V.S. Makeev, A.S. Zaytsev

Prediction Of Dynamics Of Insider Threat Of Sabotage Using The System Dynamics Modeling

Keywords: IT-sabotage, insider, system-dynamic modeling

This article present a research of the threat of it-sabotage with the use of information resources of organization.Based on statistical information and relevant research, here was designed a system-dynamic model and represented results of test simulations.

В.С. Макеев, А.С. Зайцев

ПРОГНОЗИРОВАНИЕ РАЗВИТИЯ УГРОЗЫ ИНСАЙДЕРСКОГО САБОТАЖА ПРИ ПОМОЩИ СИСТЕМНО-ДИНАМИЧЕСКОГО МОДЕЛИРОВАНИЯ

До недавних пор основным направлением исследований в области обеспечения информационной безопасности (ИБ) оставалось противодействие внешним угроза, в то время как защита от внутренних угроз оставалась на втором плане. Однако, согласно данным исследования компании Positive Technologies [1], внутренние угрозы, такие как злоумышленные и незлоумышленные нарушения политики ИБ сотрудниками, зачастую оказываются более опасны, чем вирусы и внешние атаки. Более чем в половине опрошенных Positive Technologies компаний (58%) такие инциденты привели к существенным проблемам: в 31% компаний это были нарушения информационно-телекоммуникационной инфраструктуры (ИТ-инфраструктура), 15% компаний понесли серьезные финансовые потери, а 12% компаний был нанесен урон репутации.

Проблема внутреннего нарушителя исследуется не так давно, поэтому на данный момент не существует полноценной методологии защиты ИТ-инфраструктуры и ресурсов от внутренних угроз ИБ. Исследование внутренних нарушителей ИБ осложняется необходимостью оценивать как технические, так и поведенческие аспекты, анализ и прогнозирование которых не всегда однозначны и зависят от множества факторов.

Поведение внутреннего нарушителя, реализующего угрозу саботажа с использованием информационных систем организации (ИТ-саботаж), наиболее сложно предугадать ввиду его импульсивного поведения (саботажник использует информационные системы для нанесения вреда организации или конкретному сотруднику). Поэтому перед применением контрмер крайне полезной для руководителя является возможность прогнозирования поведения инсайдера после различных действий со стороны организации.

В качестве метода для моделирования развития угрозы ИТ-саботажа целесообразно использовать системную динамику Дж. Форрестера [2]. Данный метод был впервые применен для исследования внутренних угроз ИБ в работах [3,4], где нотация системной динамики применена для разработки диаграммы поведения ИТ-саботажника, но математический аппарат метода не задействован и полноценного моделирования не произведено.

Разработка системно-динамической модели ИТ-саботажа

Разработка системно-динамической модели ИТ-саботажа состоит из последовательных стадий построения схемы взаимодействия основных элементов системы пове-

дения, диаграммы причинно-следственных связей (ДПСС), диаграммы потоков (ДП), задания параметров ДП и проведения тестового моделирования.

В рамках исследования проанализировано более 50 случаев ИТ-саботажа, найденных в открытых источниках и сформирована схема взаимодействия основных элементов системы поведения ИТ-саботажника.

Ключевым фактором в ИТ-саботаже является мотивация инсайдера – желание внутреннего нарушителя совершить диверсионный акт. Поведение инсайдера зависит от его мотивации и технических возможностей. При недостаточном уровне доступа ИТ-саботажник может провести действия по повышению уровня доступа к информационной системе организации: создание недекларированных учетных записей, изменение параметров доступа к системе, установка шпионского программного обеспечения, кража учетных данных коллег. На мотивацию оказывают влияние личные качества инсайдера, нежелательные действия со стороны работодателя, а также факт увольнения, являющийся одной из наиболее распространенных причин ИТ-саботажа. Поведение инсайдера приводит к ущербу для организации, а также является источником технических и поведенческих индикаторов, по которым организация может получить информацию об инциденте ИБ и отреагировать на это ограничением доступа для инсайдера или увольнением.

Основные элементы системы поведения ИТ-саботажника приведены в табл. 1, а схема их взаимодействия – на рис. 1.

