использованием LLL-решателя. Современные системы работают с рюкзаками высокой плотности — их применимость на настоящий момент под вопросом. Наконец, гибридные шифрсистемы наиболее эффективно противостоят всем известным атакам, но оказываются более медленными.

СПИСОК ЛИТЕРАТУРЫ:

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2013. — 816 с.
2. *Kate A., Goldberg I.* Generalizing cryptosystems based on the subset sum problem // International Journal of Information Security. 2011. Т. 10. № 3. Р. 189–199.
3. *Okamoto T.* Quantum Public-Key Cryptosystems Lecture Notes in Computer Science / Ed. M. Bellare. Springer Berlin Heidelberg, 2000. Р. 147–165.
4. *Murakami Y., Nasako T.* Knapsack Public-Key Cryptosystem Using Chinese Remainder Theorem // IACR Cryptology ePrint Archive. 2007. — 12 p.
5. *Schnorr C.-P.* Attacking the Chor-Rivest cryptosystem by improved lattice reduction. Springer, 1995. Р. 1–12.
6. *Rastaghi R.* Cryptanalysis and Improvement of Akleylek et al.'s cryptosystem. 2013.
7. *Kasahara M.* Construction of New Classes of Knapsack Type Public Key Cryptosystem Using Uniform Secret Sequence, K (II) ΣП PKC, Constructed Based on Maximum Length Code // IACR Cryptology ePrint Archive. 2012. — 8 p.
8. *Pan Y., Deng Y., Jiang Y., Tu Z.* A New Lattice-Based Cryptosystem Mixed with a Knapsack // IACR Cryptology ePrint Archive. 2009. — 12 p.

REFERENCES:

1. *Schneier B.* Applied cryptography. Protocols, Algorithms, and Source Code in C. John Wiley & Sons. Inc., 2013. — 816 p.
2. *Kate A., Goldberg I.* Generalizing cryptosystems based on the subset sum problem // International Journal of Information Security. 2011. Т. 10. № 3. Р. 189–199.
3. *Okamoto T.* Quantum Public-Key Cryptosystems Lecture Notes in Computer Science / / Ed. M. Bellare. Springer Berlin Heidelberg, 2000. Р. 147–165.
4. *Murakami Y., Nasako T.* Knapsack Public-Key Cryptosystem Using Chinese Remainder Theorem // IACR Cryptology ePrint Archive. 2007. — 12 p.
5. *Schnorr C.-P.* Attacking the Chor-Rivest cryptosystem by improved lattice reduction. Springer, 1995. Р. 1–12.
6. *Rastaghi R.* Cryptanalysis and Improvement of Akleylek et al.'s cryptosystem. 2013.
7. *Kasahara M.* Construction of New Classes of Knapsack Type Public Key Cryptosystem Using Uniform Secret Sequence, K (II) ΣП PKC, Constructed Based on Maximum Length Code // IACR Cryptology ePrint Archive. 2012. — 8 p.
8. *Pan Y., Deng Y., Jiang Y., Tu Z.* A New Lattice-Based Cryptosystem Mixed with a Knapsack // IACR Cryptology ePrint Archive. 2009. — 12 p.

V. S. Makeev, A. S. Zaytsev

Research of IT-sabotage Problem

Key words: IT-sabotage, insider, fishbone diagram

This article presents a research of the threat of IT-sabotage with the use of information resources of an organization. Based on statistical information and relevant research, a scheme and a fishbone diagram of insider were designed here.

В. С. Макеев, А. С. Зайцев

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ИТ-САБОТАЖА

До сих пор основным направлением исследований в области обеспечения ИБ было противодействие внешним угрозам, в то время как защита и предотвращение внутренних угроз оставались на втором плане. Однако, по данным исследования компании Positive Technologies [1] в 2013 г., внутренние угрозы, такие как нарушение правил безопасности и злонамеренные действия сотрудников, зачастую оказываются более опасны, чем вирусы и внешние атаки.

