Моделирование процессов обеспечения информационной безопасности промышленных экосистем с применением интеллектуальных алгоритмов

Е. С. Митяков[1], А. И. Ладынин[1], А. А. Вяткин[1], С. Н. Митяков[2]

[1]*МИРЭА – Российский технологический университет*

[2]*Нижегородский государственный технический университет им. Р.Е. Алексеева*

iyao@mail.ru, andrey.ladynin@hotmail.com, artem@vuatkin.ru

***Аннотация*. Исследование посвящено развитию модели управления инцидентами информационной безопасности в промышленных экосистемах с интеграцией методов искусственного интеллекта. Предложены формализованные соотношения для оценки и минимизации ущерба от киберинцидентов, где алгоритмы машинного обучения используются для прогнозирования критичности угроз и оптимизации распределения ресурсов реагирования. Проведен модельный эксперимент на синтетических данных, иллюстрирующий применение подхода к прикладным задачам с учетом специфики промышленных экосистем. Модель учитывает такие параметры, как время реакции, вероятность успешного устранения инцидента и стоимость мероприятий, позволяя повысить эффективность управления безопасностью за счет адаптивного анализа данных и интеллектуальной поддержки принятия решений.**

Ключевые слова: информационная безопасность, промышленная экосистема, защита информации

I. Введение

Актуальность темы исследования обусловлена стремительным развитием промышленных экосистем, которые становятся все более зависимыми от информационных систем и сетевых технологий, что делает их уязвимыми перед киберугрозами. Растущее число и сложность кибератак на промышленные предприятия, включая промышленный шпионаж, диверсии усугубляют ситуацию. Кроме того, внедрение новых технологий, таких как Интернет вещей и промышленные роботы, открывая новые возможности, одновременно порождает новые риски для информационной безопасности.

Увеличение объема и ужесточение законодательных актов, а также стандартов, регулирующих информационную безопасность в промышленности, подчеркивают значимость данной проблемы. Моделирование процессов информационной безопасности способствует выявлению уязвимостей и рисков внутри экосистемы, разработке и внедрению эффективных механизмов защиты от киберугроз, совершенствованию управления информационной безопасностью и обеспечению соответствия нормативным требованиям. Целью настоящего исследования является разработка модели оценки и минимизации ущерба информационной безопасности в промышленных экосистемах, учитывающей как внутренние процессы предприятий, так и межорганизационные взаимодействия для эффективного управления инцидентами информационной безопасности.

II. Проблемы моделирования процессов информационной безопасности

Моделирование процессов информационной безопасности играет ключевую роль в их понимании, проектировании и управлении. В научной литературе можно найти различные подходы к данному типу моделирования. В одном из исследований показано, что системы информационной безопасности должны быть интегрированными и иерархическими, что обеспечивает как горизонтальную, так и вертикальную интеграцию внутренней и внешней информации [1]. Такой подход поддерживает проведение комплексных аудитов наряду с визуальным моделированием информационных потоков и участников. В другой статье рассматривается имитационное моделирование с использованием специализированных инструментов, таких как GNS3 и Kali Linux, для изучения динамики систем информационной безопасности [2]. Данный метод позволяет оценивать пропускную способность сети, выявлять уязвимости и эффективно планировать меры по обеспечению информационной безопасности. В еще одном исследовании предлагается формализм гибридных автоматов как инструмент для анализа конфликтов между информационными системами и угрозами безопасности [3]. Этот подход помогает понять распространение деструктивных информационных процессов и изменения состояний компонентов системы.

В научном дискурсе представлена концептуальная модель принятия инвестиционных решений в сфере информационной безопасности [4]. В другом исследовании рассматривается моделирование угроз в географически распределенных информационных системах с применением методов машинного обучения и нечетких нейронных сетей [5]. Этот подход помогает выявлять реальные угрозы и минимизировать финансовые затраты. Еще одна работа обсуждает метод многоперспективного моделирования, объединяющего технологические, бизнес-организационные и стратегические аспекты для проектирования и управления системами информационной безопасности [6]. В работе [7] исследуют моделирование защищенных

бизнес-процессов, которое предполагает связывание социальных субъектов с их обязанностями и обязательствами с использованием концепций транзакций DEMO и метода анализа норм для интеграции мер безопасности в модели бизнес-процессов.