Таблица 1. Основные элементы системы поведения ИТ-саботажника

№	**Элемент**	**Другие элементы, оказывающие на него воздействие**
1	Мотивация инсайдера	Увольнение инсайдера. Реакция организации. Личные качества и особенности инсайдера
2	Реакция организации	Получение информации организацией
3	Получение информации организацией	Поведение инсайдера
4	Технические возможности инсайдера	Реакция организации. Увольнение инсайдера. Технические действия по подготовке к саботажу
5	Технические действия по подготовке к саботажу	Технические возможности инсайдера. Мотивация инсайдера
6	Ущерб организации	Поведение инсайдера
7	Увольнение инсайдера	Мотивация инсайдера. Реакция организации
8	Поведение инсайдера	Мотивация инсайдера. Технические возможности инсайдера
9	Личные качества и особенности инсайдера	

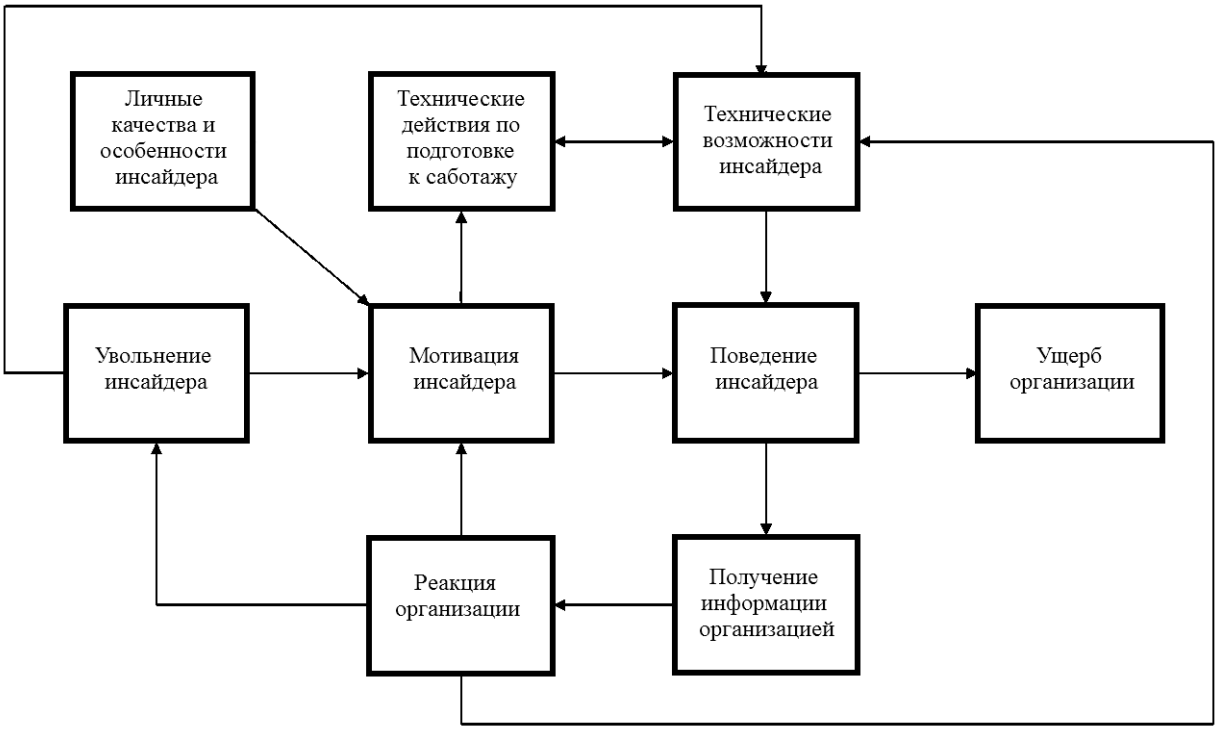

Рис. 1. Схема взаимодействия основных элементов системы поведения ИТ-саботажника

В рамках исследования статистической информации разработаны портрет типичного ИТ-саботажника и основные особенности угрозы, приведенные в табл. 3 и 4, соответственно.

