УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2021 Том 21 № 4 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
July–August 2021 Vol. 21 No 4 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2021-21-4-553-561
УДК 004.89; 004.942

Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности

Сергей Валентинович Беззатеев[1]✉, Татьяна Николаевна Елина[2], Владимир Аркадьевич Мыльников[3], Илья Иосифович Лившиц[4]

[1,4] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[1,2,3] Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация

[1] bsv@aanet.ru✉, https://orcid.org/0000-0002-0924-6221
[2] elinatn@yandex.ru, https://orcid.org/0000-0001-5221-7621
[3] va.mylnikov@yandex.ru, https://orcid.org/0000-0002-7532-9607
[4] Livshitz.il@yandex.ru, https://orcid.org/0000-0003-0651-8591

Аннотация

Предмет исследования. Получение достоверных оценок надежности и безопасности корпоративных информационных систем является актуальной проблемой. В настоящее время недостаточно наличие только оценок защищенности программных и программно-аппаратных компонентов. Необходимы постоянный мониторинг действий пользователя и комплексный анализ его поведения в системе. Новизна предлагаемого подхода состоит в применении методов психологического профилирования, моделей нейро-нечеткого вывода и механизмов многомерного анализа данных. Уязвимости компьютерных информационных систем определяются на основе ретроспективного анализа инцидентов информационной безопасности. **Метод.** На основе анализа поведения пользователя построен профиль, и определены паттерны в конкретной компьютерной информационной системе. Исследовано влияние преднамеренного и непреднамеренного поведений пользователя на вероятность реализации угроз информационной безопасности. Выявлены пороговые значения количества и частоты событий, которые свидетельствуют об инциденте безопасности. Построена модель поиска нарушителя при реализации инцидента. **Основные результаты.** Проведена апробация предложенной методики в пакете программ MatLab. Экспериментальные расчеты потенциальных уязвимостей выполнены в системе программ «1С: Предприятие 8.3». В качестве исходных данных для расчета использованы записи журнала регистраций действий более 100 пользователей с различными ролями в течение года. Отмечено, что политика управления рисками должна включать в себя постоянный анализ действий пользователей и их последствий для выявления и предотвращения инцидентов информационной безопасности. Показано, что при реализации представленной методики необходимо постоянное выявление пользователей, которые не должны иметь доступ к важной информации так как нарушитель может находиться в границах компьютерной информационной сети. **Практическая значимость.** Применение разработанной методики позволит повысить уровень обеспечения безопасности при постоянном изменении «рабочего окружения» информационной системы. Упростится процесс принятия объективного и обоснованного управленческих решений о наиболее вероятной реализации инцидентов информационной безопасности. Реализация методики позволит заблаговременно предпринимать необходимые предупредительные меры.

Ключевые слова

моделирование, психологическое профилирование, нейро-нечеткий вывод, многомерный анализ данных, оценка угроз информационной безопасности

Ссылка для цитирования: Беззатеев С.В., Елина Т.Н., Мыльников В.А., Лившиц И.И. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 4. С. 553–561. doi: 10.17586/2226-1494-2021-21-4-553-561

Risk assessment methodology for information systems, based on the user behavior and IT-security incidents analysis

Sergey V. Bezzateev[1]✉, Tatyana N. Elina[2], Vladimir A. Mylnikov[3], Ilya I. Livshitz[4]

[1,4] ITMO University, Saint Petersburg, 197101, Russian Federation
[1,2,3] Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation

[1] bsv@aanet.ru✉, https://orcid.org/0000-0002-0924-6221
[2] elinatn@yandex.ru, https://orcid.org/0000-0001-5221-7621
[3] va.mylnikov@yandex.ru, https://orcid.org/0000-0002-7532-9607
[4] Livshitz.il@yandex.ru, https://orcid.org/0000-0003-0651-8591

Abstract

Obtaining trustworthy estimates for the reliability and security of corporate information systems is an urgent problem. It is not enough just to have estimations for security of software and hardware components. Constant monitoring of a user's actions and a comprehensive analysis of his (her) behavior in the system are necessary. The novelty of the proposed approach consists in application of psychological profiling methods, models of neuro-fuzzy inference and mechanisms of multidimensional data analysis. Vulnerabilities of computer information systems are determined on the basis of a retrospective analysis of information security incidents. The user's profile is based on the analysis of his (her) behavior. The patterns of this behavior in a particular computer information system are determined. The work studies the influence of intentional and unintentional user behavior on the probability of information security threats and identifies the threshold values of the number and frequency of the events indicating an information security incident. Such data helped to build a model to search for an intruder during an information security incident. The proposed method was tested in the MatLab software package. The experimental calculations of potential vulnerabilities were performed in the "1C: Enterprise 8.3" system of programs. As the initial data for the calculation, we used the log entries of the actions of more than 100 users with different roles for a period of one year. It is noted that the risk management policy should include a continuous analysis of user actions, as well as the consequences of these actions, in order to identify the goals of such behavior and prevent information security incidents. It is shown that when implementing the proposed methodology, it is necessary to constantly identify users who should not have access to sensitive information from the inside, assuming that a current violator is located within the boundaries of a computer information network. The application of the proposed methodology allows us to increase the level of information security with a constant change in the "working environment" of the information system. It will help to significantly simplify the process of making an objective and reasonable management decision about the most likely implementation of information security incidents. This allows one to take appropriate preventive measures in advance.