Статья [8] подчеркивает, что модели оценки рисков информационной безопасности должны учитывать распространение уязвимостей и эволюцию бизнес-процессов для повышения общей эффективности [8]. Хауфе К. с соавторами описывают структуру процесса системы менеджмента информационной безопасности, основанную на таких стандартах, как ISO 27000, COBIT и ITIL [9]. Такой подход помогает системно управлять информационной безопасностью организации и повышать ее эффективность. Векслер В. с соавторами рассматривают когнитивные модели злоумышленников, защитников и пользователей, которые могут значительно улучшить средства и модели кибербезопасности за счет учета человеческого фактора и прогнозирования поведения атакующего [10].

III. Проблемы моделирования процессов информационной безопасности

Модель информационной безопасности для промышленных экосистем предназначена для управления инцидентами в условиях взаимодействия множества предприятий, функционирующих в рамках единой экосистемы. Она учитывает как внутренние процессы каждого предприятия, так и межорганизационные взаимодействия, обмен данными и координацию действий. Выделим следующие ключевые компоненты модели:

Множество инцидентов информационной безопасности, $I_k = \{I_{k1}, I_{k2}, \dots, I_{kn}\}$, , где I_{ki} представляет собой инцидент информационной безопасности на k-м предприятии. Каждый инцидент характеризуется такими параметрами, как время обнаружения, критичность, вероятность реализации угрозы и другие факторы. Необходимо учитывать как локальные инциденты, так и инциденты, возникающие вследствие взаимодействия между предприятиями. Общее множество инцидентов в экосистеме обозначается следующим образом:

$$I = \bigcup_{k=1}^{K} I_k,$$

где K – общее количество предприятий в экосистеме.

A. Множество действий по управлению инцидентами.

$\{A_{k1}, A_{k2}, \dots, A_{km}\}$ – множество действий, направленных на устранение инцидентов на k-м предприятии. Помимо внутренних действий, вводится множество совместных действий между предприятиями для координации усилий и обеспечения безопасности всей экосистемы, обозначаемое как A_{ext}. Общее количество действий выражается следующим образом:

$$A = \bigcup_{k=1}^{K} A_k \cup A_{ext}.$$

Время реагирования на инцидент $T(I_{ki})$ обозначает время реагирования на инцидент I_{ki} для k-го предприятия. В рамках экосистемы целесообразно учитывать дополнительное время, необходимое для координации действий между предприятиями:

$$T_{ecosystem}(I_{ki}) = T(I_{ki}) + T_{coord}(k, j),$$

где $T_{coord}(k, j)$ – дополнительное время, затрачиваемое на координацию между предприятиями k и j.

B. Функция ущерба от инцидента

$D(I_{ki})$ – функция, оценивающая потери k-го предприятия в результате инцидента. В рамках экосистемы также необходимо учитывать потенциальные потери, которые могут возникнуть на других предприятиях вследствие взаимодействий:

$$D_{\text{ecosystem}}(I_{ki}) = D(I_{ki}) + \sum_{j \neq k} D_{\text{interaction}}(I_{ki}, I_j),$$

где $D_{\text{interaction}}(I_{ki}, I_j)$ – потенциальный ущерб, причиняемый k-м предприятием предприятию с индексом j.

C. Функция вероятности устранения инцидента

$P(A_{kj}, I_{kj})$ вероятность успешного устранения инцидента I_{kj} предприятием k с помощью действия A_{kj}. Данная вероятность зависит не только от действий внутри отдельного предприятия, но и от уровня координации.

$$P_{\text{ecosystem}}(A_{kj}, I_{ki}) = P(A_{kj}, I_{ki}) \times P_{coord}(A_{kj}, A_{ext}),$$

где $P_{coord}(A_{kj}, A_{ext})$ – вероятность успешной координации.