Таблица 2. Портрет нарушителя для ИТ-саботажа

№	Характеристика	Описание
1	Занимаемая должность в организации	Системный администратор, программист, сервис-менеджер – привилегированная (чаще техническая) должность с доступом к множеству ресурсов компании
2	Методы атаки	Как технически простые с использованием легально предоставленных прав и полномочий, так и сложные, требующие специализированных знаний (написание логических бомб, переконфигурирование сети)
3	Характер действий	Удаление/порча критически важных файлов и настроек информационных систем, неправомерный доступ к сервисам (после увольнения), физическая порча объектов информационной инфраструктуры компании
4	Длительность преступления	Чаще всего 1 день (единичное действие – взлом/порча имущества), реже – несколько недель (при удаленном продолжительном негативном воздействии на ИС организации)
5	Обнаружение преступления	По факту исполнения преступления, либо мониторинг ИБ и ИТ-аудит на наличие недекларированных путей доступа к информационной системе организации

Таблица 3. Характерные особенности ИТ-саботажа

№	Характерная особенность	Элемент системы
1	В большинстве случаев мотивом совершения диверсии является обида на руководство организации и желание отомстить. Среди причин обиды необходимо отметить увольнение сотрудника, отказ в повышении по службе, неоправданные ожидания сотрудника	Мотивация инсайдера
2	На совершение ИТ-саботажа зачастую влияют межличностные конфликты в компании (с коллегами и руководством), алкогольная и наркотическая зависимости, проблемы с психикой и склонность к агрессии	Поведение инсайдера. Личные качества инсайдера
3	Большинство инсайдеров, осуществляющих диверсионные акты, обладают привилегированным доступом к файлам и системам организации, поэтому действуют без сговора, в одиночку	Технические возможности инсайдера. Поведение инсайдера
4	Если причиной реализации угрозы является увольнение, или инсайдер его ожидает, то в большинстве случаев он проводит подготовку: создает пути доступа, неизвестные для организации, скрытые учетные записи и собирает пароли учетных записей коллег и групповых учетных записей	Увольнение инсайдера. Технические действия по подготовке к взлому
5	Как правило, организации не удается обнаружить технические индикаторы, предшествующие диверсионному акту	Получение информации организацией
6	Большинство инсайдеров совершают диверсионные акты в возрасте от 30-ти лет и являются опытными специалистами	Личные качества инсайдера
7	Ввиду отсутствия физических и электронных средств контроля и управления доступом инсайдеры, как правило, имеют полный доступ к критически важным данным и ИС	Получение информации организацией. Технические возможности инсайдера

С учетом выделенных особенностей схема взаимодействия элементов поведения ИТ-саботажника детализирована до уровня диаграммы причинно-следственных связей (ДПСС), представленной на рис. 2.

По результатам анализа ДПСС следующие параметры выделены в качестве уровней: желание инсайдера совершить диверсию; уровень недовольства; вероятность совершения диверсии; осведомленность организации; уровень обеспечения ИБ; доверие к сотруднику; уровень доступа сотрудника. ДП для ИТ-саботажа представлена на рис. 3.