Keywords

modeling, psychological profiling, neuro-fuzzy inference, multidimensional data analysis, information security threat assessment

For citation: Bezzateev S.V., Elina T.N., Mylnikov V.A., Livshitz I.I. Risk assessment methodology for information systems, based on the user behavior and IT-security incidents analysis. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 4, pp. 553–561 (in Russian). doi: 10.17586/2226-1494-2021-21-4-553-561

Введение

Проблемы оценки надежности и безопасности корпоративных информационных систем (КИС) часто связаны с необходимостью проведения постоянного мониторинга действий пользователя и комплексного анализа его поведения в системе [1]. Отметим, что термин КИС применяется как в России (Федеральный закон № ФЗ-63 «Об электронной подписи»), так и в европейской директиве eIDAS. Один из важных классов решений при мониторинге — UEBA/UBA-системы, позволяющие строить модели поведения отдельных пользователей и их групп, отслеживать отклонения от моделей как в режиме реального времени, так и ретроспективно на основе массивов данных о пользователях и объектах системы с помощью алгоритмов машинного обучения и статистического анализа [2]. Данные системы представляют собой комплекс статистических отчетов, и основной их недостаток — большое количество ложноположительных реакций. В связи с этим обеспечить абсолютную защиту и устойчивость системы не представляется возможным.

Результат большого количества ложноположительных срабатываний — последующее игнорирование уведомлений системы безопасности о возможных событиях, что приводит к перегруженности персонала и низкой эффективности выполнения операционной деятельности в области информационной безопасности.

В случае реализации угрозы информационной безопасности и в зависимости от характера события важными являются вопросы выявления уязвимостей в КИС, оценка безопасности ее элементов и поиск нарушителя. Политика управления рисками информационной безопасности в КИС должна включать в себя постоянный анализ действий пользователей, а также последствий этих действий с целью выявления такого поведения для предотвращения инцидентов. Для оценки рисков информационной безопасности можно рекомендовать стандарты ISO/IEC 27005[1], ISO 31000[2], IEC 31010[3] и др. Серьезную проблему для современных КИС представляют утечки данных, происходящие в результате случайных или преднамеренных действий пользова-

[1] ISO/IEC 27005:2018 Information technology — Security techniques – Information security risk management.

[2] ISO 31000:2018 Risk management — Guidelines.

[3] IEC 31010:2019 Risk management — Risk assessment techniques.

телей. Большинство таких утечек составляют данные, которые создаются и используются самими пользователями, поэтому очевидным является начало анализа состояния информационной безопасности изнутри, исходя из предположения, что действующий нарушитель уже находится в периметре КИС. Также необходимо постоянное выявление пользователей, которые не должны иметь доступ к важной информации.

Решение задачи определения уязвимостей КИС, связанных с действиями пользователя на основе ретроспективного анализа событий информационной безопасности, позволит выявить уязвимости, которые могут быть использованы для реализации угрозы информационной безопасности. Таким образом, можно выделить следующие задачи при формировании модели оценки рисков безопасности в КИС на основе анализа поведения пользователей:

— построение модели расчета профиля человека и определения паттернов его поведения в конкретной КИС [3];
— определение влияния преднамеренного и непреднамеренного поведений пользователя на вероятность реализации угрозы информационной безопасности, определение пороговых значений количества и частоты событий, свидетельствующих об инциденте безопасности, с целью минимизации ложноположительных срабатываний;
— построение модели поиска нарушителя при реализации инцидента информационной безопасности с целью выявления уязвимостей КИС.

Профилирование

Профайлинг представляет собой построение модели сотрудника, описывающей его поведение, тенденции в характере и прочую информацию [4]. Также профайлинг включает выявление направления движения мыслей и характера действий злоумышленника, с целью определения ответных или упреждающих действий службы безопасности для обеспечения более высокого уровня информационной безопасности и предотвращения утечки данных [5, 6]. Профайлинг использует комплекс методик для составления психологического портрета человека и определения искренности его намерений [7]. В профайлинге для анализа действий сотрудников пользуются методикой оценки:

— невербального поведения [8];
— речи и ее структуры [9];
— социального взаимодействия и ролей [10].

Принцип работы модели профилирования (рис. 1) представляет собой сбор и консолидацию данных из DLP (Data Leak Prevention)-системы [11], их структурирование и анализ, определение личностных качеств сотрудника на основе его действий в системе [12], выявление характерных тенденций и формирование «файла» каждого пользователя. Данная модель использует методы статистического анализа, машинного обучения и нейро-нечеткого моделирования [13].

Каждый блок модели на рис. 1 представляет собой систему показателей, рассчитываемых на основании ретроспективной информации о действиях пользователя в КИС. Результатом расчета модели будет система комплексных показателей, определяющих уровень соответствия каждого пользователя.

Потенциальные криминальные тенденции {**K**}:

— склонность к интригам, особенно с руководством, стремление быть незаменимым сотрудником k_1;
— возможна непреднамеренная выдача конфиденциальной информации k_2;
— склонность к демонстративным, но при этом незначительным нарушениям корпоративных норм и правил k_3;
— возможны махинации, мелкое мошенничество и хищение (при условии легкости и доступности информации) k_4.

Уровень амбиций {**A**}:

— предъявляет высокие требования к обстоятельствам и коллегам a_1;
— отличается высокой самооценкой, сильным желанием реализоваться и стремлением проявить себя a_2;
— нарушение политики информационной безопасности и корпоративных стандартов вероятны, если нет возможности реализовать собственные амбиции a_3.

