СПИСОК ЛИТЕРАТУРЫ:

1. *Giordano J., Maciag C.* Cyber Forensics: A Military Operations Perspective // International Journal of Digital Evidence. 2002. V. 1. I. 2. P. 1–13.
2. *Jozwiak I., Kedziora M., Melinska A.* Theoretical and Practical Aspects of Encrypted Containers Detection – Digital Forensics Approach // Dependable Computer Systems. 2011. P. 75–85.
3. *Weston P., Wolthusen S.* Forensic Entropy Analysis of Microsoft Windows Storage Volume // Information Security for South Africa. 2013. P. 1–7.
4. Digital Forensics File Carving Advances [Электронный ресурс]: KoreLogic DFRWS-2006 Project. 2006. URL: http://www.korelogic.com/Resources/Projects/dfrws_challenge_2006/DFRWS_2006_File_Carving_Challenge.pdf.

REFERENCES:

1. *Giordano J., Maciag C.* Cyber Forensics: A Military Operations Perspective // International Journal of Digital Evidence. 2002. V. 1. I. 2. P. 1–13.
2. *Jozwiak I., Kedziora M., Melinska A.* Theoretical and Practical Aspects of Encrypted Containers Detection – Digital Forensics Approach // Dependable Computer Systems. 2011. P. 75–85.
3. *Weston P., Wolthusen S.* Forensic Entropy Analysis of Microsoft Windows Storage Volume // Information Security for South Africa. 2013. P. 1–7.
4. Digital Forensics File Carving Advances: KoreLogic DFRWS-2006 Project. 2006. URL: http://www.korelogic.com/Resources/Projects/dfrws_challenge_2006/DFRWS_2006_File_Carving_Challenge.pdf.

A. P. Mikhalkova, A. S. Zaytsev

The Baysean Approach Appliance for Early Detection of Insider Threat

Key words: insider, Bayesian network

Purpose of report is to increase the information security level of an organization from insider threats. The report presents the method of detection and determination of the type of supposed insider threat with the help of the Bayesian approach.

А. П. Михалькова, А. С. Зайцев

О ПРИМЕНЕНИИ БАЙЕСОВСКОГО ПОДХОДА ДЛЯ РАННЕГО ОБНАРУЖЕНИЯ ВНУТРЕННИХ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время существует множество исследований, посвященных противодействию внешним угрозам ИБ, разработаны полноценные методологии и специализированное программное обеспечение. Вопрос противодействия внутренним угрозам ИБ проработан не настолько хорошо, но в то же время 77,6 % руководителей ИТ и ИБ заявляют, что основная опасность для организаций связана с внутренними угрозами, а именно с утечкой информации ограниченного доступа, нелояльным или преступным поведением сотрудников и пр. [1]. Основа успешного противодействия инсайдеру – его раннее выявление. Ввиду этого крайне актуальной задачей является разработка эффективного метода обнаружения внутренних нарушителей на раннем этапе реализации угрозы ИБ.

В качестве математической основы для выявления внутренних угроз ИБ целесообразно использовать статические модели, такие как нечеткие нейронные сети, регрессионный анализ и сети Байеса [2, 10]. В работе [2] обоснован выбор байесовских сетей доверия как наиболее эффективного метода раннего обнаружения внутренних угроз, разработана соответствующая сеть Байеса и проведено экспериментальное моделирование. В исследованиях отмечены существенные недостатки, которые снижают точность полученных моделей: использование только поведенческих индикаторов, применение сети Байеса без режима обучения, что ставит корректность модели в зависимость от квалификации эксперта, осуществляющего задание параметров сети.

В данной работе разработан собственный метод обнаружения внутренних нарушителей ИБ, основанный на байесовском подходе и учитывающий достоинства и недостатки существующих исследований. На основе информации, доступной в открытых источниках, сформирована база из более чем 100 инцидентов, произошедших по вине внутренних нарушителей ИБ. В результате анализа базы в части проявленных индикаторов выделено 5 основных классов внутренних угроз ИБ:

- ИТ-саботаж;
- кража интеллектуальной собственности;
- мошенничество на неруководящей должности;
- мошенничество на руководящей должности;
- ИТ-шпионаж.

