DOI: 10.24412/2413-2527-2023-234-50-57

Методика выявления потенциальных внутренних нарушителей информационной безопасности

к.т.н. С. В. Корниенко, А. В. Пантюхина
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
sv.diass99@ya.ru, shikhova.nastya43@gmail.com

Аннотация. **Рассматривается подход к классификации внутренних нарушителей информационной безопасности организации. Представлены предложения по выявлению склонных к противоправным действиям лиц (потенциальных нарушителей) путем контроля их деятельности и оценки психоэмоционального состояния. Для этого предлагается методика предварительной оценки психоэмоционального состояния персонала по клавиатурному почерку, реализованная в виде прототипа программного средства анализа основных параметров клавиатурного почерка.**

Ключевые слова: **защита информации, информационная безопасность, внутренний нарушитель, клавиатурный почерк.**

Введение

Вопросы обеспечения информационной безопасности в любой организации являются неотъемлемой составляющей построения успешных бизнес-процессов. Один из наиболее актуальных вопросов обеспечения информационной безопасности — выявление внутренних нарушителей информационной безопасности. Это сложная проблема, требующая нестандартных решений.

Внутренние нарушители — это сотрудники и внешние специалисты, имеющие доступ к конфиденциальным данным, обрабатываемым в информационной системе (ИС) организации. Угрозы информационной безопасности, исходящие от потенциальных внутренних нарушителей, могут быть случайными (ошибки при вводе информации и выполнении операций в ИС) и преднамеренными (кража информации). В обоих случаях важно своевременно выявить потенциального нарушителя для уменьшения риска утечки или несанкционированной модификации информации.

Кроме того, выявление внутренних нарушителей помогает улучшить культуру информационной безопасности в организации. Постоянный контроль и надзор за персоналом стимулирует сотрудников соблюдать правила и процедуры компании, а также повышает их ответственность и профессионализм.

Таким образом, выявление внутренних нарушителей информационной безопасности является актуальной и крайне важной задачей для любой организации, которая заботится о своей безопасности и защите конфиденциальной информации.

Один из возможных подходов к решению этой проблемы состоит в оценке и контроле психоэмоционального состояния сотрудников. Различные исследования показывают, что нарушения нормальных поведенческих характеристик например, напряжение, тревожность, скрытность, могут стать значимыми для выявления потенциальных внутренних нарушителей.

Классификация внутренних нарушителей

Существует несколько подходов к классификации внутренних нарушителей, но по отношению к психоэмоциональному состоянию сотрудников наиболее интересной представляется классификация внутренних нарушителей в зависимости от мотивации (табл. 1) [1].

Первые две группы нарушителей могут быть определены как «лояльные», или незлонамеренные, так как они совершают свои действия в интересах компании. Для предотвращения последствий необходимо применять тех-

Таблица 1

Типы внутренних нарушителей

Тип	Умысел	Корысть	Постановка задачи	Действия при возможности
Халатный	Нет	Нет	Нет	Сообщение
Манипулируемый	Нет	Нет	Нет	Сообщение
Обиженный	Да	Нет	Сам	Отказ
Нелояльный	Да	Нет	Сам	Имитация
Подрабатывающий	Да	Да	Сам/Извне	Отказ/Имитация/Взлом
Внедренный	Да	Да	Извне	Взлом

нические методы блокирования попыток нарушения безопасности информации и объяснять таким сотрудникам неприемлемость планируемых действий.

Следующая группа нарушителей отличается от предыдущих тем, что они осознают, что своими действиями наносят вред компании, в которой работают. Они могут быть подразделены на три типа: саботажников, нелояльных и мотивируемых извне, в зависимости от мотивов своих враждебных действий и поведения, которое помогает предсказать их действия. «Обиженные» и «нелояльные» нарушители представляют среднюю степень опасности. Они сами выбирают объект, который хотят украсть, уничтожить или изменить, а также место, где можно это продать. Если они не могут украсть информацию или обойти систему безопасности, то не будут искать технический способ сделать это. Кроме того, вероятно, что у таких нарушителей недостаточно технических навыков для совершения преступления.

«Подрабатывающие» и «внедренные» нарушители реализуют осознанные действия с целью украсть информацию по требованиям конкретного заказчика. Такие нарушители представляют наиболее высокую степень опасности, стараются максимально скрыть свои действия, но их мотивация различается.

Широко распространенный тип сотрудников, известный как «подрабатывающие», включает в себя людей, которые ищут дополнительный заработок, а также тех, кто сталкивается с шантажом и вымогательством со стороны третьих лиц и вынужден выполнить запрошенные задачи любыми доступными им способами. В зависимости от ситуации они могут прекратить свои попытки, симулировать необходимость производства или даже совершить взлом и подкупить других сотрудников, чтобы получить доступ к нужной информации.

«Внедренные» инсайдеры используются не только для промышленного, но и для государственного шпионажа. Такие нарушители могут быть оснащены эффективными специальными устройствами или программами для обхода ограничений, что позволят им получать данные из корпоративной сети. Они используют самые продвинутые средства и имеют большой опыт взлома.