Рис. 2. Диаграмма причинно-следственных связей ИТ-саботажа

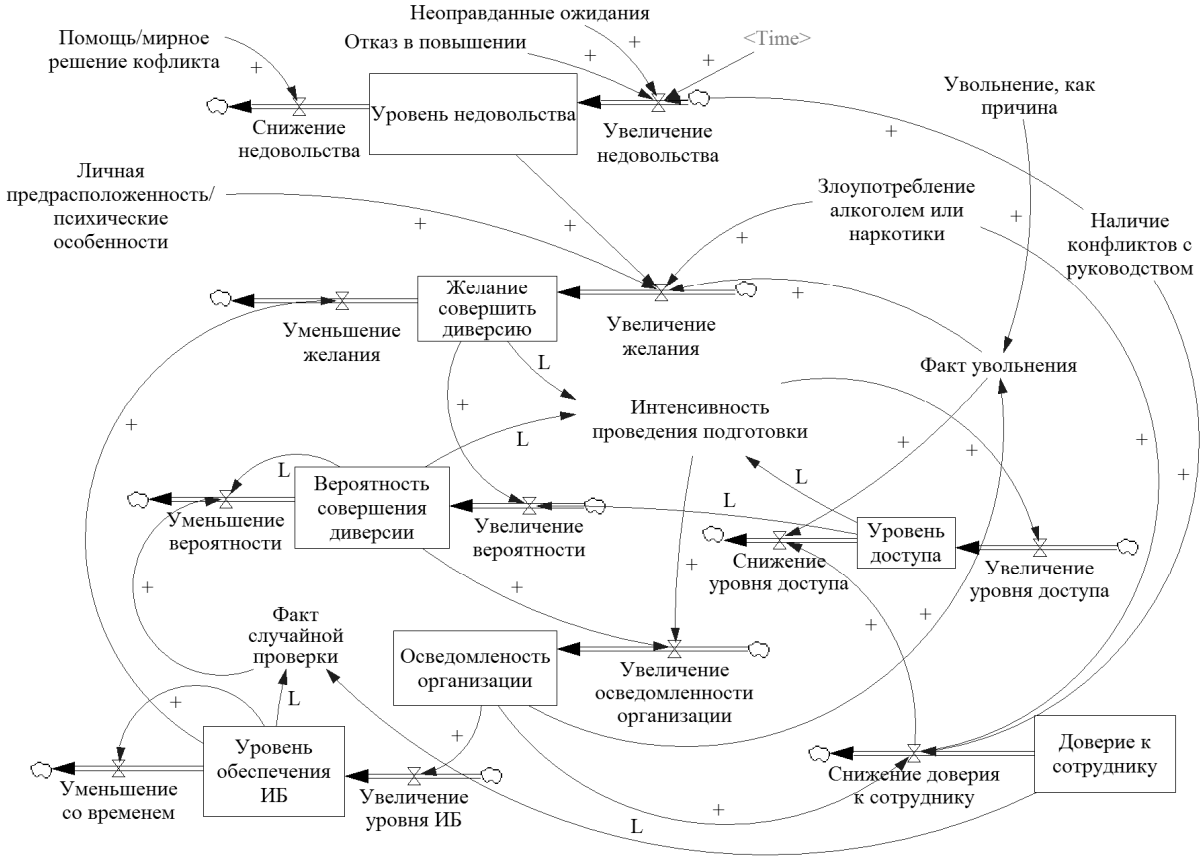

Рис. 3. ДП для ИТ-саботажа

Тестовое моделирование ИТ-саботажа

Проведено тестовое моделирование с получением визуальной информации о поведении внутреннего нарушителя ИБ для угрозы саботажа с использованием информационных систем организации.

В первом эксперименте (рис. 4) причиной диверсионного акта явился отказ в повышении, при этом низкий уровень обеспечения ИБ и достаточное доверие к сотруднику позволили инсайдеру повысить свои привилегии в ИС организации и совершить ИТ-саботаж. Впоследствии инсайдер был уволен.

