УДК 004.732

С.Ю. Исхаков, А.А. Шелупанов, А.Ю. Исхаков

Имитационная модель комплексной сети систем безопасности

Предложен подход к построению имитационной модели информационной безопасности комплексных сетей систем безопасности. Определены характерные особенности сетей данного типа и показана разница в подходах к обеспечению их защиты по сравнению с типовыми локально-вычислительными сетями. Предложена имитационная модель, учитывающая не только внешние, но и внутренние угрозы нарушения информационной безопасности системы.
Ключевые слова: комплексные сети систем безопасности, имитационная модель, инцидент безопасности, частная модель.

Проблемы мониторинга комплексных сетей систем безопасности. Решение задач, связанных с обеспечением безопасности жизни и здоровья человека на предприятиях, базируется на двух аспектах. С одной стороны, действующее законодательство обязывает работодателя обеспечить безопасность жизни и здоровья сотрудников во время исполнения ими своих служебных обязанностей. С другой стороны, любая организация является участником рыночных отношений и заинтересована в обеспечении сохранности своего имущества. Необходимо отметить, что системы безопасности априори не являются источником дохода для компании. Основной принцип таких систем – снижение рисков нанесения материального ущерба.

Для достижения баланса между затрачиваемыми экономическими ресурсами и стоимостью рисков реализации угроз безопасности большинство современных организаций оборудуют свои объекты системами безопасности. К ним относятся охранно-пожарные сигнализации, видеонаблюдение, системы контроля и управления доступом, системы автоматического пожаротушения и оповещения о пожаре, а также различные инженерные системы диспетчеризации.

В большинстве случаев перед администраторами систем безопасности возникает задача объединения их в единый комплекс с централизованным управлением. Широко распространенным подходом к решению подобных задач является объединение гетерогенного оборудования на базе технологий локальных сетей: все управляющие блоки задействованных систем связываются в комплексную сеть систем безопасности (КССБ).

Под КССБ понимается сложный гетерогенный комплекс аппаратного и программного обеспечения (ПО), различающегося по принципам действия и типу предоставляемой оператору информации, но объединенного общей задачей. Задача такого комплекса состоит в обеспечении безопасности человека на предприятии и снижении вероятности нанесения материального ущерба компании.

В качестве платформы для создания единой системы передачи информации используются технологии локально-вычислительных сетей (ЛВС). Эксплуатация таких комплексов связана с рядом исключительных особенностей:

1. *Гетерогенность оборудования и ПО.* Из-за чрезмерно большой области задач, решаемых с помощью КССБ, существует огромное количество производителей и решений для каждой из подсистем. Действующее законодательство не регламентирует создание таких комплексов. Государственные регуляторы контролируют проектирование, монтаж и эксплуатацию систем, связанных с обеспечением пожарной безопасности объектов. Все остальные слаботочные инженерные системы не являются обязательными и внедряются исключительно по желанию хозяйствующего субъекта. Это приводит к проблемам агрегирования информации, предоставляемой различными подсистемами.

2. *Апериодичность нагрузок.* Одной из наиболее характерных особенностей функционирования КССБ является отсутствие какой-либо периодичности в распределении нагрузки на элементы. Все системы безопасности направлены на выявление и предупреждение о возникновении внештатной ситуации. Большую часть времени они работают в режиме ожидания, и нагрузка на элементы минимальна. Так, например, в КССБ нередко используется видеосервер, к которому подключены аналоговые видеокамеры. Сервер собирает информацию и помещает ее в локальное хранилище. В данном режиме генерируемый им трафик минимален. В случае подключения к серверу клиентского

приложения с удаленной рабочей станции начинается передача информации. Особенностью трансляции видео в ЛВС является потребление всей свободной части канала передачи данных.

3. *Высокая степень приоритетности обслуживания.* В состав КССБ входят подсистемы обеспечения безопасности жизнедеятельности человека (системы пожарной безопасности, электронные проходные и т.д.), поэтому данная сеть требует повышенных мер по организации бесперебойной работы и приоритетности обслуживания.