Общая характеристика нарушителя заключается в том, что он совершает преступление из-за своих психологических особенностей, антиобщественных взглядов, отрицательного отношения к моральным ценностям и выбора опасного пути для удовлетворения своих потребностей или из-за недостатка активности в предотвращении негативных последствий.

Нарушитель имеет определенные психологические особенности, которые приводят к его антиобщественному поведению. Общественная опасность означает, что у него есть потенциал для совершения преступлений в определенных обстоятельствах. Это связано с его внутренними предпосылками для такого поведения [2].

Нарушителей можно разделить на две группы по характеру поведения при совершении противоправных действий на объекте: осторожные и неосторожные [3].

Для осторожных нарушителей характерны низкий уровень тревожности, общительность и установление межличностных контактов, высокий уровень социальной адаптации, отсутствие моральных проблем после совершения преступления. Отличить таких нарушителей от добросовестных сотрудников по отклонению психоэмоциональных характеристик от нормального состояния невозможно. Для выявления подобных нарушителей необходимо применять другие методы.

Неосторожные нарушители характеризуются высоким уровнем тревожности, склонны к интрапунитивным реакциям в ситуации фрустрации, чем отличаются от умышленных преступников, которые склонны к экстрапунитивным реакциям, то есть к вине окружающих людей в своих неудачах, проявляют неуверенность в себе, склонность к волнениям при стрессе, избыточный самоконтроль, дезорганизованное поведение, показывают эмоциональные реакции на угрозы в экстремальной ситуации.

Таким образом, можно построить модель потенциального внутреннего нарушителя, которая описывает процесс внутренней угрозы для компьютерной системы или сети [4]. Основными характерными показателями потенциального инсайдера будут следующие:

1. Мотивация — причина, по которой сотрудник становится внутренним нарушителем. К мотивации могут относиться финансовые причины, личные обиды, нежелание выполнять работу и многие другие факторы.

2. Возможность — уровень доступа, который имеет сотрудник к компьютерной системе или сети. Доступ может быть предоставлен согласно должности сотрудника или получен несанкционированным способом.

3. Средства — программы или аппаратура, которые использует нарушитель для совершения преступления. Средства могут быть различными: вредоносное ПО, программы для сбора паролей, сканеры уязвимостей, а также физические устройства, такие как USB-накопители или внешние жесткие диски.

4. Действие — само преступление, которое совершает внутренний нарушитель. Оно может включать в себя воровство данных, электронный шпионаж, уничтожение или изменение данных и другие действия.

5. Обнаружение — процесс выявления преступления. Обнаружение может происходить как в реальном времени, так и позже при анализе системных журналов, логов и других данных.

6. Реакция — комплекс мер, которые предпринимаются для нейтрализации внутренней угрозы и устранения ее последствий. Реакция может включать в себя блокирование доступа к системе, вызов правоохранительных органов, восстановление удаленных данных и другое.

Методы выявления внутренних нарушителей

Проблема защиты информации от внутреннего нарушителя является одной из наиболее сложных проблем в области информационной безопасности, так как зависит от психологических и поведенческих аспектов, которые с трудом поддаются оценке и прогнозированию.

Существует стандартный комплекс организационных и технологических мер, которые в определенной степени способствуют обнаружения инсайдеров:

1. Защита информационных систем от атак или инцидентов — мониторинг сети организации, установка антивирусного программного обеспечения на все АРМы, использование средств межсетевого экранирования и криптозащиты каналов связи, сканера безопасности, системы

обнаружения вторжений, системы централизованного мониторинга событий безопасности.

2. Организация бизнес-структур и процессов для такого формата ведения бизнеса, при котором снижается вероятность инцидента или атаки, а в случае возникновения его влияние сводится к минимальным потерям, что заключается в четком разделении обязанностей сотрудников, назначении ответственных за защиту информации в подразделениях, построении корректной модели управления доступом.

3. Формирование культуры, ценностей и убеждений в организации, создание общих целей, например путем повышения квалификации, а также контроль знаний обслуживающего персонала и пользователей.

Меры по выявлению внутреннего нарушителя различаются в зависимости от этапа действий инсайдера.

Для предотвращения и прогнозирования внутренних угроз необходимо проанализировать потенциальные показатели и использовать правильную внутреннюю политику, которая включает контроль соблюдения нормативных требований и предотвращение инсайдерских атак.

Обнаружение внутренней угрозы на этапе ее реализации является сложным процессом, который может быть облегчен с помощью мониторинга рабочих программ и процессов, а также ведения журналов. Необходимо учитывать, что выявление внутренних инцидентов реализуется гораздо сложнее, чем внешних.

Реагирование на внутреннюю угрозу включает исправление недостатков и пресечение дальнейших инцидентов, чтобы минимизировать последствия и вероятность их возникновения в будущем. Организации также должны принимать разумные меры в отношении соответствующих инсайдеров [5].

