важнейшим этапом управления является принятие решений.

Ключевые слова: информационная система, злоумышленник, система защиты информации, события безопасности, мониторинг событий безопасности, принятие решений, методы поддержки приятия решений.

Введение

Развитие крупномасштабных систем в современных условиях не возможно без внедрения информационных технологий. Но тогда встает проблема обеспечения безопасности функционирования внедренных информационных систем и ресурсов, циркулирующих, хранящихся и обрабатывающихся в них. Из-за функционирования в крупномасштабных системах, система защиты информации также является большой и сложной системой. Поэтому к управлению самой системой следует добавить и управление ее системой защиты информации. Важнейшим этапом управления является принятие решений. Системы поддержки принятия решений имеют широкое применение в области менеджмента и только начинают находить свое применение в сфере защиты информации. Существуют различные подходы к поддержке принятия решений. Но все они предполагают генерацию решений на основе анализа больших данных. В данной статье предлагается подход к принятию решений на основе данных мониторинга безопасности информационных систем. Для автоматизации процесса принятия решений на основе результатов мониторинга событий предложен программный комплекс. В рамках статьи рассмотрена его формализованная модель и архитектура. Результатом работы программного комплекса является интегральная оценка текущего уровня безопасности информационной системы. Оценка формируется посредством анализа частных показателей безопасности, полученных на основе данных периодического мониторинга информационной системы.

1 Компоновка текстового материала

В настоящее время большинство предприятий сталкиваются с рядом проблем из-за недостаточной эффективности управления информационной безопасностью своих информационных систем. Анализ статистических данных, которые были получены ведущими компаниями в области информационной безопасности [1-2], показывает, что на 2018 год около 76% информационных систем являются уязвимыми к угрозам нарушения информационной безопасности.

Данные угрозы могут проявляться как в виде внутренних и внешних атак злоумышленника, так и в виде дестабилизирующих воздействий случайного характера. В результате реализации данных угроз предприятие несет финансовые потери, связанные с перебоями в работе производства, прерыванием бизнес-процессов, потерей клиентов и репутации.

Согласно [3] процесс управления информационной безопасностью состоит из планирования, выполнения, проверки и действия. Эти шаги определяют цикл PDCA.

Процесс начинается с первоначального проектирования системы защиты информации. Он построен на основе нормативных документов, применимых к конкретной информационной системе. Далее в информационной системе реализуется проект системы защиты информации. После этого организуется мониторинг событий безопасности, происходящих в информационной системе. На основе данных мониторинга принимается решение о целесообразности изменения существующего проекта системы защиты информации.

2 Модель принятия решений на основе данных мониторинга информационных систем

В основе разработанного программного комплекса принятия решений на основе данных мониторинга информационных систем заложена формализованная модель. Целевым назначением

модели является интегральная оценка текущего уровня безопасности информационной системы. Оценка реализуется посредством анализа частных показателей безопасности, которые получены на основе данных периодического мониторинга информационной системы. Для этого решается набор следующих задач: сбор данных о событиях в информационной системы; классификация событий; определение значений частных показателей безопасности; интегральная оценка текущего уровня безопасности информационной системы; принятие корректирующего решения.

С учетом выделенных особенностей разрабатываемую систему принятия решений на основе данных мониторинга информационной системы MPS =(MIS, ACE, DF) предлагается разбить на три ключевых множества подсистем: подсистему мониторинга событий информационной системы - MIS; подсистему оценки частных показателей безопасности информационной системы - ACE; подсистему принятия решений и оценку уровня безопасности информационной системы – DF.