Особенностью ИТ-саботажа является то, что данные инциденты достаточно трудно предотвратить ввиду сложности отслеживания подготовки диверсионного акта, в особенности при его импульсивном характере.

Задачей данного исследования является разработка диаграммы причинно-следственных связей поведения ИТ-саботажника для лучшего понимания угрозы и дальнейшей разработки прогнозной модели.

В рамках исследования на основе сведений из открытых источников сформирована база инцидентов с участием внутренних нарушителей ИБ, состоящая из более чем 100 случаев, в том числе 20 случаев ИТ-саботажа. На основании данной статистики и актуальных исследований [2, 3] определены особенности поведения ИТ-саботажника, в виде схемы представленные на рисунке 1.

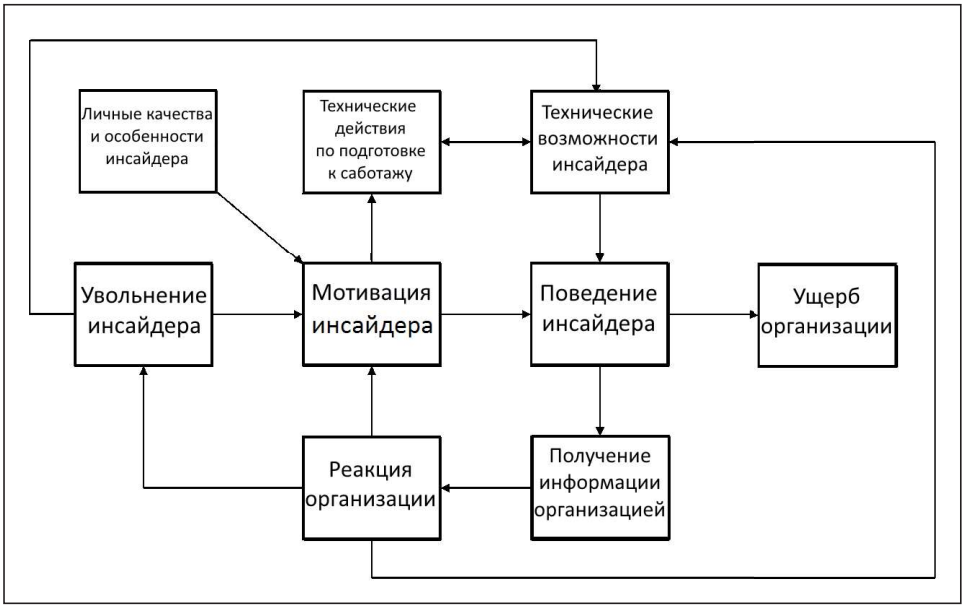

Рис. 1. Схема поведения ИТ-саботажника

Данная схема детализирована до диаграммы причинно-следственных связей (ДПСС), изображенной на рис. 2.

В рамках дальнейших исследований необходимо произвести преобразование данной диаграммы в полноценную прогнозную модель и разработать методы уточнения модели на основе статистической информации.