Для каждого класса внутренних угроз в соответствии со статистической информацией и исследованиями [2, 4, 5, 6] выделен характерный набор технических и поведенческих индикаторов. Например, для мошенничества на руководящей должности характерны следующие индикаторы:

• *поведенческие:*

1) финансовые проблемы (BI1);
2) неожиданный доход (BI2);
3) состояние стресса без видимых на то причин (BI3);

• *технические:*

1) подозрительные транзакции (TI1);
2) мошеннические операции (TI2);
3) финансовое несоответствие (TI3);
4) фальсификация документов (TI4).

Для определения вероятности принадлежности сотрудника к тому или иному классу внутренних нарушителей для каждого класса реализована обучаемая сеть Байеса, применение которой позволяет производить:

- обучение в процессе работы;
- работу с заведомо неточными и неполными данными [7].

Байесовская сеть представляет собой направленный ациклический граф, каждой вершине которого соответствует случайная переменная. Если узлы (переменные) не соединены дугами, то их считают условно независимыми [8]. Сеть Байеса для мошенничества на руководящей должности изображена на рис. 1.

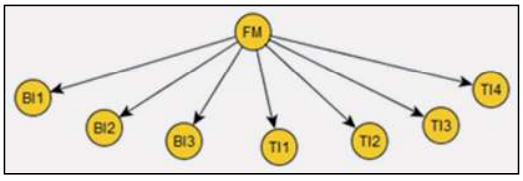

Рис. 1. Сеть Байеса для угрозы мошенничества на руководящей должности

Вершине FM соответствует значение вероятности реализации угрозы конкретным сотрудником, вершинам BI1—BI3 — значения вероятностей поведенческих индикаторов, вершинам TI1—TI4 — значения вероятностей технических индикаторов. Поскольку индикаторы не соединены дугами между собой, они условно независимы друг от друга. Каждый индикатор зависит только от выбранной модели поведения. Априорные вероятности для сетей были получены с использованием существующих работ [2] и статистики исследуемых случаев. Входами каждой сети являются индикаторы, проявляемые потенциальным внутренним нарушителем ИБ. Выходом каждой сети является вероятность принадлежности сотрудника к конкретному классу внутренних нарушителей ИБ.

Обучение сети происходит на основе 100 инцидентов с помощью EM-алгоритма. EM-алгоритм — алгоритм, используемый для нахождения оценок максимального правдоподобия параметров вероятностных моделей в случае, когда некоторые переменные не наблюдались [9]. EM-алгоритм находит наиболее вероятную гипотезу h (параметр модели), которая максимизирует $E[ln(p(FM\,|h)]$ — математическое ожидание логарифмической функции правдоподобия. После нахождения всех неизвестных параметров модели в процессе обучения сеть изменяет собственную таблицу условных вероятностей. Таким образом, чем больше инцидентов мы исследуем, тем точнее сеть сможет определять внутреннего нарушителя информационной безопасности.

В рамках дальнейших исследований необходимо расширить статистическую базу для обучения полученных моделей, реализовать механизмы получения индикаторов с использованием стандартных технологий и протоколов и экспериментально обосновать более высокую эффективность байесовских сетей для задачи раннего обнаружения внутренних нарушителей ИБ по сравнению с другими методами статического моделирования.

СПИСОК ЛИТЕРАТУРЫ:

1. Infowatch. Безопасность информации в корпоративных информационных системах. Внутренние угрозы. 2013. URL: http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Report_2013_ugroz.pdf
2. *Greitzer F. L., Kangas L. J., Noonan C. F.* Identifying At-Risk Employees: A Behavioral Model for Predicting Insider Threats. Richland, WA: Pacific Northwest National Laboratory, 2010.
3. *Chickering D. M., Heckerman D., Meek C.* Bayesian Approach to Learning Bayesian Networks with Local Structure — Microsoft Research Redmond WA, 1998.
4. Fraud Indicators — USAID Office of the Inspector General Investigations.
5. *Зайцев А. С., Малюк А. А.* Исследование проблемы внутреннего нарушителя // Вестник РГГУ. 2012. № 14. С. 117—133.
6. *Журин С. И.* Основы противодействия инсайдерским угрозам. М.: НИЯУ МИФИ, 2013. — 264 с.
7. *Атаманов А. Н.* Вопросы оценки рисков информационной безопасности в автоматизированных системах // Современная наука: Актуальные проблемы теории и практики. 2012. URL: http://www.nauteh-journal.ru/index.php/ru/----etn12-02/371-a (дата обращения 11.03.2015).
8. *Бидюк П. И., Терентьев А. Н.* Построение и методы обучения Байесовских сетей // Таврический вестник информатики и математики. 2004. № 2. С. 1—3.
9. *Neal R. M., Hilton G. E.* A view of the EM algorithm that justifies incremental, sparse, and other variants. University of Toronto, 1999.
10. *Greitzer F. L., Paulson P. R., Kangas L. J., Franklin L. R., Edgar T. W., Frincke D. A.* Predictive Modeling for Insider Threat Mitigation. Richland. WA: Pacific Northwest National Laboratory, 2009.