Разработан программный комплекс для реализации системы, архитектура которого состоит из нескольких подсистем. Пользовательский интерфейс имеет графический вид и предназначен для ввода данных, взаимодействия с пользователем и вывода результатов мониторинга. Подсистема сбора данных с журнала событий предназначена для распределенного сбора информации из журналов событий операционной системы и составления списка событий с указанием их ключевых атрибутов. Подсистема анализа параметров событий предназначена для классификации состояний событий на нормальные, аномальные, опасные, и расчета параметров событий: частота возникновения, потенциальный ущерб. Подсистема оценки рисков и ранжирования событий по уровню опасности предназначена для расчета рисков по каждому событию, расчету общего уровня риска информационной безопасности, подсчета количества аномальных и опасных событий. Подсистема классификации состояний ИС предназначена для предварительной классификации состояний информационной системы на аномальные, нормальные и опасные. База данных хранит шаблоны базовых множеств нормальных и опасных событий, параметры векторов состояний информационной системы и данные о результатах предыдущего мониторинга. Подсистема принятия решений, предназначена для формирования векторов текущего и требуемого состояния уровней безопасности информационной системы, вычисления метрик близости векторов и принятия решений о принадлежности текущего системы к одному из пяти уровней безопасности информационной системы.

3 Экспериментальные исследования

Экспериментальное исследование направлено на получение интегральной оценки текущего уровня безопасности информационной системы посредством анализа частных показателей безопасности, полученных на основе данных периодического мониторинга информационной системы. На основании оценки уровня безопасности генерируется управляющее решение. Для этого необходимо выполнить следующие этапы: выбрать журнал событий, подлежащий анализу (первый этап), осуществить обработку собранной выборки событий (второй этап), провести классификацию событий и состояний системы (третий этап), рассчитать значение уровня безопасности системы (четвертый этап).

Эксперименты проводились на тестовой информационной системе. Общий показатель уровня безопасности системы был определен как «опасный», что в первую очередь связано с наличием большого числа опасных событий – 32%. Подобный уровень указывает на необходимость детального анализа событий происходящих в системе, разбора инцидентов информационной безопасности, зафиксированных в последний месяц. А также срочного принятия мер по устранению и локализации причин и источников опасных событий.

Анализ частоты обнаруженных опасных событий показал, что наиболее распространенной группой нарушений являются опасные события. На основе полученных данных работы программного комплекса принятия решение на основе мониторинга событий информационной системы с целью повышения уровня безопасности информационной системы и противодействия актуальным угрозам, связанным с обнаруженными событиями предлагаются следующие решения: применить политику использования надежных паролей и более коротких сроков действия паролей; ввести ограничение на количество попыток входа в систему и в случае превышения порогового значения производить блокировку учетной записи; проводить дополнительный мониторинг и аудит действий, связанных с повышением привилегий и работой под учетной записью администратора; использовать дополнительные программные или программно-аппаратные средства доверенной загрузки и защиты от несанкционированного доступа в систему.

Литература

1. Уязвимости в АСУ ТП: итоги 2018 года // Аналитика компании Positive Technologies. / URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-vulnerabilities-2019.
2. Глобальное исследование утечек конфиденциальной информации в 2018 году // Отчет InfoWatch. / URL: https://www.infowatch.ru/resources/report2018.
3. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. 2006.
4. *Козлов Д.Б.* Метод принятия решений в условиях неопределенности // Известия ТулГУ. Технические науки. 2008. №2. – С. 278-286.
5. *Витенбург Е.А., Калинин П.А.* Архитектура модели интеллектуальной поддержки принятия решений в области защиты информации // Современные концепции развития науки. Сборник статей Международной научно-практической конференции, 2016. – С. 9-13.
6. *Xingmei L., Yaxian W., Qingyou Ya., Xinchao Zh.* Uncertain mean-variance model for dynamic project portfolio selection problem with divisibility // Fuzzy Optimization and Decision Making. Volume 18, Issue 1. 2019. – pp. 37–56.
7. *Zhihua Ch., Yanfei L., Ruiqing Zh.* Impacts of risk attitude and outside option on compensation contracts under different information structures // Fuzzy Optimization and Decision Making. Volume 17, Issue 1. 2018. – pp. 13–47.
8. *Yong-Jun L., Wei-Guo Zh.* Fuzzy portfolio selection model with real features and different decision behaviors // Fuzzy Optimization and Decision Making. Volume 17, Issue 3. 2018. – pp. 317–336.