D. Затраты на минимизацию последствий инцидента.

$C(A_{kj}, I_{ki})$ – затраты на устранение инцидента для k-го предприятия. В данном случае экосистема учитывает не только внутренние затраты, но и дополнительные ресурсы, необходимые для координации между предприятиями:

$$\mathrm{C}_{\text{ecosystem}}(A_{kj}, I_{ki}) = \mathrm{C}(A_{kj}, I_{ki}) - \sum_{j \neq k} C_{coord}(A_{kj}, A_j),$$

где $C_{coord}(A_{kj}, A_j)$ – затраты на координацию действий между k-м и j-м предприятиями.

$$Z = \sum_{k=1}^{K} \sum_{j=1}^{m_k} \sum_{i=1}^{n_k} \Big[D_{\text{ecosystem}}(I_{ki}) \cdot \big(1 - P_{\text{ecosystem}}(A_{kj}, I_{ki})\big) + \mathrm{C}_{\text{ecosystem}}(A_{kj}, I_{ki}) \Big],$$

где Z – совокупный ущерб и затраты на реализацию мер реагирования для всех инцидентов в экосистеме, n_k – количество инцидентов на k-м предприятии, m_k – количество мер, направленных на устранение инцидентов на k-м предприятии, C_{coord} – дополнительные затраты на координацию. Модель содержит следующие ограничения:

1. Время реагирования на инциденты не должно превышать установленного максимального значения:

$$T_{ecosystem}(I_{ki}) = T_{max}, I_{ki} \in I.$$

2. Затраты на реагирование на инциденты не должны превышать доступных ресурсов экосистемы:

$$\sum_{k=1}^{K}\sum_{j=1}^{m_k}\sum_{i=1}^{n_k} \mathrm{C}_{\text{ecosystem}}\left(A_{kj}, I_{ki}\right) \le R.$$

Вероятность устранения инцидентов должна быть выше установленного минимального порога:

$$P_{\text{ecosystem}}\left(A_{kj}, I_{ki}\right) \ge P_{min}.$$

Предложенная модель может быть представлена в графическом виде, что позволяет лучше структурировать и объединить все необходимые этапы (рис. 1).

Целевая функция направлена на минимизацию суммарного ущерба и затрат для всех межорганизационных взаимодействий:

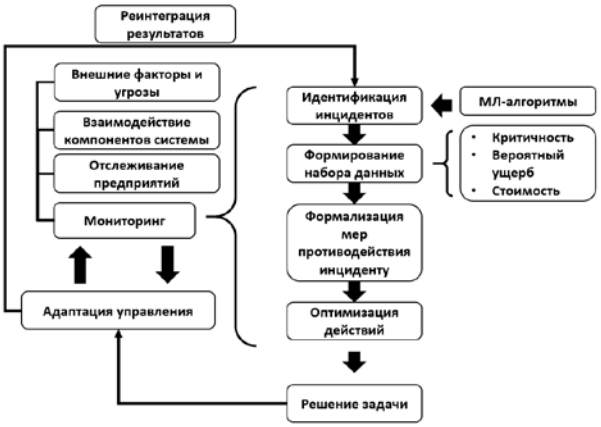

Рис. 1. Модель обеспечения информационной безопасности

Пошаговую процедуру реализации предложенного подхода можно описать следующим образом:

1. Обнаружение инцидентов на предприятиях экосистемы.
2. Сбор данных об инцидентах, включая их критичность, возможный ущерб и затраты на устранение.
3. Оценка вероятности успешного устранения инцидентов с учетом координации между предприятиями.
4. Минимизация ущерба и затрат в масштабах всей экосистемы.
5. Мониторинг реализации мер и корректировка стратегии.

Вышеуказанная процедура может быть модифицирована в соответствии с конкретной ситуацией и условиями, в которых находится экосистема. Методика оптимиции была протестирована на синтетических данных, иллюстрирующих процедуру, ограничения модели и возможные результаты.

