УДК 004.056

СОВЕРШЕНСТВОВАНИЕ ПОДСИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННОГО ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ НА ОСНОВЕ ВНЕДРЕНИЯ ГИС-ТЕХНОЛОГИЙ

Сазонов С. Ю., канд. техн. наук, доцент
«Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А. А. Леонова» – филиал федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии»
Королев, Российская Федерация

Аннотация. Инновационное развитие национальной экономики в современных социально-экономических условиях требует повышения уровня защищенности критически важных объектов территориально-распределенных промышленных производственных предприятий за счет внедрения современных аналитических инструментов, способных минимизировать риски и обеспечить устойчивость корпоративной информационной среды в условиях динамично развивающегося киберпространства.

Ключевые слова: информационная безопасность, корпоративная система информационной безопасности, геоинформационная система, пространственно-распределенное предприятие.

Современные промышленные предприятия являются ключевыми элементами инновационного развития и национальной безопасности России, что предъявляет повышенные требования к защите их информационных активов. Особую значимость приобретает обеспечение информационной безопасности (ИБ) в условиях возрастающего количества киберугроз, усложнения методов атак и ужесточения регуляторных требований.

Деятельность производственных предприятий связана с обработкой конфиденциальной и секретной информации, что делает ее потенциальной мишенью для кибератак, включая промышленный шпи-

онаж и диверсии. В связи с этим обеспечение информационной безопасности (ИБ) корпорации требует применения современных технологий, способных не только обнаруживать угрозы, но и прогнозировать их возникновение. Управление информационной безопасностью осуществляется на основе международного стандарта по обеспечению информационной безопасности ISO 17799:2000 «Информационные технологии – практические правила управления информационной безопасностью» [1].

В настоящее время корпоративные системы информационной безопасности сталкиваются с необходимостью внедрения инновационных технологий, позволяющих повысить эффективность управления рисками. Одним из перспективных направлений является использование геоинформационных систем (ГИС), которые обеспечивают пространственный анализ данных, визуализацию угроз и моделирование сценариев их развития. ГИС-технологии позволяют интегрировать разрозненные источники информации, выявлять закономерности в возникновении инцидентов ИБ и прогнозировать потенциально уязвимые направления атак.

Проведенный анализ выявил типовые проблемы в организации КСИБ территориально-распределенных предприятий, связанные с использованием устаревшего оборудования в промышленных сетях и отсутствием единого центра мониторинга для всех производственных площадок. Среднее время реакции на инциденты в филиалах превышает аналогичный показатель центрального узла в среднем на 35 %. Несмотря на соответствие базовым требованиям ФСТЭК и наличием многоуровневой системы криптозащиты, имеются серьезные недостатки. Наиболее критичными из них являются преобладание ручных процессов управления уязвимостями, отсутствие прогностических функций в SIEM-системе и фрагментарный подход к оценке рисков, не учитывающий взаимосвязи в промышленных системах управления технологическими процессами.

Геоинформационные системы (ГИС) применительно к задачам информационной безопасности опираются на комплекс фундаментальных принципов, которые кардинально меняют подход к анализу и прогнозированию киберугроз. Эти принципы формируют методологическую основу для преобразования традиционных систем защиты в пространственно-ориентированные интеллектуальные ком-

плексы. Применение геоинформационных систем в защите информации базируется на трех фундаментальных принципах:

1. Пространственная привязка данных - каждому событию информационной безопасности присваиваются географические координаты, позволяющие установить его связь с конкретным объектом инфраструктуры.

2. Многослойное представление информации – ГИС позволяет накладывать на цифровую карту различные слои данных: от физического расположения серверов до маршрутов передачи данных и зон ответственности подразделений.

3. Временная динамика – системы способны отображать изменение ситуации во времени, выявляя закономерности в возникновении инцидентов.

ГИС-системы используют сложный математический аппарат для обработки пространственных данных. Основу составляют:

– методы пространственной статистики (анализ горячих точек, ядерная оценка плотности);

– геостатистическое моделирование (кригинг, пространственная интерполяция);

– сетевой анализ (построение оптимальных маршрутов, анализ связности).

Для задач информационной безопасности особую ценность представляет пространственно-временной анализ, позволяющий выявлять закономерности в возникновении инцидентов. Например, модель пространственной автокорреляции Морана помогает обнаруживать кластеры кибератак, связанные с географическим положением объектов.

Архитектурное решение строится на принципах модульности, масштабируемости и глубокой интеграции с существующей инфраструктурой предприятий. Ядром новой архитектуры становится геоинформационный аналитический центр безопасности, который выполняет функции интегратора данных от всех компонентов системы защиты. Этот центр аккумулирует информацию от традиционных средств защиты (межсетевых экранов, систем обнаружения вторжений, антивирусных решений) и обогащает ее пространственными характеристиками. Особое внимание уделено обеспечению обработки данных в реальном времени с минимальной задержкой, что критически важно для оперативного реагирования на инциденты в условиях распределенной инфраструктуры предприятия (рис. 1).

Инновационным аспектом предлагаемой архитектуры является реализация пространственно-временного анализа событий информационной безопасности. Каждое событие, регистрируемое системами мониторинга, проходит этап геокодирования, в ходе которого определяется его принадлежность к конкретному объекту корпоративной инфраструктуры. Для этого разрабатывается цифровая модель территории предприятия с точным позиционированием всех элементов сети.

Рисунок 1 – Архитектура системы

Особую сложность представляет обработка данных от мобильных и временно подключаемых устройств. Решение этой задачи обеспечивается за счет гибридной системы позиционирования, сочетающей физические координаты оборудования с его логическим расположением в сетевой топологии. При этом учитываются такие параметры, как удаленность от центральных узлов, пропускная способность каналов связи и историческая частота инцидентов в конкретной локации.

Ядро аналитического модуля включает набор специализированных алгоритмов, адаптированных для задач информационной безопасности:

1. Пространственная кластеризация инцидентов (метод DBSCAN с географической метрикой).

2. Прогнозирование распространения угроз (модель на основе уравнений диффузии).

3. Анализ сетевых маршрутов (алгоритм A* с учетом факторов риска).

4. Выявление аномальной активности (LSTM-сети с пространственными признаками).

Эти алгоритмы реализованы в виде микросервисной архитектуры, что обеспечивает горизонтальную масштабируемость системы при росте нагрузки. Для обучения моделей могут использоваться исторические данные об инцидентах на предприятии, обогащенные внешними источниками информации о киберугрозах.

Интерактивный интерфейс системы предоставляет:

– 3D-карту объектов предприятия с наложением слоев угроз;

– динамические тепловые карты киберактивности;

– пространственно-временные линии развития инцидентов;

– инструменты для «что-если» анализа.

Разработанная методика предоставляет инструментарий для оптимизации процессов обнаружения и нейтрализации кибератак в распределенных сетевых инфраструктурах, характерных для крупных промышленных холдингов. Полученные результаты могут служить основой для создания типовых решений в области информационной безопасности, адаптируемых под специфику различных территориально-распределенных производственных предприятий. Реализация проекта открывает перспективы для сокращения операционных затрат на обеспечение информационной безопасности за счет автоматизации процессов анализа угроз и повышения точности прогнозирования инцидентов.

Список использованных источников

1. ISO 17799:2000. Информационные технологии – практические правила управления информационной безопасностью : международный стандарт. – М. : Стандартинформ, 2006. – 56 с.