4. *Наличие критически важной информации* [1]. Внутри КССБ хранится и передается информация, имеющая критическое значение для компании. К ней относятся не только оповещения о внештатных ситуациях, но и видеозаписи камер охранного наблюдения, журналы доступа к объектам, настройки средств противодействия шпионажу и т.д.

5. *Территориальная распределенность.* Из-за высокой стоимости внедрения и обслуживания КССБ обычно разворачивается на предприятиях среднего и крупного бизнеса. Основным инструментом снижения затрат на системы безопасности являются унификация структуры и объединение территориально удаленных объектов компании с созданием единого центра управления.

Несмотря на то, что в основе КССБ лежат технологии локальных сетей, подходы к обеспечению информационной безопасности (ИБ) [1, 2], используемые в типовых ЛВС, ограниченно применимы для КССБ. Это объясняется тем, что нарушение доступности или целостности таких сетей может привести к возникновению чрезвычайных ситуаций. Разница подходов к ИБ для типовых ЛВС и КССБ представлена в таблице.

Различия подходов к обеспечению ИБ в ЛВС и КССБ

Вопросы ИБ	ЛВС	КССБ
Средства антивирусной защиты	Широкое применение	Используются редко
Жизненный цикл системы	3–5 лет	8–10 лет
Установка исправлений безопасности	Регулярно	Нерегулярно
Управление изменениями	Систематически	При необходимости
Критически важная информация	Задержки допускаются	Задержки недопустимы
Доступность	Задержки допускаются	Задержки недопустимы
Аудит ИБ	Планируется и реализуется внешними организациями	Внутренний аудит

Из сравнительной таблицы видно, что типовые методы обеспечения ИБ ЛВС применимы для КССБ в малой степени. Это определяет необходимость защиты КССБ дополнительными средствами.

Многие из систем, входящих в КССБ, обладают собственными средствами защиты, которые необходимо согласовать между собой. Поскольку для обеспечения безопасности любой корпоративной информационной системы важно наличие общей платформы, то необходима эффективная политика безопасности [3] как основа для согласования всех компонентов защиты. Для обеспечения защиты КССБ проектировщиками и администраторами принимаются решения, направленные на максимальную изоляцию от общей сети передачи данных (СПД) компании, вплоть до разделения на физическом уровне. В точках соприкосновения с СПД внедряют системы обнаружения вторжений [5].

Основная проблема заключается в том, что при использовании такого подхода рассматриваются только риски [9, 10], связанные с внешними вторжениями в КССБ. Степень вероятности реализации внутренних угроз [3] нарушения доступности, целостности или конфиденциальности системы обычно принимают низкой. К таким угрозам можно отнести выход из строя видеокамеры либо архива видеозаписей, потерю питания станций пожарной сигнализации, отключение считывателей карт доступа, распространение вредоносных программ по причине человеческого фактора и т.д. В случае реализации таких угроз могут произойти как однозначно выявленные (явные), так и скрытые инциденты безопасности [1].

В случае КССБ под инцидентом безопасности (инцидентом) понимается любое незаконное, неразрешенное, неблагоприятное событие (НС), которое совершается в информационной системе.

К явным ИБ можно отнести, например, выход из строя видеосервера, и как следствие исчезновение сигнала с нескольких видеокамер. Если в организации имеется пост охраны, куда выводятся данные с видеокамер, то такое событие, вероятно, будет незамедлительно обнаружено и оперативно будут приняты меры по нейтрализации данной угрозы.

В случае выхода из строя сетевого хранилища камеры продолжат свою работу, видеосъемка будет продолжаться, но архива записей не будет. Время выявления такого инцидента может возрасти

до нескольких дней. Наступление такого события можно охарактеризовать как скрытый инцидент. Если в период окна опасности [1, 5], возникшего по причине скрытого инцидента, произойдет другой инцидент (например, кража имущества из помещения, контролируемого только видеокамерой), то стоимость риска кратно повысится, так как невозможно будет предпринять действия по идентификации нарушителя и провести расследование.

Таким образом, несмотря на изолированность КССБ и наличие средств защиты периметра, остается актуальной задача контроля текущего состояния КССБ и обеспечения выполнения основных функций всех систем безопасности. Для решения такой задачи необходимо организовать управление рисками реализации не только внешних, но и внутренних угроз. Учитывая приведенное ранее определение инцидента безопасности, в список угроз должны быть включены события, способные привести к аппаратным сбоям элементов системы.