Максимально уменьшить риски нарушения информационной безопасности позволяет введение элементов проактивной защиты от инсайдеров, которые направлены на раннее обнаружение потенциальных нарушителей и недопущение совершения преступления.

Для выявления потенциальных внутренних нарушителей необходимо проводить анализ поведения сотрудников в рабочих программах, анализировать изменения в корпоративном общении и изучать изменения метрик их эффективности. Это включает мониторинг и анализ поведения, обнаружение поведенческих отклонений и установку приоритетов для них, чтобы оперативно реагировать на наиболее серьезные и массовые изменения в поведении.

Для обнаружения инсайдерской деятельности в организации может оцениваться потенциальная склонность сотрудника организации к инсайдерской деятельности. Анализируются следующие показатели:

1. Личностные показатели: находится ли сотрудник в состоянии депрессии, наличие у него зависимостей (алкогольной, наркотической, от азартных игр), недавнее психологическое потрясение (смерть близкого человека), наличие тяжелых или хронических заболеваний у сотрудника или у его близких родственников, проблемы в личной жизни, неудовлетворенность должностью, оплатой или условиями труда.

2. Поведенческие показатели: нарушение сотрудником установленных в организации правил или трудового распорядка, переработки, резкие высказывания и агрессия, а также преднамеренное нанесение вреда.

3. Контекстные показатели: несогласие с единым мнением в организации, наличие судимости, доступ к финансам организации, ведение собственного бизнеса, наличие долгов и кредитов.

4. Скрининговые показатели: наличие зависимостей (алкогольной, наркотической, от азартных игр), недавнее психологическое потрясение (смерть близкого человека), наличие тяжелых или хронических заболеваний у сотрудника или у его близких родственников, плохая репутация на прошлых местах работы, наличие долгов и кредитов, предоставление недостоверных данных при устройстве на работу, наличие неоднозначных связей с криминальными личностями, распространение конфиденциальной информации, совершение противоправных действий [6].

Существующие программы для защиты информации обычно не могут эффективно отслеживать и обнаруживать необычное поведение сотрудников, хотя системы управления информационной безопасностью и другие инструменты могут помочь в выявлении внутренних угроз. Однако даже такой подход не гарантирует полную защиту от внутренних нарушителей.

Изучение информации о действиях пользователей может помочь обнаружить внутренние угрозы, такие как использование системы в нерабочее время, копирование или загрузка больших объемов данных, доступ к информации, которая не относится к рабочим обязанностям и т. д. [7, 8].

Для такой категории нарушителей, как «неосторожные» нарушители, возможно проактивное (на ранних этапах) выявление потенциальных, склонных к противоправным действиям лиц путем контроля их деятельности и оценки психоэмоционального состояния.

В качестве одного из технических индикаторов, которые могут указывать на наличие потенциальной инсайдерской угрозы, может выступать клавиатурный почерк в совокупности таких показателей, как темп набора, скорость печати, динамика ввода, системные опечатки и использование определенных букв, символов и «горячих» клавиш [9, 10]. Совокупность определенных значений каждого из этих показателей образует достаточно индивидуальную картину, соответствующую конкретному человеку в определенном психоэмоциональном состоянии.

Клавиатурный почерк — это комплекс навыков, основанных на печатно-двигательном функционально-динамическом процессе, который отображается в печатных символах и включает в себя субъективные и объективные образы набираемых символов. У исполнителя развивается специальная система движений, которая автоматизирует процесс передачи символов на экран с помощью клавиатуры.

Клавиатурный почерк — одна из динамических биометрических характеристик, которая описывает привычные подсознательные действия пользователя. Исследования показывают, что клавиатурный почерк конкретного пользователя также является стабильным.

Опознавание клавиатурного почерка состоит в выборе соответствующего эталона из списка хранимых в памяти компьютера эталонов на основе оценки степени близости этому эталону параметров почерка одного из операторов, имеющих право на работу с данным компьютером. Реше-

ние задачи опознавания состояния пользователя сводится к решению задачи распознавания образов. Использование клавиатурного почерка не требует установки специальных аппаратных средств и кадров для установки и поддержки, является прозрачным для конечного пользователя, то есть не причиняет неудобств пользователю.

Классический статистический подход к распознаванию психоэмоционального состояния пользователя по клавиатурному почерку (набор ключевых слов) выявил ряд интересных особенностей: зависимости почерка от буквенных сочетаний в слове, существование глубоких связей между набором отдельных символов, наличие «задержек» при вводе символов [11].

Для составления алгоритма определения эмоционального состояния пользователя по клавиатурному почерку необходимо выявить связь между особенностями почерка и определенными эмоциональными состояниями. Необходимо составить психологический портрет внутреннего нарушителя, определить особенности его поведения.

Оценка психоэмоционального состояния человека по клавиатурному почерку

Для оценки психоэмоционального состояния человека по клавиатурному почерку выявления внутреннего нарушителя по клавиатурному почерку необходимо пройти несколько этапов.