REFERENCES:

1. Infowatch. Bezopasnost' informatsyi v korporativnyh informatsionnyh sistemah. Vnutrennie ugrozy. 2013.
2. *Greitzer F. L., Kangas L. J., Noonan C. F.* Identifying At-Risk Employees: A Behavioral Model for Predicting Insider Threats. Richland, WA: Pacific Northwest National Laboratory, 2010.
3. *Chickering D. M., Heckerman D., Meek C.* Bayesian Approach to Learning Bayesian Networks with Local Structure — Microsoft Research Redmond WA, 1998.
4. Fraud Indicators — USAID Office of the Inspector General Investigations.

5. *Zaytsev A. S., Malyuk A. A.* Issledovanie problemy vnutrennego narushitelya // Vestnik RGGU. 2012. № 14. P. 117–133.
6. *Gurin S. I.* Osnovy protivodeystviya insayderskim ugrozam. M.: NRNU MEPHI, 2013.
7. *Atamanov A. N.* Voprosy otsenki riskov informatsionnoy bezopasnosti v avtomatizirovannyh sistemah // Sovremennaya nauka: Aktualnye problem teorii i praktiki. 2012 URL: http://www.nauteh-journal.ru/index.php/ru/----etn12-02/371-a
8. *Bidyuk P. I., Terentyev A. N.* Postroenie i metody obucheniya Bayesovskih setey // Tavricheskiy vestnik informatiki i matematiki. 2004. № 2. P. 1–3.
9. *Neal R. M., Hilton G. E.* A view of the EM algorithm that justifies incremental, sparse, and other variants. University of Toronto, 1999.
10. *Greitzer F. L., Paulson P. R., Kangas L. J., Franklin L. R., Edgar T. W., Frincke D. A.* Predictive Modeling for Insider Threat Mitigation. Richland. WA: Pacific Northwest National Laboratory, 2009.

A. A. Modestov, E. A. Belyaeva

Valuation Method for Hardware-Software Unites of Trusted Boot

Key words: feature, integrated assessment, expertise, unauthorized access

The science-based approach to obtaining integrated assessment of features for hardware-software unites of trusted boot based on an algorithm of receiving a comprehensive measure to assess the effectiveness of protection against unauthorized access and comparative evaluation methodology by "cost — effectiveness is presented by the authors of the article.

А. А. Модестов, Е. А. Беляева

МЕТОДИКА ОЦЕНКИ АППАРАТНО-ПРОГРАММНЫХ МОДУЛЕЙ ДОВЕРЕННОЙ ЗАГРУЗКИ[1]

Рассматривается наиболее широко применяемый класс аппаратно-программных средств защиты информации — аппаратно-программные модули доверенной загрузки (АПМДЗ). Проблема обеспечения научно обоснованного выбора АПМДЗ для решения задач по защите от НСД решается путем разработки научно обоснованной методики получения комплексной оценки функциональных возможностей АПМДЗ, позволяющей выявить АПМДЗ с наилучшими характеристиками обеспечения защиты информации от НСД.

Пусть $A = \{A_i\}$ — множество АПМДЗ, $S = \{S_i\}$ — множество стоимостей АПМДЗ. Каждый АПМДЗ $A_i \in A$ характеризуется: $V_{main} = \{V^j_{main}\}$ — множеством основных функциональных возможностей, $V_{add} = \{V^l_{add}\}$ — множеством дополнительных функциональных возможностей. $E(A_i) = f(V_{main}, V_{add})$, S — критерий эффективности АПМДЗ A_i в части обеспечения защиты обрабатываемой информации от НСД.

Найти такие $A' \in A$, при которых: $E(A') = f(V_{main}(A'), V_{add}(A'), S(A')) = \max(E(A_i))$ [1].

Разработанный алгоритм получения значения показателя для оценки функциональных возможностей АПМДЗ, в зависимости от типа оцениваемых функциональных возможностей (основные или дополнительные), включает в себя следующие этапы:

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполненного совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050