Организация контроля текущего состояния системы сводится к проектированию и внедрению систем мониторинга ЛВС. Однако для сохранения принципа систем безопасности необходимы также средства прогнозирования инцидентов.

Определение нестабильного состояния системы на основе данных мониторинга. Задача обнаружения сбоев в работе ЛВС является весьма сложной из-за невозможности четкого определения критериев и разделения инцидентов безопасности и штатного изменения режима работы системы [7]. В данном случае наиболее обоснованным является подход к решению такой задачи с помощью мониторинга необходимого числа параметров с целью выявить отклонения в стабильной работе системы. В [8] рассмотрены основные аспекты использования подобных систем. Установлено, что принцип их работы основан либо на использовании сигнатур, либо на привлечении статистических методов.

Учитывая вышеописанные особенности КССБ, решение поставленных задач предпочтительно осуществлять с помощью статистических методов. Авторами была предложена методика [2], позволяющая определять необходимый и достаточный набор параметров для обнаружения инцидентов безопасности при заданном уровне детализации.

Полученные в результате использования предложенной методики частные модели сетевых элементов (СЭ) можно описать в виде (1)

$$\mathbf{E} = (p_1, p_2, \ldots, p_k), \tag{1}$$

где $p_1, \ldots, p_k$ – параметры СЭ, k – количество выбранных параметров для данной частной модели.

В текущий момент времени каждый из параметров СЭ характеризуется определенным значением δ. Текущее состояние СЭ есть совокупность текущих значений его параметров в данный момент времени. Если обозначить состояние СЭ как $\boldsymbol{\sigma}$, то

$$\boldsymbol{\sigma}_i = (\delta_1, \delta_2, \ldots, \delta_k), \tag{2}$$

где i – это текущий момент времени.

Задача выявления сбоев в работе системы сводится к определению, является ли текущее значение параметра δ_k свидетельством наступления инцидента безопасности.

Критерии выявления инцидентов безопасности могут быть представлены в виде логических функций

$$Criterion = (O, P, Z). \tag{3}$$

Функция (3) имеет булеву область значений и принимает значение ИСТИНА, когда параметр P объекта O находится в пределах допустимых значений Z, и ЛОЖЬ – в противном случае.

СЭ находится в безопасном состоянии, когда все связанные с ним функции Criterion принимают значение ИСТИНА.

Из предложенной в [4] методики следует, что если конкретный параметр СЭ входит в его частную модель (при заданном уровне детализации), то должно существовать правило, относящее его к данному СЭ (4).

$$r(O, P), \tag{4}$$

где O – конкретный СЭ; P – конкретный параметр СЭ.

Тогда $R = \{r = r(O, P)\}$ – множество правил r, сформированное в результате применения методики для определения необходимого и достаточного набора параметров для обнаружения инцидентов безопасности.

Имитационную модель информационной безопасности КССБ при заданном уровне детализации можно описать совокупностью СЭ, наборов параметров и критериев, разработанных для проверки соответствия состояния системы требованиям действующей политики безопасности (5):

$$\begin{aligned} &\forall O \in S, \\ &\forall P \exists r = r(O,P) \in R, \\ &\forall P \exists Criterion = (O,P,Z). \end{aligned} \tag{5}$$

Применение имитационной модели для оценки состояния системы. Полученную имитационную модель можно использовать для определения текущего состояния системы (рис. 1). На вход модели подаются текущие значения параметров СЭ, полученные на этапе сбора информации. В случае выполнения всех условий (5) вычисляется значение критерия для каждого из проверяемых показателей. Если в результате проверки все критерии имеют значение ИСТИНА, то система находится в безопасном состоянии, в противном случае – нет. Другими словами, система находится в безопасном состоянии, если текущие значения параметров всех СЭ соответствуют требованиям политики безопасности.

Рис. 1. Применение имитационной модели информационной безопасности КССБ

После получения имитационной модели нерешенным остается вопрос формирования критериев. Учитывая масштабы КССБ и особенности ее функционирования, множество *R* может содержать десятки и сотни критериев. На ранних стадиях исследования авторами предпринимались попытки решения данной задачи путем формирования критериев в виде пороговых значений для каждого параметра. Исследования показали, что такой подход не является эффективным.