Для получения данных о клавиатурном почерке каждого пользователя необходимо использовать специальную программу (кейлоггер, так называемый «клавиатурный шпион»), которая записывает скорость и стиль печати, нажимаемую клавишу и задержку между нажатиями клавиш [12–14]. Существуют два вида кейлоггеров: программный и аппаратный. Программный кейлоггер инсталлируется на компьютер и скрытно фиксирует нажатия клавиш в журнале регистрации действий. Аппаратный кейлоггер присоединяется к компьютеру через USB-порт и фиксирует все данные, передаваемые от клавиатуры по системной шине.

Первоначально анализируются зависимости между различными характеристиками клавиатурного почерка каждого сотрудника и происходит определение индивидуального профиля клавиатурного почерка пользователя. Для этого анализируются все параметры печати, определяются общие черты и особенности каждого человека.

Зависимости клавиатурного почерка человека могут определяться по нескольким критериям [15]:

1. Частота использования определенных клавиш. Некоторые люди могут чаще нажимать определенные клавиши, что может быть связано с их привычками или особенностями руки.

2. Скорость набора текста. У разных людей может быть разная скорость набора, что связано с их опытом работы с клавиатурой и уровнем навыков.

3. Стиль набора текста. Некоторые люди могут использовать определенные техники набора текста, например печатать вслепую или использовать только определенные пальцы.

4. Ошибки при наборе текста. Определенные ошибки при наборе текста (например, частое нажатие клавиши Caps Lock) могут свидетельствовать о привычках и особенностях человека.

Для определения зависимостей клавиатурного почерка человека могут использоваться специальные программы, которые анализируют набор текста и выявляют различные характеристики и особенности клавиатурного почерка.

С точки зрения определения психоэмоционального состояния сотрудника значимыми представляются следующие признаки компьютерного почерка:

1. Интервал между нажатиями клавиш — это время, которое проходит между нажатием одной клавиши и следующей. Этот интервал может быть разным для разных людей и зависит от их навыков печати на клавиатуре.

Интервал между нажатиями клавиш может зависеть от психоэмоционального состояния человека. Например, при стрессе или нервозности интервал между нажатиями клавиш может быть сокращен, что может привести к ошибкам при наборе текста. С другой стороны, при расслабленном состоянии интервал между нажатиями клавиш может быть увеличен, что может улучшить качество набора текста. Также интервал между нажатиями клавиш может зависеть от уровня усталости человека. При усталости интервал между нажатиями клавиш может быть увеличен, что может привести к снижению скорости набора текста и увеличению количества ошибок.

В целом, психоэмоциональное состояние человека может оказывать существенное влияние на интервал между нажатиями клавиш, но это зависит от многих факторов и может быть индивидуальным для каждого человека.

2. Количество опечаток — это процент опечаток относительно набранного текста. Большое количество опечаток может быть связано с различными факторами, в том числе и психоэмоциональное состояние человека может оказывать влияние на количество опечаток в его текстах. Например, если человек находится в состоянии стресса, усталости или беспокойства, он становится менее внимательным и более склонным к ошибкам при наборе текста. Также, если человек испытывает сильные эмоции, например радость или гнев, то он может набирать текст быстрее, но при этом допускать больше опечаток. Кроме того, психоэмоциональное состояние может влиять на концентрацию и внимание человека, что также может приводить к ошибкам при наборе текста. Например, если человек занят мыслями о какой-то проблеме или событии, то он может быть менее внимательным к деталям и допускать больше опечаток.

Таким образом, психоэмоциональное состояние человека может оказывать влияние на количество опечаток в его текстах, поэтому важно учитывать этот фактор при анализе ошибок в текстах.

Далее с определенной периодичностью или по необходимости на основе полученного эталонного профиля сотрудника можно проводить контроль клавиатурного почерка человека. При анализе клавиатурного почерка можно выявить признаки, указывающие на психическое напряжение, уровень тревоги и депрессии, наличие агрессивности и другие внутренние нарушения. При наблюдении отклонений от эталонных значений и других аномалий в клавиатурном почерке пользователя необходимо проанализировать их в контексте деятельности сотрудника на рабочем месте. Это позволит своевременно выявить потенциального внутреннего нарушителя и предпринять

меры по предотвращению утечки данных или других опасных инцидентов.

Методика оценки психоэмоционального состояния персонала

По результатам проведенного анализа разработана методика предварительной оценки психоэмоционального состояния персонала с целью выявления потенциальных инсайдеров, которая основывается на выявлении аномалий двух основных показателей клавиатурного почерка:

1. Интервал между нажатиями клавиш. Кейлоггер постоянно фиксирует все нажатия клавиш и время выполнения действий. Средство мониторинга и анализа на основании данных отчета периодически рассчитывает среднее значение интервала между нажатиями клавиш за определенный временной промежуток. Если эталонное значение превышено более чем на 25 %, администратором безопасности будет получено предупреждение о напряженном состоянии пользователя. Если интервал между нажатиями клавиш на 50 % больше эталонного значения, администратор получит уведомление о том, что сотрудник, скорее всего, находится в критическом психоэмоциональном состоянии.