Рис. 1. Модель формирования психологического профиля личности
Fig. 1. Model for the formation of the personality psychological profile

Базовые ценности {**B**}:
— внимание и признание окружающих b_1;
— статус и влияние b_2;
— успех и сопричастность b_3.

Видно, что данные показатели имеют качественное выражение, следовательно, для их определения эффективным будет использование механизмов нечеткого логического вывода.

Порог воздействия

Для параметров профиля пользователя сформирован базовый набор выходных данных, соответствующий минимально «триаде безопасности» — конфиденциальности, целостности и доступности[1]. Важно, что в соответствии с «классическими» требованиями (ISO, ГОСТ Р, NIST) базовый набор может быть расширен, например, за счет свойств неотказуемости, подотчетности и прослеживаемости. Для решения задачи данной работы принимается базовый набор данных, который определяет «порог влияния» личных качеств пользователя на реализацию угрозы информационной безопасности:
— уровень конфиденциальности данных *Conf*;
— уровень целостности данных *Int*;
— уровень доступности данных *Acc*.

Цель работы – подбор пороговых значений параметров психологического профиля личности, обеспечивающих требуемый уровень информационной безопасности. В качестве критерия оптимальности использована скорость реагирования системы на события информационной безопасности, которые считаются потенциальными инцидентами (*S*), определяемую количеством событий, корректно выявленных системой в единицу времени:

$$S = \frac{\sum_{j=1}^{j} n_j}{T} \to \min, \tag{1}$$

где n_j — количество инцидентов, произошедших на объекте $j = 1,\ldots, J$ за расчетный период T.

Для целевой функции (1) определены ограничения, с учетом используемых системой ресурсов: стоимость владения системой (*Cost*) не должна превышать требуемую инвестором стоимость в формуле:

$$Cost^{\text{расч}} \le Cost^{\text{треб}}, \tag{2}$$

где расч, треб — указатели на расчетное и требуемое значения критерия.

Потенциальные криминальные тенденции личности (K_i), уровень амбиций и базовые ценности (A_i, B_i):

$$K_i^{\text{расч}} \in (K_i^{\min} \ldots K_i^{\max}) \times k_{\text{изм}}^{K}, \tag{3}$$

$$A_i^{\text{расч}} \in (A_i^{\min} \ldots A_i^{\max}) \times k_{\text{изм}}^{A}, \tag{4}$$

$$B_i^{\text{расч}} \in (B_i^{\min} \ldots B_i^{\max}) \times k_{\text{изм}}^{B}, \tag{5}$$

где max и min — указатели на максимальное и минимальное требуемые значения критерия; $k_{\text{изм}}$ — коэффициент погрешности измерений, возникающей вследствие неточных методик психологической оценки личности, должны находиться в пределах допустимых значений для конкретного рабочего места в рамках отдельного предприятия. Данные требования определяются должностными инструкциями персонала, уровнем доступа к данным и выполняемыми бизнес-процессами. Ограничения по обеспечению требуемой степени конфиденциальности, целостности и доступности данных рассмотрены в формулах принадлежности:

$$Conf^{\text{расч}} \le Conf^{\text{треб}}, \tag{6}$$

$$Int^{\text{расч}} \ge Int^{\text{треб}}, \tag{7}$$

$$Acc^{\text{расч}} \ge Acc^{\text{треб}}, \tag{8}$$

определяются параметрами КИС и зависят от соответствующих показателей защищаемой информации.

Отметим, что $k_{\text{изм}}$ в ограничениях (3)–(5) играет важную роль — оценка применимости выбранной методики и, соответственно, не может определяться только эмпирически. Рекомендуется при определении $k_{\text{изм}}$ применять объективные и воспроизводимые методики аудитов безопасности, например, в соответствии с международными стандартами ISO 19011[2] и ISO 27006[3] [14, 15].

Результат решения данной оптимизационной задачи — получение множеств матриц пороговых значений $\{\mathbf{M}_j\}$ психологических характеристик групп ($i = 1,\ldots, I$) сотрудников, работающих с определенными объектами ($j = 1,\ldots, J$) КИС, сгруппированными по уровню обеспечения безопасности:

$$\mathbf{M}_j = \begin{bmatrix} \mathbf{K}_{11} & \mathbf{K}_{12}\ldots & \mathbf{K}_{1I} \\ \mathbf{A}_{21} & \mathbf{A}_{22}\ldots & \mathbf{A}_{2I} \\ \mathbf{B}_{31} & \mathbf{B}_{32}\ldots & \mathbf{B}_{3I} \end{bmatrix}. \tag{9}$$

Структура сети

Основная проблема анализа инцидентов информационной безопасности — большое количество данных о событиях, происходящих с различными объектами КИС, и активных/пассивных действиях пользователей системы, которые могут иметь, негативные последствия [16]. Предпочтительно выявлять события в точно определенный (заданный) период *T*, не доводя до реализации негативного сценария инцидента безопасности. Данные могут выражаться как в количественных, так и в качественных измерителях, иметь постоянный или периодический характер.

Учитывая данные свойства, для целей анализа уязвимостей системы и поиска виновника инцидента целесообразно использовать механизмы нейро-нечеткого вывода. Поскольку среди всех данных, поступающих

[1] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements — Technical Corrigendum 2.

[2] ISO 19011:2018 Guidelines for auditing management systems.

[3] ISO 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems.

от DLP-системы предприятия, реально влияющими на реализацию угрозы информационной безопасности, является лишь их небольшая часть, то в качестве базовой модели нейро-нечеткой сети была выбрана модель обратного логического вывода [17]. Данная модель позволяет на основании фактов о произошедших инцидентах безопасности исследовать возможное на них влияние значений показателей профилирования сотрудников. Структура системы, использующей обратный логический вывод [18], представлена на рис. 2.