Методы интеграции искусственного интеллекта существенно повышают адаптивность предложенной модели информационной безопасности. Алгоритмы машинного обучения, позволяют динамически оценивать критичность инцидентов посредством анализа исторических данных о кибератаках, потоков данных об угрозах и телеметрии в реальном времени от промышленных систем управления. Это обеспечивает проактивное установление приоритетов инцидентов на основе прогнозируемого воздействия, а не статических пороговых значений, сокращая задержку реагирования и повышая эффективность распределения ресурсов. Кроме того, методы обучения с подкреплением могут оптимизировать выбор мер реагирования путем обучения на результатах прошлых инцидентов, непрерывно уточняя функцию вероятности за счет взаимодействия со средой экосистемы. Глубокие нейронные сети и модели прогнозирования временных рядов предоставляют расширенные возможности для прогнозирования распространения потенциального ущерба между взаимосвязанными предприятиями. Усовершенствование с помощью ИИ также может обеспечивать адаптивное управление ограничениями. Это преобразует модель из статического инструмента оптимизации в самоадаптирующуюся систему поддержки принятия решений, способную находить баланс между безопасностью, затратами и операционной непрерывностью в условиях неопределенности.

IV. Верификация модели

Рассмотрим тестирование предложенной модели на синтетических данных для промышленных экосистем, в которых несколько предприятий взаимодействуют и совместно реагируют на инциденты информационной безопасности. Предполагается, что экосистема включает два предприятия E_1 и E_2, каждое из которых сталкивается с инцидентами, оказывающими влияние на всю экосистему. Пусть в ходе анализа экосистемы выявлены инциденты, представленные в табл. 1.

ТАБЛИЦА I. Данные синтетических тестов

Инциденты	**Ожидаемые потери, у.е.**	**Время реакции**	**Критичность**	**Предприятие**
Утечка данных клиентской базы	200 000	2	Высокая	$\boldsymbol{E_1}$
Вирусная атака на серверы	100 000	5	Средняя	$\boldsymbol{E_2}$
Несанкционированный доступ к сети	50 000	1	Низкая	$\boldsymbol{E_1}$
Отказ систем управления	150 000	3	Высокая	E_2

Предположим, что существуют следующие ограничения:

- общий бюджет на устранение инцидентов не превышает R=60 000 условных единиц;
- максимальное время реагирования на все инциденты составляет 8 часов.

Пусть для каждого инцидента имеется несколько возможных мер реагирования с различными затратами, вероятностью устранения и временем выполнения (табл. 2).

ТАБЛИЦА II. Возможные меры по устранению инцидентов

Инцидент	**Действие**	**Затраты (C), у.е.**	**Вероятность успеха (P)**
Утечка данных (I_{11})	Отключение внешних соединений ($\boldsymbol{A_{11}}$)	15 000	0.7
	Уведомление клиентов и устранение уязвимости ($\boldsymbol{A_{12}}$)	25 000	0.9
Вирусная атака(I_{21})	Перезагрузка серверов и запуск антивируса ($\boldsymbol{A_{21}}$)	10 000	0.8
	Замена оборудования и	20 000	0.95

Инцидент	Действие	Затраты (C), у.е.	Вероятность успеха (P)
	восстановление данных ($\boldsymbol{A_{22}}$)		
Несанкционированный доступ (I_{12})	Завершение сеанса нарушителя ($\boldsymbol{A_{13}}$)	5 000	0.6
	Сетевой аудит и корректировка конфигурации ($\boldsymbol{A_{14}}$)	8 000	0.85
Отказ систем управления (I_{22})	Перезагрузка систем (A_{23})	12 000	0.75
	Диагностика и устранение неисправностей (A_{24})	18 000	0.9

Для минимизации ущерба и затрат целесообразно выбирать оптимальные меры реагирования для каждого инцидента с учетом временных и бюджетных ограничений. Для инцидента I_{21} мера A_{21} стоит 10 000 у.е. при вероятности успеха 0,8. Поскольку данная мера вписывается в бюджет и имеет приемлемую вероятность успеха, выбираем A_{21}. Для инцидента I_{12}: мера A_{13} является наиболее дешевой, однако ее вероятность успеха составляет лишь 0,6. Учитывая невысокую критичность инцидента, выбираем меру A_{13}. Для инцидента I_{22}: мера A_{23} дешевле (стоит всего 12 000 у.е.) при вероятности успеха 0,75. Выбираем данную меру, поскольку она укладывается в бюджетные ограничения.