2. Количество ошибок (нажатия клавиш удаления). Существует много разных способов исправления ошибок (например, выбор с помощью мыши и замена с помощью нажатий клавиш). Невозможно уловить все вероятные сценарии коррекции, поэтому, как наиболее распространенный вариант, учитываются нажатия клавиш Delete и Backspace. Такие данные дают усредненное представление о количестве допущенных ошибок при наборе текста. За эталонное значение принято 1,5 % ошибок относительно набранного текста. Если количество допущенных пользователем ошибок превышает эталонное более чем на 1,5 %, администратор безопасности получит уведомление о повышенной невнимательности сотрудника.

Однако следует отметить, что разработанная методика имеет свои ограничения и не может заменить более традиционные методы оценки личности, например психологические тесты или интервью. Также важно учитывать, что эмоциональное состояние человека может меняться в течение дня или в зависимости от ситуации, поэтому результаты оценки следует интерпретировать с осторожностью.

Таким образом, методика оценки психоэмоционального состояния персонала по клавиатурному почерку может быть полезным дополнением к другим методам оценки, однако ее использование требует профессионального подхода и компетентности.

Прототип программного средства оценки психоэмоционального состояния персонала

Для оценивания эффективности предложенной методики было разработано программное средство мониторинга и анализа клавиатурного почерка человека.

Для мониторинга выбранных параметров почерка использовался кейлоггер собственной разработки. По результатам его работы формируется отчет о действиях с клавиатурой достаточно стандартного вида (рис. 1).

В отчете зафиксировано время нажатия клавиши и ее синтаксическое значение. Далее выполняется автоматизированный анализ полученных данных: расчет и оценивание

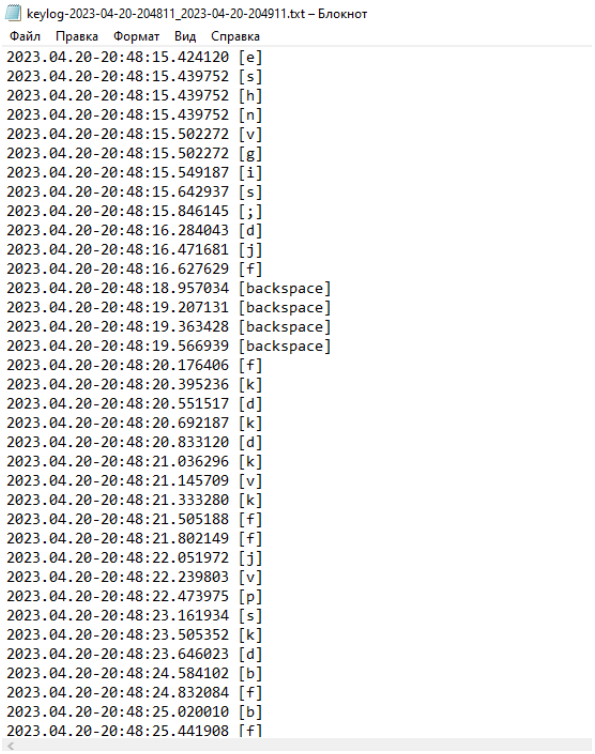

Рис. 1. Пример отчета кейлоггера

ние пауз между нажатиями клавиш, количество нажатий клавиш Delete и Backspace, сравнение значений полученных показателей с рассчитанным эталонным профилем пользователя и формирование отчета по результатам анализа. При выявлении значимых отклонений от эталонных «нормальных» значений администратору безопасности передается сообщение.

Примеры отчета по результатам анализа представлены на рисунках 2 и 3.

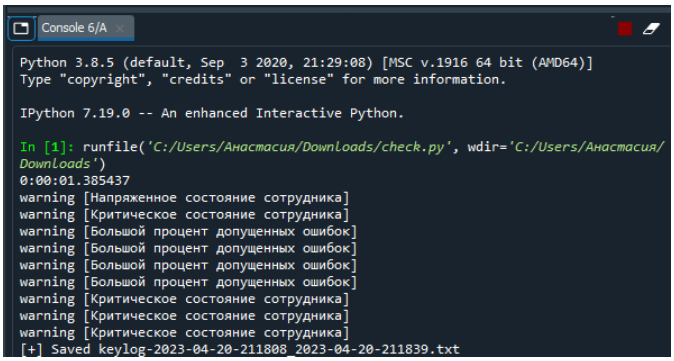

Рис. 2. Предупреждения о нестабильном психоэмоциональном состоянии сотрудника

Результаты проведенных экспериментов показали, что выбранные признаки являются достаточно информативными.