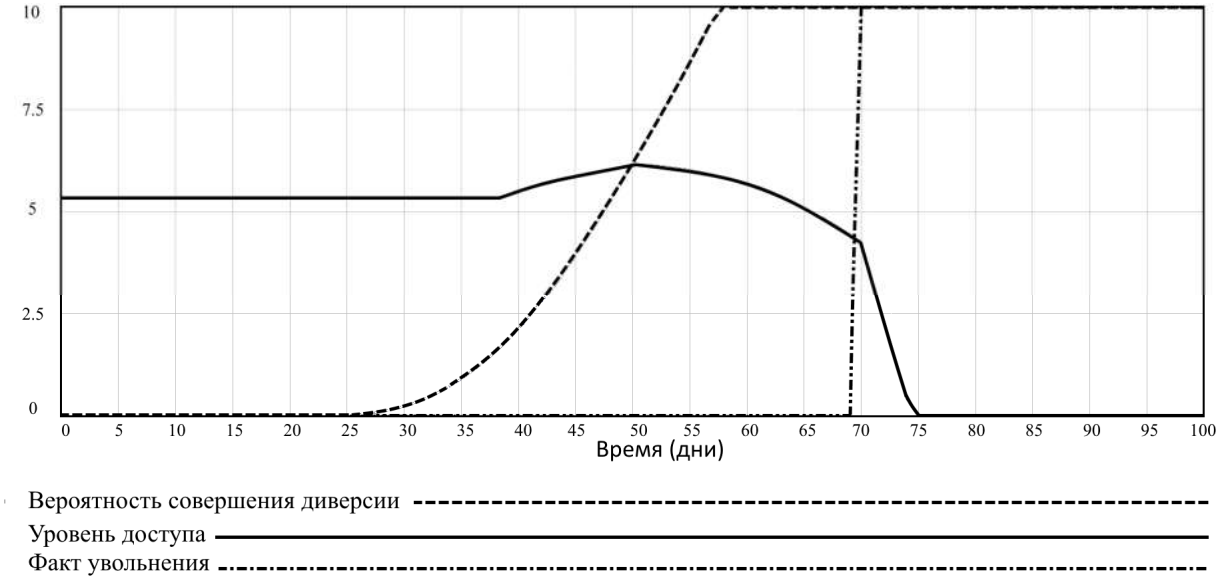

Рис. 4. «Классическое» развитие ИТ-саботажа

Во втором эксперименте (рис. 5) сотруднику также отказали в повышении, уровни доступа и доверия были достаточно высоки, но диверсионный акт не был совершен по причине высокого уровня обеспечения безопасности: регулярных проверок безопасности, обучения сотрудников и прочих мер, которые уменьшают желание сотрудников совершать противоправные действия.

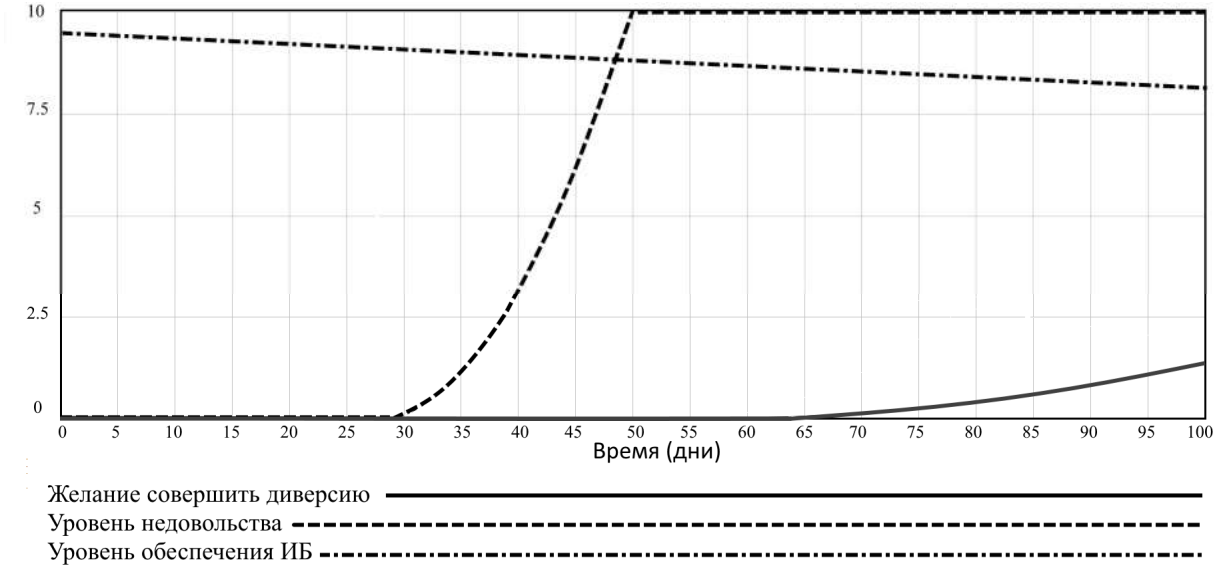

Рис. 5. Успешное купирование угрозы

В третьем эксперименте (рис. 6) изначальный уровень доступа и низкий уровень обеспечения ИБ позволяли сотруднику совершить диверсию, но из-за конфликтов с руководством уровень доверия и соответственно уровень доступа были понижены. Это явилось причиной проведения подготовки к саботажу, повышения уровня доступа и последующей реализации атаки.