Во-первых, количество контролируемых параметров прямо пропорционально количеству СЭ в системе, которое имеет тенденцию увеличиваться. Это приводит к увеличению времени и ресурсов, необходимых для формирования всех критериев.

Во-вторых, формирование критериев возможно только на основе экспертных оценок, построенных на базе продолжительных наблюдений.

В-третьих, особенности функционирования КССБ, связанные с апериодичностью в работе систем безопасности, являются причиной частого появления ложных сигналов о наступлении инцидентов безопасности.

Основываясь на вышеприведенных позициях, авторами были сформированы основные требования к процедуре формирования критериев:

– критерии должны формироваться регулярно для оценки каждого поступившего на вход модели значения;

– метод формирования критериев должен учитывать предыдущие значения показателя за некоторый предыдущий период с учетом их распределения во времени.

Одним из наиболее подходящих методов, удовлетворяющих поставленным условиям, является использование методов прогнозирования для оценки текущих значений параметров.

Заключение. Использование технологий локальных сетей для агрегирования информации, поступающей из гетерогенных систем, позволило сформировать понятие КССБ – специализированный вид ЛВС, обладающий характерными особенностями функционирования. Учитывая, что основное предназначение КССБ заключается в обеспечении безопасности жизни и здоровья человека, актуальным является вопрос моделирования работы таких систем и мониторинга состояния их систем защиты.

Предложенные авторами имитационная модель и подход к формированию критериев определения текущего состояния системы позволяют учитывать не только риски реализации внешних угроз, но и наступления событий, способных привести к аппаратным сбоям элементов системы. Отличительной особенностью данной имитационной модели является независимость от типа параметра объекта и его физического смысла.

Исходя из сформированных требований к процедуре формирования критериев, можно сделать вывод, что для оценки текущего состояния защищенности систем безопасности необходимо на ос-

нове оценки предыдущих значений исследуемого параметра формировать прогноз и сравнивать его с текущим значением. В [4] авторами был предложен подход к анализу данных мониторинга и формированию критериев оценки с помощью методов прогнозирования.

Литература

1. Мещеряков Р.В. Специальные вопросы информационной безопасности / Р.В. Мещеряков, А.А. Шелупанов. – Томск: Изд-во Института оптики атмосферы СО РАН, 2003. – 224 с.

2. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1. – С. 28–35.

4. Исхаков С.Ю. Разработка методического и программного обеспечения для мониторинга работы локальных сетей / С.Ю. Исхаков, А.А. Шелупанов // Телекоммуникации. – 2013. – № 6. – С. 16–21.

5. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 278 с.

6. Зайцев А.П. Технические средства и методы защиты информации: учебник / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2012. – 442 с.

7. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных / О.О. Евсютин, А.А. Шелупанов // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 119–125.

8. Исхаков С.Ю. Прогнозирование в системе мониторинга локальных сетей / С.Ю. Исхаков, А.А. Шелупанов, С.В. Тимченко // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 100–103.

9. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

10. Кускова А.А. Оценка рисков информационной безопасности телекоммуникационной системы / А.А. Кускова, А.А. Шелупанов, Р.В. Мещеряков, С.С. Ерохин // Информационное противодействие угрозам терроризма. – 2009. – № 13. – С. 90–92.

Исхаков Сергей Юнусович
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: frosty86@mail.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, проректор по научной работе ТУСУРа
Тел.: 8 (382-2) 514-302
Эл. почта: saa@tusur.ru

Исхаков Андрей Юнусович
Аспирант каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: iay@keva.tusur.ru

Iskhakov S.Y., Shelupanov A.A., Iskhakov A.Y.
Engineering of imitation model of a complex network of security systems

Approach to creation of imitating model of information security of complex networks of systems of safety is offered. Characteristics of networks of this type are defined and the difference in approaches to ensuring their protection in comparison with standard local computer networks is shown. The imitating model considering not only external, but also internal threats of violation of information security of system is offered.
Keywords: complex networks of systems of safety, imitating model, safety incident, private model.