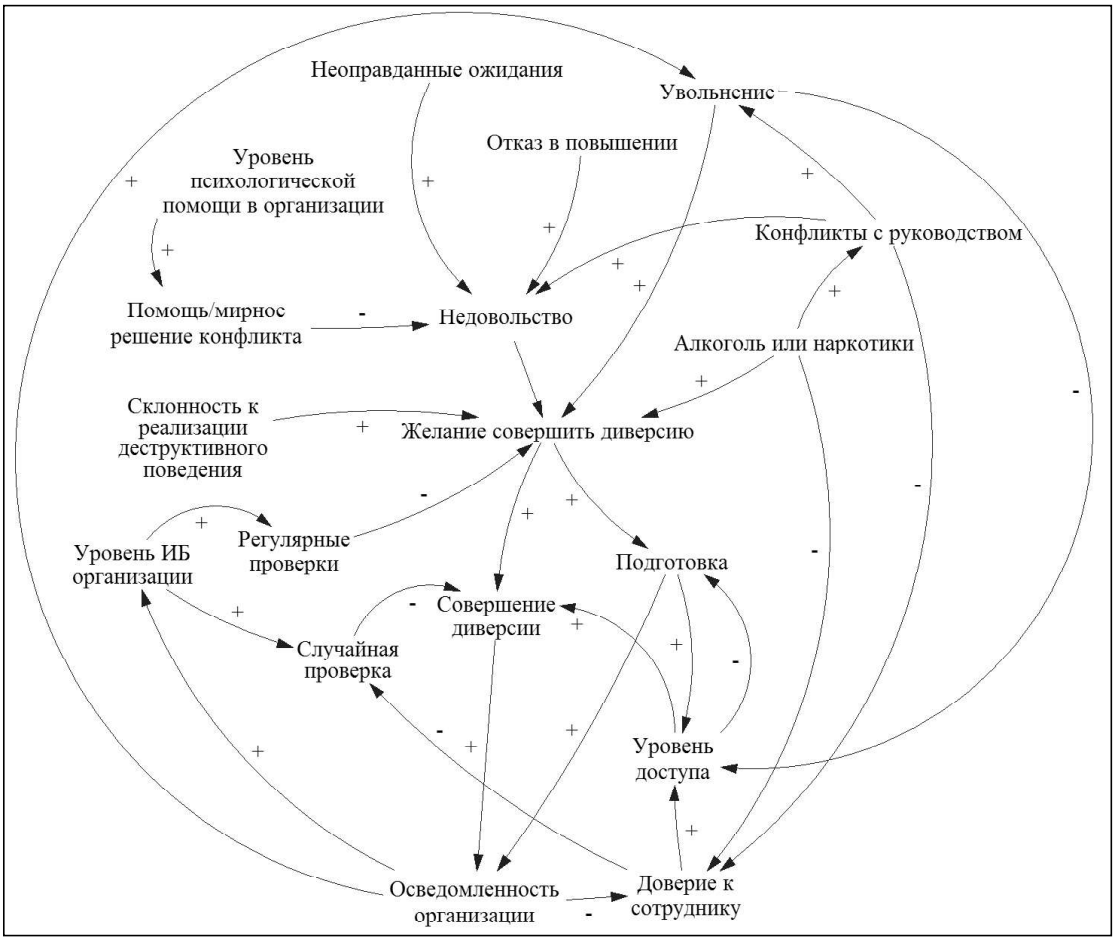

Рис. 2. Диаграмма причинно-следственных связей ИТ-саботажа

СПИСОК ЛИТЕРАТУРЫ:

1. Positive Technologies. Инциденты в информационной безопасности крупных российских компаний. 2014. URL: http://www.ptsecurity.ru/download/PT_Security_Incidents_2014_rus.pdf (дата обращения: 05.12.2014).
2. *Silowash G., Cappelli D., Moore A., Trzeciak R., Shimeall T. J., Flynn L.* Common Sense Guide to Mitigating Insider Treats. 4th Edition. Software Engineering Institute. CERT Program. 2012.
3. *Moore A. P., Cappelli D., Trzeciak R. F.* The "Big Picture" of Insider IT Sabotage Across U. S. Critical Infrastructures. 2008. URL: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2008_005_001_14981.pdf (дата обращения: 05.12.2014).

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. *Silowash G., Cappelli D., Moore A., Trzeciak R., Shimeall T. J., Flynn L.* Common Sense Guide to Mitigating Insider Treats. 4th Edition. Software Engineering Institute. CERT Program. 2012.
3. *Moore A. P., Cappelli D., Trzeciak R. F.* The "Big Picture" of Insider IT Sabotage Across U. S. Critical Infrastructures. 2008. URL: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2008_005_001_14981.pdf.