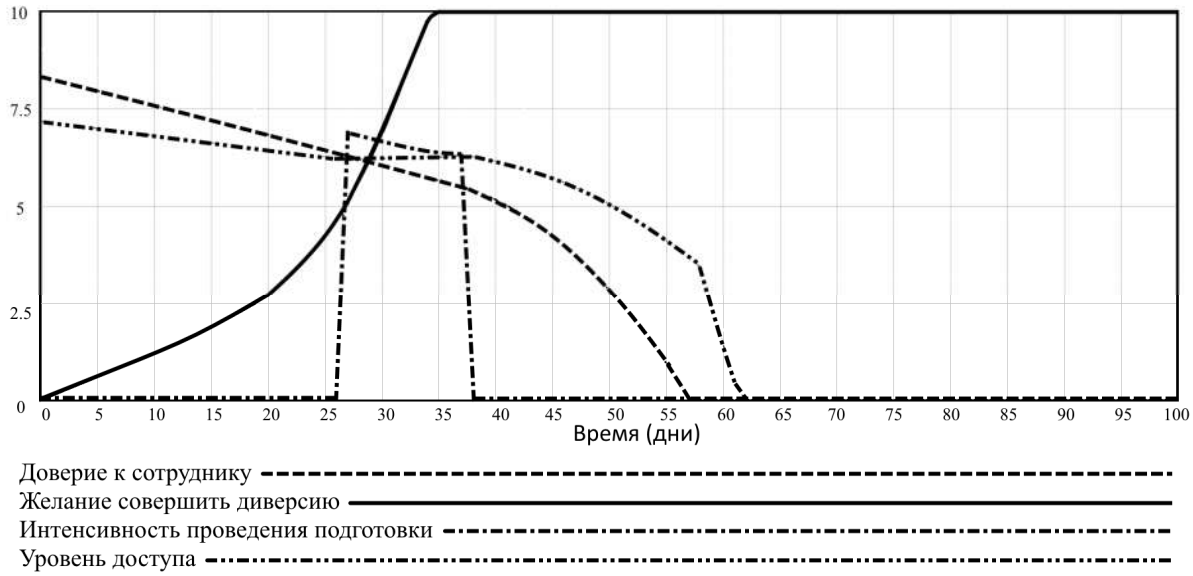

Рис. 6. ИТ-саботаж с подготовкой

Заключение

В статье проведено исследование угрозы саботажа с использованием информационных систем организации. На основании статистической информации и актуальных исследований разработаны: портрет ИТ-саботажника, основные особенности ИТ-саботажа, схема взаимодействия основных элементов системы поведения ИТ-саботажника, ДПСС и ДП. Проведено задание параметров модели и тестовая симуляция, подтверждающая корректность разработанной модели.

СПИСОК ЛИТЕРАТУРЫ:

1. PositiveTechnologies. Инциденты в информационной безопасности крупных российских компаний. 2014.[Электронный ресурс]URL: http://www.ptsecurity.ru/download/PT_Security_Incidents_2014_rus.pdf (дата обращения 05.12.2014).
2. Форрестер Дж. Основы кибернетики предприятия. М.: Прогресс, 1971.
3. Moore A., Cappelli D., Trzeciak R. The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures // Software Engineering Institute Carnegie Mellon University, CERT Program, 2008.
4. Band S., Cappelli D., Fischer L., Moore A., Shaw E., Trzeciak R. Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis // Software Engineering InstituteCarnegie Mellon University, CERT Program, 2006.

REFERENCES:

1. Positive Technologies, «Information security incidents in major Russian companies», 2014, URL: http://www.ptsecurity.ru/download/PT_Security_Incidents_2014_rus.pdf
2. Forrester J. Industrial Dynamics. M.: Progress, 1971.
3. Moore A., Cappelli D., Trzeciak R. The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures // Software Engineering Institute Carnegie Mellon University, CERT Program, 2008.
4. Band S., Cappelli D., Fischer L., Moore A., Shaw E., Trzeciak R. Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis // Software Engineering InstituteCarnegie Mellon University, CERT Program, 2006.