Анализ интервала между нажатиями клавиш в значительной степени связан с обыденностью выполняемых действий. Например, если один и тот же человек обычно печатает с определенным интервалом между нажатиями клавиш, а потом внезапно начинает набирать текст с другим интервалом, это может указывать на то, что он использует клавиатуру необычным способом, например копирует конфиденциальную информацию.

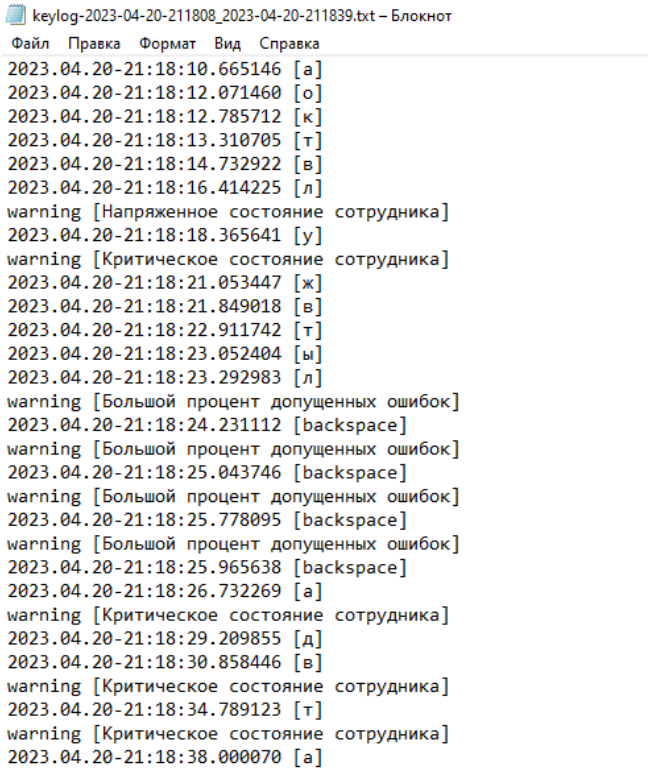
keylog-2023-04-20-211808_2023-04-20-211839.txt – Блокнот
Файл Правка Формат Вид Справка
2023.04.20-21:18:10.665146 [а]
2023.04.20-21:18:12.071460 [о]
2023.04.20-21:18:12.785712 [к]
2023.04.20-21:18:13.310705 [т]
2023.04.20-21:18:14.732922 [в]
2023.04.20-21:18:16.414225 [л]
warning [Напряженное состояние сотрудника]
2023.04.20-21:18:18.365641 [у]
warning [Критическое состояние сотрудника]
2023.04.20-21:18:21.053447 [ж]
2023.04.20-21:18:21.849018 [в]
2023.04.20-21:18:22.911742 [т]
2023.04.20-21:18:23.052404 [ы]
2023.04.20-21:18:23.292983 [л]
warning [Большой процент допущенных ошибок]
2023.04.20-21:18:24.231112 [backspace]
warning [Большой процент допущенных ошибок]
2023.04.20-21:18:25.043746 [backspace]
warning [Большой процент допущенных ошибок]
2023.04.20-21:18:25.778095 [backspace]
warning [Большой процент допущенных ошибок]
2023.04.20-21:18:25.965638 [backspace]
2023.04.20-21:18:26.732269 [а]
warning [Критическое состояние сотрудника]
2023.04.20-21:18:29.209855 [д]
2023.04.20-21:18:30.858446 [в]
warning [Критическое состояние сотрудника]
2023.04.20-21:18:34.789123 [т]
warning [Критическое состояние сотрудника]
2023.04.20-21:18:38.000070 [а]

Рис. 3. Отчет по результатам анализа психоэмоционального состояния сотрудника

Еще одним фактором, который может помочь в выявлении внутренних нарушителей, является количество ошибок при наборе текста. Если человек обычно печатает без ошибок, а потом внезапно начинает делать много ошибок, это может указывать на то, что пользователь нервничает, так как скрывает какие-то свои действия.

Заключение

Оценка психоэмоционального состояния персонала является достаточно значимым инструментом для повышения качества работы организации в области информационной безопасности.

Сопоставление полученных результатов с теоретическим анализом закономерностей воздействия эмоций на поведение человека позволило объяснить психофизиологический механизм влияния отрицательных эмоций на клавиатурное письмо.

Анализ интервала между нажатиями клавиш и количества ошибок может быть полезным инструментом при выявлении внутренних нарушителей. Это связано с тем, что каждый человек имеет свой индивидуальный стиль набора текста на клавиатуре. Анализ этого стиля может помочь в выявлении подозрительных действий.

Безусловно необходимым для обеспечения защиты информации от внутренних нарушителей является использование комплекса организационных и технических мер по обнаружению потенциальных проблем внутри компании. Предлагаемое решение — лишь один из дополнительных инструментов по выявлению потенциальных нарушителей информационной безопасности. Данная методика позволяет своевременно обратить внимание на нестабильное поведение сотрудника, которое в том числе может свидетельствовать и о готовности к совершению им противозаконных действий.