Подставляя данные в целевую функцию, получаем результирующие затраты, которые обозначаются следующим образом: $Z = (200.000 \cdot (1 - 0{,}9) + 25.000) + (50.000 \cdot (1 - 0{,}6) + 5.000) + (100.000 \cdot (1 - 0{,}8) + 10.000) + (150.000 \cdot (1 - 0{,}75) + 12.000) = 149.500$.

Таким образом, при расчете на синтетических данных целевая функция ZZ, отражающая совокупные потери экосистемы и затраты на ликвидацию инцидентов, составила 149 500 у.е. При этом были учтены параметры инцидентов, вероятности успешного устранения и затраты.

V. Заключение

В статье предложен подход к решению задач оценки и минимизации ущерба информационной безопасности с учетом специфики промышленных экосистем. Несмотря на то, что модель была протестирована на синтетических данных, ее принципы и механизмы могут быть успешно применены на практике. Это объясняется тем, что многие аспекты, такие как взаимодействие между предприятиями, управление инцидентами и оценка рисков, остаются релевантными независимо от конкретных характеристик данных. Однако следует отметить, что получение реальных данных о киберинцидентах и причиненном ими ущербе представляет собой сложную задачу. Это обусловлено прежде всего нежеланием предприятий экосистемы делиться конфиденциальной информацией, а также постоянной изменчивостью угроз кибербезопасности. Таким образом, дальнейшие исследования должны быть сосредоточены на адаптации и настройке модели.

Список литературы

[1] Kryvoruchko O., Desiatko A., & Synichuk O. (2020). Modeling of the information system of information security independent audit. Management of Development of Complex Systems. https://doi.org/10.32347/2412-9933.2020.43.67-75.

[2] Korniyenko B., & Galata L. (2019). Modeling of information security system in computer network. Information systems and technologies security. https://doi.org/10.17721/ists.2019.1.36-41

[3] Goncharov N., Goncharov I., Parinov P., Dushkin A., & Maximova M. (2019). Modeling of Information Processes for Modern Information System Security Assessment. 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 1758-1763. https://doi.org/10.1109/EICONRUS.2019.8656828.

[4] Dor D., & Elovici Y. (2016). A model of the information security investment decision-making process. Comput. Secur., 63, 1-13. https://doi.org/10.1016/j.cose.2016.09.006.

[5] Minyaev A. (2021). Modeling information security threats in territorial-distributed information systems. H&ES Research. https://doi.org/10.36724/2409-5419-2021-13-2-52-65.

[6] Goldstein A., & Frank U. (2016). Components of a multi-perspective modeling method for designing and managing IT security systems. Information Systems and e-Business Management, 14, 101-140. https://doi.org/10.1007/S10257-015-0276-5.

[7] Barjis J. (2009). Information Systems Security based on Business Process Modeling. , 213-218. https://doi.org/10.5220/0002006502130218.

[8] Hariyanti E., Djunaidy A., & Siahaan D. (2018). A Conceptual Model for Information Security Risk Considering Business Process Perspective. 2018 4th International Conference on Science and Technology (ICST), 1, 1-6. https://doi.org/10.1109/ICSTC.2018.8528678.

[9] Haufe K., Colomo-Palacios R., Dzombeta S., Brandis K., & Stantchev V. (2022). A process framework for information security management. International Journal of Information Systems and Project Management. https://doi.org/10.12821/IJISPM040402.

[10] Veksler V., Buchler N., Hoffman B., Cassenti D., Sample C., & Sugrim S. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00691.