Система состоит из трех основных модулей: психологической оценки сотрудников, реализованной на основании данных, оперативно поступающих из журналов действий пользователей, опросов и тестирований пользователей КИС; определения пороговых значений показателей, относящихся к событиям информационной безопасности, реализованных на базе нейронной сети обратного распространения; поиска уязвимостей и нарушителей по результатам инцидентов безопасности на основе системы обратного логического вывода. Данные для проведения расчетов оперативно поступают от корпоративных DLP-систем, агрегируются и передаются в расчетный блок. Результаты расчета представляются в виде сводных отчетов с использованием OLAP (Online Analytical Processing)-технологии [19].

Результаты расчета

Предлагаемая методика оценки рисков информационной безопасности автоматизированной системы включает следующие этапы.

1. Формирование профилей пользователей информационной системы, оценка значений показателей {**K**}, {**A**} и {**B**} для каждой группы.
2. Расчет матрицы пороговых значений показателей профилирования групп по формулам (1)–(9).
3. Определение вероятности осуществления инцидента в зависимости от принадлежности пользователя к определенной группе с помощью нейро-нечеткой модели (рис. 2).

Расчет риска реализации инцидента безопасности выполняется с учетом влияния каждой группы — размер возможного ущерба от нарушения конфиденциаль-

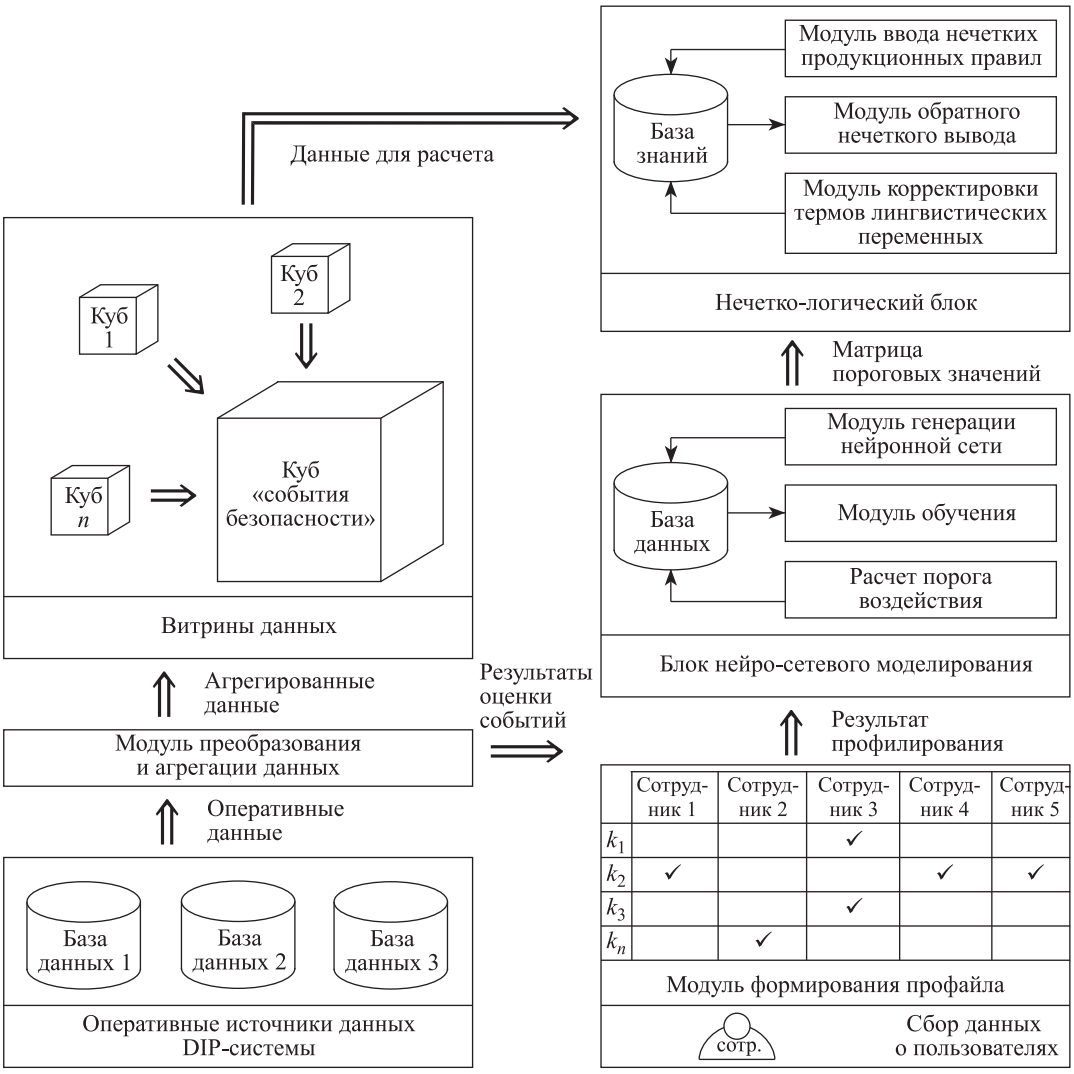

Рис. 2. Архитектура системы оценки рисков информационной безопасности

Fig. 2. Architecture of the Information security risk assessment system

ности, целостности и доступности данных, скорректированного на коэффициент вероятности его реализации.