Необходимо отметить, что для выполнения полноценного анализа психоэмоционального состояния человека требуется проведение разноплановых психологических тестов, мониторинг расширенной совокупности параметров и технических индикаторов деятельности сотрудника.

Литература

1. Зайцев, А. С. Исследование проблемы внутреннего нарушителя / А. С. Зайцев, А. А. Малюк // Вестник РГГУ. Серия «Информатика. Защита информации. Математика». 2012. № 14 (94). С. 114–134.

2. Иванов, А. Ю. Классификация нарушителей и угроз безопасности автоматизированной информационной управляющей системы МЧС России / А. Ю. Иванов, М. Ю. Синещук // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2013. № 4. С. 74–79.

3. Дровникова, И. Г. Модель нарушителя в системе безопасности / И. Г. Дровникова, Т. А. Буцынская // Системы безопасности. 2008. № 5. С. 144–147.

4. Поляничко, М. А. Критерии классификации инсайдеров / М. А. Поляничко, А. И. Королев // Естественные и технические науки. 2018. № 9 (123). С. 149–151.

5. Исаева, М. Ф. О внутренних угрозах информационной безопасности // Международный научно-исследовательский журнал. 2019. № 5-1 (83). С. 26–28. DOI: 10.23670/IRJ.2019.83.5.005.

6. Корниенко, А. А. Метод обнаружения инсайдерской деятельности в организации / А. А. Корниенко, М. А. Поляничко // Программные системы и вычислительные методы. 2019. № 1. С. 30–41. DOI: 10.7256/2454-0714.2019.1.29048.

7. Поляничко, М. А. Использование технических индикаторов для выявления инсайдерских угроз // Кибернетика и программирование. 2018. № 6. С. 40–47. DOI: 10.25136/2306-4196.2018.6.27970.

8. Поляничко, М. А. О возможностях применения имитационного моделирования для обнаружения инсайдерских угроз / М. А. Поляничко, А. О. Хазбиев // Естественные и технические науки. 2019. № 1 (127). С. 155–158.

9. Поляничко, М. А. Критерии оценивания эффективности мер противодействия инсайдерской деятельности // Двойные технологии. 2019. № 4 (89). С. 82–85.

10. Epp, C. Identifying Emotional States Using Keystroke Dynamics / C. Epp, M. Lippold, L. R. Mandryk // Proceedings of the 29th Annual CHI Conference on Human Factors in Computing Systems (CHI '11), (Vancouver, Canada, 07–12 May 2011). — Association for Computing Machinery, 2011. — Pp. 715–724. DOI: 10.1145/1978942.1979046.

11. Федюнина, А. П. Выявление характерологических признаков и составление психологического портрета возможного нарушителя и лояльного сотрудника в сфере информационной безопасности // Вестник Астраханского государственного технического университета. 2007. № 4 (39). С. 231–236.

12. Гребенников, Н. Клавиатурные шпионы. Принципы работы и методы обнаружения. Часть I // Securelist — Аналитика и отчеты о киберугрозах «Лаборатории Кас-

перского». — 2007. — 29 марта. URL: http://securelist.ru/keyloggers-part-i/68 (дата обращения 26.04.2023).

13. Гребенников, Н. Клавиатурные шпионы. Варианты реализации кейлоггеров в ОС Windows. Часть II // Securelist — Аналитика и отчеты о киберугрозах «Лаборатории Касперского». — 2007. — 20 апреля. URL: http://securelist.ru/keyloggers-part-ii/77 (дата обращения 26.04.2023).

14. Зайцев, О. Современные клавиатурные шпионы // КомпьютерПресс. 2006. № 5. С. 156–158.

15. Цветкова, А. Д. Криминалистическое исследование компьютерного (клавиатурного) почерка // Электронное приложение к «Российскому юридическому журналу». 2022. № 2. С. 55–65. DOI: 10.34076/22196838_2022_2_55.

DOI: 10.24412/2413-2527-2023-234-50-57

Methodology for Identifying Potential Insiders

PhD S. V. Kornienko, A. V. Pantyukhina
Emperor Alexander I St. Petersburg State Transport University
Saint Petersburg, Russia
sv.diass99@ya.ru, shikhova.nastya43@gmail.com

Abstract. **The article considers an approach to the classification of insiders. Suggestions are presented to identify persons prone to illegal actions (potential insiders) by monitoring their activities and assessing their psychoemotional state. For this purpose, a method of initial assessment of the psychoemotional state of personnel by keyboard handwriting is proposed, implemented in the form of a prototype of a software tool for analyzing the main parameters of keyboard handwriting.**

Keywords: **information security, data security, insider, keyboard handwriting.**

REFERENCES

1. Zaitsev A. S. Malyuk, A. A. Investigation of Information Security Internal Intruder Problem [Issledovanie problemy vnutrennego narushitelya], *RSUH/RGGU Bulletin. Series «Computer Science. Data Protection. Mathematics» [Vestnik RGGU. Seriya «Informatika. Zashchita informatsii. Matematika»]*, 2012, No. 14 (94), Pp. 114–134.

2. Ivanov A. Yu., Sineshchuk M. Yu. Classification of Offenders and Security Threats Aius of the Ministry of Emergency Situations of Russia [Klassifikatsiya narushiteley i ugroz bezopasnosti avtomatizirovannoy informatsionnoy upravlyayushchey sistemy MChS Rossii], *Bulletin of St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia [Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoy protivopozharnoy sluzhby MChS Rossii]*, 2013, No. 4, Pp. 74–79.

3. Drovnikova I. G.., Butsynskaya T. A. The Intruder Model in the Security System [Model narushitelya v sisteme bezopasnosti], *Security and Safety [Sistemy bezopasnosti]*, 2008, No. 5, Pp. 144–147.

4. Polyanichko M. A., Korolev A. I. Criteria for Classification of Insiders [Kriterii klassifikatsii insayderov], *Natural and Technical Sciences [Estestvennye i tekhnicheskie nauki]*, 2018, No. 9 (123), Pp. 149–151.

5. Isaeva M. F. On Internal Information Security Threats [O vnutrennikh ugrozakh informatsionnoy bezopasnosti], *International Research Journal [Mezhdunarodnyy nauchno-issledovatelskiy zhurnal]*, 2019, No. 5-1 (83), Pp. 26–28. DOI: 10.23670/IRJ.2019.83.5.005.

6. Kornienko A. A., Polyanichko M. A. A Method for Insiders Detection in the Organization [Metod obnaruzheniya insayderskoy deyatelnosti v organizatsii], *Software Systems and Computational Methods [Programmnye sistemy i vychislitelnye metody]*, 2019, No. 1, Pp. 30–41. DOI: 10.7256/2454-0714.2019.1.29048.

7. Polyanichko M. A. Using Technical Indicators to Identify Insider Threats [Ispolzovanie tekhnicheskikh indikatorov dlya vyyavleniya insayderskikh ugroz], *Cybernetics and Programming [Kibernetika i programmirovanie]*, 2018, No. 6, Pp. 40–47. DOI: 10.25136/2306-4196.2018.6.27970.

8. Polyanichko M. A., Khazbiev A. O. The problem of Applying Imitation Modelling Insider Threats Detection [O vozmozhnostyakh primeneniya imitatsionnogo modelirovaniya dlya obnaruzheniya insayderskikh ugroz], *Natural and Technical Sciences [Estestvennye i tekhnicheskie nauki]*, 2019, No. 1 (127), Pp. 155–158.

9. Polyanichko M. A. Criteria for Evaluating the Effectiveness of Countermeasures to Insider Activity [Kriterii otsenivaniya effektivnosti mer protivodeystviya insayderskoy deyatelnosti], *Dual Technologies [Dvoynye tekhnologii]*, 2019, No. 4 (89), Pp. 82–85.

10. Epp C., Lippold M., Mandryk L. R. Identifying Emotional States Using Keystroke Dynamics, *Proceedings of the 29th Annual CHI Conference on Human Factors in Computing Systems (CHI '11), Vancouver, Canada, May 07–12, 2011*. Association for Computing Machinery, 2011, Pp. 715–724. DOI: 10.1145/1978942.1979046.

11. Fedyunina A. P. Identification of Characteristic Peculiarities and Making Up a Psychological Portrait of a Possible Lawbreaker and a Loyal Employee in the Sphere of Information Security [Vyyavlenie kharakterologicheskikh priznakov i sostavlenie psikhologicheskogo portreta vozmozhnogo narushitelya i loyalnogo sotrudnika v sfere informatsionnoy bezopasnosti], *Vestnik of Astrakhan State Technical University [Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta]*, 2007, No. 4 (39), Pp. 231-236.

12. Grebennikov N. Keyloggers: How They Work and How to Detect Them (Part 1), *Securelist — Kaspersky`s Threat Research and Reports*. Published online at March 29, 2007. Available at: http://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138 (accessed 26 Apr 2023).

13. Grebennikov N. Keyloggers: Implementing keyloggers in Windows. Part Two, *Securelist — Kaspersky`s Threat Research and Reports*. Published online at April 20, 2007. Available at: http://securelist.com/keyloggers-implementing-keyloggers-in-windows-part-two/36358/ (accessed 26 Apr 2023).

14. Zaitsev O. Modern Keyloggers [Sovremennye klaviaturnye shpiony], *Computer Press [KompyuterPress]*, 2006, No. 5, Pp. 156–158.

15. Tsvetkova A. D. The Forensic Examination of Computer (Keyboard) Handwriting [Kriminalisticheskoe issledovanie kompyuternogo (klaviaturnogo) pocherka], *Electronic Supplement to the Russian Juridical Journal [Elektronnoe prilozhenie k «Rossiyskomu yuridicheskomu zhurnalu»]*, 2022, No. 2, Pp. 55–65. DOI: 10.34076/22196838_2022_2_55.