Реализация описанных моделей в системе MatLab позволила выполнить экспериментальные расчеты потенциальных уязвимостей КИС на базе «1С: Предприятие 8.3» [20]. В качестве данных для анализа были использованы записи журнала регистраций действий пользователей за период, равный одному календарному году. Данная система, работающая в рамках конкретного предприятия, имеет следующие характеристики:

— количество пользователей не более 100 человек;
— роли пользователей: полные права — 4 человека; управление пользователями, редактирование данных — 5 человек; редактирование данных — не более 40 человек; чтение данных — не более 60 человек.

Источником данных для модуля оценки и анализа событий могут быть журналы регистрации событий, изменение справочных данных и документов КИС. Сложность анализа поведения заключается в том, что требуется расчет показателей оценки качества для каждого нового события системы с последующим сравнением динамики их изменений.

Рассмотрим пример оценки сотрудников по следующим показателям:

— число новых клиентов;
— число обслуживаемых клиентов;
— статусы выполнения заявок;
— личный вклад в динамику развития компании;
— предварительный расчет размера заработной платы.

Качественную оценку динамики показателей возможно обеспечить следующим образом:

— отсутствие изменения показателей — оценка изменения данных в справочниках и документах на предмет корректности их заполнения;
— увеличение показателей — оценка подтверждения положительной динамики, проверка личного вклада сотрудника;
— уменьшение показателей у одного сотрудника — оценка причины уменьшения показателя, уведомление и отметка подтверждения правильности события от руководителя звена. Возможная причина события – отказ клиента от дальнейшего оказания услуг, возврат денежных средств за товар или оказанные услуги;
— уменьшение показателей у одного и увеличение у другого сотрудника — оценка причины перераспределения показателей, уведомление и отметка подтверждения правильности события от руководителя звена. Возможная причина события — перераспределение заявок среди сотрудников, повторное оказание услуг другим сотрудником по рекламации.

Для руководителей верхнего уровня важна динамика развития компании в целом, а для руководителей оперативного звена важно контролировать участие сотрудников, фактическую отработку и распределение поощрения за их вклад. Если сотрудник начинает понимать «нюансы» системы поощрений, то могут проявляться попытки модификации данных для повышения личного вклада. Например, создать от своего имени заявку, плановый документ с модифицированным содержанием, при этом на фоне всей компании изменение основных финансовых показателей может не наблюдаться.

В каждой конкретной организации могут разрабатываться корпоративные политики информационной безопасности на базе собственного опыта и рекомендаций специалистов. При разработке модулей оценки и анализа событий необходимо однозначно выявить факт возникновения инцидента, определить причины и последствия, выявить виновника инцидента. После расследования инцидента необходимо разработать механизм организационных действий и скорректировать систему бизнес-правил для дальнейшего предотвращения подобных действий со стороны сотрудников. На основании данных, полученных от DLP-системы, составлены профили пользователей анализируемой КИС. В таблице представлены значения количества пользователей системы «1С: Предприятие 8.3» в каждой из четырех групп, определяемых правами доступа к информации, относящихся к определенному значению показателей **К**, **А** и **В**.

Матрица пороговых значений, рассчитанная по формулам (1)–(9) на основании данных таблицы:

$$\mathbf{M} = \begin{bmatrix} С & С & В & С \\ С & С & В & В \\ Н & Н & В & С \\ Н & Н & В & С \\ С & В & С & Н \\ С & В & Н & Н \\ В & В & С & Н \\ С & С & С & С \\ С & С & С & Н \\ Н & Н & С & С \end{bmatrix},$$

где столбцы — группы сотрудников, строки — показатели профилирования сотрудников.

В результате анализа событий информационной безопасности и оценки вероятности реализации угрозы безопасности для рассматриваемой КИС сформирован график зависимости вероятности реализации инцидента безопасности от принадлежности пользователя к определенной группе (рис. 3).

Рассмотрен следующий перечень событий безопасности (на базе ISO 27005) [21]:

1) утечка персональных данных клиентов;
2) несанкционированное раскрытие конфиденциальной информации;
3) предоставление доступа в систему третьим лицам;
4) умышленное прерывание работы системы;
5) изменение конфигурации и настроек программного обеспечения;
6) реагирование на фишинговое письмо;
7) потеря оборудования, содержащего конфиденциальную информацию;
8) передача данных в непредусмотренном формате в систему, с целью разрушить или нарушить ее нормальную работу;
9) попытка извлечения паролей пользователей.

Таблица. Психологические профили пользователей
Table. Psychological profiles of users

Показатель			Количество пользователей в группе, человек			
			Группа 1	Группа 2	Группа 3	Группа 4
			Полные права	Управление пользователями, редактирование данных	Редактирование данных	Чтение данных
К	k_1	В/С/Н	0/1/3	1/1/2	9/18/13	0/20/40
	k_2	В/С/Н	0/0/4	0/0/4	10/13/17	25/25/10
	k_3	В/С/Н	0/0/4	0/1/2	15/10/15	12/23/25
	k_4	В/С/Н	0/0/4	0/0/4	10/15/15	20/20/20
А	a_1	В/С/Н	0/2/2	4/0/0	10/10/20	0/12/48
	a_2	В/С/Н	1/0/3	3/1/0	20/15/5	12/15/33
	a_3	В/С/Н	0/0/4	1/1/2	15/10/15	5/15/40
В	b_1	В/С/Н	2/1/1	0/2/2	15/15/10	16/20/24
	b_2	В/С/Н	1/2/1	4/0/0	14/12/24	2/4/54
	b_3	В/С/Н	3/1/0	4/0/0	23/13/4	11/22/27

Примечание. Высокое (В)/среднее (С)/низкое (Н) значения показателей.

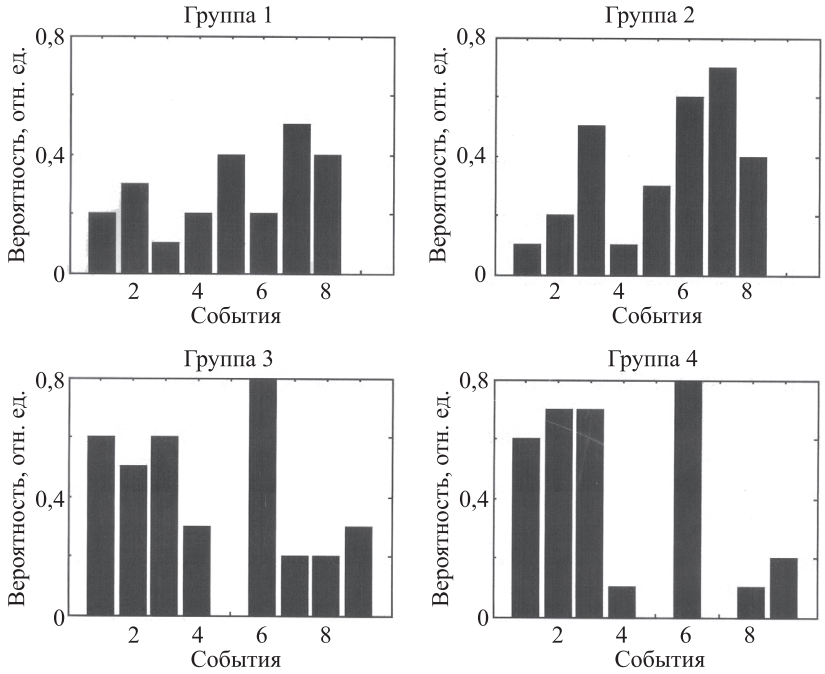

Рис. 3. Графики зависимости вероятности реализации инцидента информационной безопасности от принадлежности пользователя к определенной группе

Fig. 3. Probability of information security incidents depending on the user's membership in a certain group

Согласно построенным зависимостям, можно принимать решения о наиболее вероятной реализации инцидентов безопасности в конкретной КИС и, соответственно, предпринимать соответствующие предупредительные меры защиты.

Заключение

Современные корпоративные информационные системы имеют известный набор механизмов защиты данных на различных уровнях архитектуры: разграничение уровня доступа к объектам данных на уровне файловой системы, баз данных и др.; разграничение уровня доступа к функциям и решаемым задачам; набор бизнес-правил для определения регламента взаимодействия между объектами данных и функциями системы.

Для каждого сотрудника формируются профили безопасности в рабочем окружении операционной системы и роли безопасности в корпоративных информационных системах. Дополнительно необходимо обеспечить оперативное получение сведений об авторах/

владельцах данных, историю их изменения с фиксацией промежуточных значений. Разработку бизнес-правил с положительным эффектом применения возможно создать для корпоративных систем с жестким алгоритмом поведения сотрудника.

По статистике наибольшая частота событий информационной безопасности случайного характера проявляются у новых сотрудников, при модернизации рабочего окружения или при переходе на новую информационную систему, а также среди сотрудников с низкими уровнем обучаемости и склонных по привычке выполнять машинальные действия. Для умышленных событий безопасности требуется хорошая подготовка и время для изучения окружающей обстановки. Для этого больше «подходят» сотрудники с достаточно длительным сроком работы в данной организации. Использование типовых решений для автоматизации производственных процессов может облегчить подготовку к деструктивным действиям благодаря накопленному опыту.

В распоряжении сотрудника могут оказаться различные инструменты, применение которых может привести к реализации инцидента безопасности. Несмотря на грамотно составленный профиль, правила валидации при обработке данных и отсутствии выполнения сотрудником операций с фиксацией нарушения доступа, субъективный алгоритм поведения может привести к различным негативным последствиям при реализации инцидента безопасности.

Для реализации предложенных моделей разработана архитектура информационной системы (рис. 2), реализующая процессы поддержки принятия решений в области управления информационной безопасности, использующая OLAP-технологию хранения и анализа данных. Применение на практике разработанной методики анализа рисков позволит повысить уровень обеспечения безопасности при постоянном изменении «рабочего окружения» корпоративных информационных систем.

Литература

1. Yelina T.N., Mylnikov V.A., Bezzateev S.V. Optimal allocation of cloud service resources using multi-agent technologies // Proc. of the 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2020. P. 9131519. https://doi.org/10.1109/WECONF48837.2020.9131519
2. Сравнительный обзор решений класса UBA // БИТ. Бизнес & Информационные технологии. 2019. № 9(92). С. 14–15.
3. Черкасова Е.С. Профайлинг как метод создания психологического портрета потенциального преступника на этапе организации предварительного расследования // Вестник Новосибирского государственного университета. Серия: Право. 2013. Т. 9. № 1. С. 72–75.
4. Муравьев Н.С., Астахова Л.В. Профилактика инцидентов информационной безопасности на основе профилирования пользователей: программно-технический аспект // Вестник УрФО. Безопасность в информационной сфере. 2018. № 1(27). С. 66–70.
5. Тулупьева Т.В., Азаров А.А., Тулупьев А.Л. Социоинженерные атаки как вид социального воздействия // Научные труды Северо-Западного института управления РАНХиГС. 2013. Т. 4. № 4(11). С. 100–110.
6. Голянич В.М., Тулупьева Т.В., Ющенко Н.А., Глазырин А.А. Ценностные ориентиры и потребности государственных гражданских служащих // Научные труды Северо-Западного института управления РАНХиГС. 2013. Т. 4. № 4(11). С. 20–36.
7. Пучков И.И. Коммерческий профайлинг в DLP-системах // Молодой ученый. 2017. № 51(185). С. 75–77 [Электронный ресурс]. URL: https://moluch.ru/archive/185/47448/ (дата обращения: 02.04.2021).
8. Рюмин Д. Метод автоматического видеоанализа движений рук и распознавания жестов в человеко-машинных интерфейсах // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 4. С. 525–531. https://doi.org/10.17586/2226-1494-2020-20-4-525-531
9. Татарникова Т.М., Богданов П.Ю. Построение психологического портрета человека с применением технологий обработки естественного языка // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 1. С. 85–91. https://doi.org/10.17586/2226-1494-2021-21-1-85-91
10. Зубкова Т.М., Тагирова Л.Ф., Тагиров В.К. Прототипирование адаптивных пользовательских интерфейсов прикладных программ с использованием методов искусственного интеллекта // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 4. С. 680–688. https://doi.org/10.17586/2226-1494-2019-19-4-680-688
11. Данильченко П.А., Седина М.С. Анализ возможностей современных DLP-систем // Colloquium-journal. 2019. № 1-5 (25). С. 61–62.

References

1. Yelina T.N., Mylnikov V.A., Bezzateev S.V. Optimal allocation of cloud service resources using multi-agent technologies. *Proc. of the 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, 2020, pp. 9131519. https://doi.org/10.1109/WECONF48837.2020.9131519
2. Review of solutions of the UBA class. *BIT. Business & Information Technology*, 2019, no. 9(92), pp. 14–15. (in Russian)
3. Cherkasova E.S. Profiling as a method of creating a psychological portrait of a potential criminal at the stage of preliminary investigation, the effective. *Vestnik Novosibirskogo gosudarstvennogo universiteta. Pravo*, 2013, vol. 9, no 1, pp. 72–75. (in Russian)
4. Muravyov N.S., Astakhova L.V. Prevention of information security incidents based on user profling: program-technical aspect. *Bulletin of the Ural Federal District. Security in the Information Sphere*, 2018, no. 1(27), pp. 66–70. (in Russian)
5. Tulupeva T.V., Azarov A.A., Tulupev A.L. Socio-engineering attacks as the form of social action. *Nauchnye trudy Severo-Zapadnogo instituta upravlenija RANHiGS*, 2013, vol. 4, no. 4(11), pp. 100–110. (in Russian)
6. Golyanich V.M., Tulupeva T.V., Yushchenko N.A., Glazyrin A.A. Targets and requirements of civil servants. *Nauchnye trudy Severo-Zapadnogo instituta upravlenija RANHiGS*, 2013, vol. 4, no. 4(11), pp. 20–36. (in Russian)
7. Puchkov I.I. Commercial profiling in DLP systems. *Young Scientist*, 2017, no. 51(185), pp. 75–77. Available at: https://moluch.ru/archive/185/47448/ (accessed: 02.04.2021). (in Russian)
8. Ryumin D. Automated hand detection method for tasks of gesture recognition in human-machine interfaces. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2020, vol. 20, no. 4, pp. 525–531. (in Russian). https://doi.org/10.17586/2226-1494-2020-20-4-525-531
9. Tatarnikova T.M., Bogdanov P.Yu. Human psyche creation by application of natural language processing technologies. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 1, pp. 85–91. (in Russian). https://doi.org/10.17586/2226-1494-2021-21-1-85-91
10. Zubkova T.M., Tagirova L.F., Tagirov V.K. Prototyping of adaptive user application programming interfaces by artificial intelligence methods. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 4, pp. 680–688. (in Russian). https://doi.org/10.17586/2226-1494-2019-19-4-680-688
11. Danilchenko P.A., Sedina M.S. Analysis of opportunities of modern DLP-systems. *Colloquium-journal*, 2019, no. 1-5 (25), pp. 61–62. (in Russian)

12. Богданов Д.С. Системы распознавания речи: классификация, методы и алгоритмы реализации // Аллея науки. 2018. Т. 7. № 11(27). С. 819–823.
13. Еремеев Е.А. Распознавание образов в экспертных системах принятия решений // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 4. С. 704–713. https://doi.org/10.17586/2226-1494-2019-19-4-704-713
14. Лившиц И.И. Аудит информационной безопасности объектов топливно-энергетического комплекса // Энергобезопасность и энергосбережение. 2021. № 1. С. 5–12. https://doi.org/10.18635/2071-2219-2021-1-5-12
15. Басырова А.А., Лившиц И.И. Анализ методики аудита информационной безопасности предприятия с помощью аутсорсинговых компаний // Автоматизация в промышленности. 2020. № 7. С. 6–9. https://doi.org/10.25728/avtprom.2020.07.02
16. Purtov D., Sidorkina I. An approach combining general and highly specialized semantic analysis in DLP systems // Открытые семантические технологии проектирования интеллектуальных систем. 2020. № 4. С. 301–304.
17. Елин Н.Н., Бубнов В.Б., Мыльников В.А., Елина Т.Н. Экспертная система принятия решений по перспективному развитию системы водоснабжения городского района на основе модели обратного нечёткого логического вывода / Технологии техносферной безопасности. 2018. № 1(77). С. 81–89. https://doi.org/10.25257/TTS.2018.1.77.81-89
18. Gao Y., Xu L., Su Y., Ranasinghe D.C. Lightweight (reverse) fuzzy extractor with multiple reference PUF responses // IEEE Transactions on Information Forensics and Security. 2019. V. 14. N 7. P. 1887–1901. https://doi.org/10.1109/TIFS.2018.2886624
19. Tardío R., Maté A., Trujillo J. A new big data benchmark for OLAP cube design using data pre-aggregation techniques // Applied Sciences (Switzerland). 2020. V. 10. N 23. P. 8674. https://doi.org/10.3390/app10238674
20. Савина А.Г., Малявкина Л.И. Концепция построения архитектуры системы «1С: Предприятие» и средства разработки прикладных решений // Экономическая среда. 2021. № 1(35). С. 63–69. https://doi.org/10.36683/2306-1758/2021-1-35/63-69
21. Кузьмичёва С.А., Тарабрина О.В. Построение аналитической системы анализа событий для обеспечения информационной безопасности предприятия // Безопасность информационных технологий. 2019. Т. 26. № 1. С. 6–14.

12. Bogdanov D.S. Speech recognition systems: classification, methods and algorithms. *Alley Science*, 2018, vol. 7, no. 11(27), pp. 819–823. (in Russian)
13. Eremeev E.A. Pattern recognition in expert decision-making systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 4, pp. 704–713. (in Russian). https://doi.org/10.17586/2226-1494-2019-19-4-704-713
14. Livshitz I. Information security audit for fuel and power sector facilities. *Energy Safety and Energy Economy*, 2021, no. 1, pp. 5–12. (in Russian). https://doi.org/10.18635/2071-2219-2021-1-5-12
15. Basyrova A.A., Livshits I.I. Analyzing the methodology of enterprise cybersecurity audit with the help of outsourcing companies. *Automation in Industry*, 2020, no. 7, pp. 6–9. (in Russian). https://doi.org/10.25728/avtprom.2020.07.02
16. Purtov D., Sidorkina I. An approach combining general and highly specialized semantic analysis in DLP systems. *Open Semantic Technology for Intelligent Systems*, 2020, no. 4, pp. 301–304.
17. Yelin N.N., Bubnov V.B., Mylnikov V.A., Elina T.N. Expert system of decision-making on perspective development of system of water supply of the urban area on the basis of model of the return indistinct logical conclusion. *Technology of Technosphere Safety*, 2018, no. 1(77), pp. 81–89. (in Russian). https://doi.org/10.25257/TTS.2018.1.77.81-89
18. Gao Y., Xu L., Su Y., Ranasinghe D.C. Lightweight (reverse) fuzzy extractor with multiple reference PUF responses. *IEEE Transactions on Information Forensics and Security*, 2019, vol. 14, no. 7, pp. 1887–1901. https://doi.org/10.1109/TIFS.2018.2886624
19. Tardío R., Maté A., Trujillo J. A new big data benchmark for OLAP cube design using data pre-aggregation techniques. *Applied Sciences (Switzerland)*, 2020, vol. 10, no. 23, pp. 8674. https://doi.org/10.3390/app10238674
20. Savina A.G., Malyavkina L.I. Architecture concept of the system 1C: enterprise and means of applied solutions designing. *Economic Environment*, 2021, no. 1(35), pp. 63–69. (in Russian). https://doi.org/10.36683/2306-1758/2021-1-35/63-69
21. Kuzmicheva S.A., Tarabrina O.V. Building an analytical system for event analysis to ensure information security of the enterprise. *IT Security (Russia)*, 2019, vol. 26, no. 1, pp. 6–14. (in Russian)

Авторы

Беззатеев Сергей Валентинович — доктор технических наук, доцент, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; заведующий кафедрой, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, SC 6602425996, https://orcid.org/0000-0002-0924-6221, bsv@aanet.ru

Елина Татьяна Николаевна — кандидат экономических наук, доцент, доцент, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, SC 65044605, https://orcid.org/0000-0001-5221-7621, elinatn@yandex.ru

Мыльников Владимир Аркадьевич — кандидат технических наук, доцент, доцент, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, SC 57194518638, https://orcid.org/0000-0002-7532-9607, va.mylnikov@yandex.ru

Лившиц Илья Иосифович — доктор технических наук, профессор практики, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57191569306, https://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Authors

Sergey V. Bezzateev — D.Sc., Associate Professor, Professor, ITMO University, Saint Petersburg, 197101, Russian Federation; Head of Chair, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation, SC 6602425996, https://orcid.org/0000-0002-0924-6221, bsv@aanet.ru

Tatyana N. Elina — PhD, Associate Professor, Associate Professor, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation, SC 6504460516, https://orcid.org/0000-0001-5221-7621, elinatn@yandex.ru

Vladimir A. Mylnikov — PhD, Associate Professor, Associate Professor, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation, SC 57194518638, https://orcid.org/0000-0002-7532-9607, va.mylnikov@yandex.ru

Ilya I. Livshitz — D.Sc., Full Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57191569306, https://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Статья поступила в редакцию 31.05.2021
Одобрена после рецензирования 16.06.2021
Принята к печати 30.07.2021

Received 31.05.2021
Approved after reviewing 16.06.2021
Accepted 30.07.2021