Рис.7. Карта зоны риска затопления при наводнении(контуры черного цвета), созданная по последствиям наводнения по снимку 2010года и при сравнения со снимком 2018года (AZERSKY).

Заключение

Возможность своевременного прогнозирования чрезвычайных ситуаций по данным дистанционного зондирования и в частности по снимкам AZERSKY является важным условием для принятия предупредительных мер и эффективного планирования работ по устранению последствий наводнений. Обработка данных спутниковой съемки с целью оперативного мониторинга обширных территорий является наиболее актуальной и оптимальной с точки зрения затрат ресурсов и времени для прогноза зон затопления при наводнениях.

1. Джафарова Н.Р. Аэрокосмический мониторинг прибрежных территорий для экологического и социально-экономического картографирования. "Creativity of youth in solving aerospace problems", February readings, 2017, NAA, Baku, February 12-14, 2017, P. 114-118.
2. Геоинформатика: Учеб. Для студ. Вузов / Е.Г.Капралов, А.В.Кошкарёв, В.С.Тикунов и др.; Под ред. В.С.Тикунова. – М.:Издательский центр «Академия», 2005. — 480 с.
3. Spivak L.F., Arkhipkin O.P., Pankratov V.S., Shagárova L.V., Sagatdinova G.N. Technology of monitoring freshets and flooding in western Kazakhstan / Modern problems of remote sensing of the Earth from space. Moscow, 2004. P. 279-285.
4. Чандра А.М., Гош С.К. Дистанционное зондирование и географические информационные системы. Москва: Техносфера, 2008, 312 с.
5. Guliyeva S.H., Badalova A.N., Ismatova Kh.R. Research and prediction of freshets and floods at Kura river by using space images AZERSKY /Materials of III scientifically-practical youth conference with international participation, 2018, NAA, Baku, February 12-14, 2018, P. 114-118.

Мамырбаев О.Ж.^{1,2}, Othman M.³, Ахмедиярова А.Т.¹, Кыдырбекова А.С.^{1,2}
Конфиденциальность и безопасность организации от инсайдерских атак с использованием голосовой биометрики

¹Институт Информационных и Вычислительных Технологий

²Казахский национальный университет им. Аль-Фараби
 (Казахстан, Алматы)

³Университета Путра
 (Малайзия)

doi:10.18411/sciencepublic-12-06-2020-04

idsp: sciencepublic-12-06-2020-04

Аннотация

В статье рассмотрены современные инсайдерские атаки, борьба с которыми актуальна сегодня не только для частных и корпоративных интересов, но и в целом для

решения вопросов национальной безопасности. Авторами отмечены наиболее распространенные сегодня виды инсайдерских атак, представляющие повышенную опасность для организации. Отмечены основные направления и методы противодействия на инсайдерские атаки на современном этапе. В этом исследовании предлагается новый подход для эффективной защиты от инсайдеров обеспечив контроль с помощью голосовой биометрики. Голосовая биометрическая системы могут обеспечить непрерывную аутентификацию пользователя с высоким уровнем эффективности.

Ключевые слова: кибербезопасность, внутренняя угроза, голосовая биометрия, гнолосовая биометрия

Введение

Киберпреступность остается постоянно меняющейся глобальной проблемой. По мере того, как частота нападений на организации и нацию растет, некоторые считают, что мы «оцепенели от огромного объема и ускорения киберугроз» [1]. Общая стоимость киберпреступлений продолжает расти год за годом. По мере роста числа и стоимости глобальных киберпреступлений одно событие наносит серьезный удар организациям - атака инсайдеров. Инсайдерские атаки являются одним из главных киберпреступлений, затрагивающих бизнес. Организации сталкиваются с постоянной проблемой, выявляя злоумышленников и внешних злоумышленников, которые скомпрометировали законные учетные данные и затем маскируются под инсайдеров [2]. Некоторые указывают на то, что «независимо от того, насколько хороши защитные механизмы организации по периметру, в конечном итоге они будут скомпрометированы или преданы изнутри» [2]. Инсайдерские атаки также очень дорогостоящие, требующие времени и денег для восстановления после первоначального возникновения. Затраты, связанные с устранением последствий внутренних угроз, сильно сказываются на бюджете бизнеса. Хотя небольшое количество академических исследований с использованием реальных условий подчеркивает необходимость дополнительных широкомасштабных тематических исследований. Отсутствие отраслевых стандартов для обработки биометрических данных также подчеркивает низкий уровень зрелости биометрических систем. Кроме того, законы о конфиденциальности расходятся по всему миру в отношении использования биометрических данных. Отсутствие стандартизации делает судебные процессы серьезной проблемой для организаций, которые могут захотеть внедрить биометрические системы.

Организации считают, что внутренние угрозы трудно контролировать. Согласно докладу об угрозе для инсайдеров (2018 г.), «большинству респондентов (66%) труднее выявлять и предотвращать инсайдерские атаки, чем внешние кибератаки» (стр. 18). В нем также указывается, что «менее половины всех организаций (42%) имеют надлежащие средства контроля для предотвращения атаки инсайдеров». В нем подчеркиваются некоторые ключевые причины трудностей в обнаружении и предотвращении атак: инсайдеры имеют ключевой доступ к сетевым системам, увеличение числа приложений, уязвимых к утечкам данных, таких как социальные сети и облачные приложения, и огромное количество данных, покидающих защищенные системы. Внутренние угрозы - это проблема не только частного сектора, но также представляют угрозу для местных и национальных правительств. Правительства во всем мире усиливают свою политику по борьбе с внутренними угрозами. Одной из ключевых проблем, охватываемых политиками обнаружения, является проблема атрибуции. Атрибуция инсайдерских киберпреступлений страдает из-за отсутствия адекватного обнаружения угроз. Голосовая биометрия - это изменение мышления в области информационной безопасности, которое предлагает новое поколение решений по информационной безопасности, ориентированных на человека. Голосовая аналитика

предоставит механизм для проверки действий пользователя и определения намерений, злонамеренных или доброкачественных.

Методы аутентификации

Текущие методы аутентификации пользователей представляют серьезные проблемы, когда речь идет об угрозе изнутри. К серьезным угрозам организациям относятся авторизованные учетные данные, используемые «злонамеренными инсайдерами и скрытными атаками, которые позволяют противникам маскироваться под инсайдеров» [2]. Даже при том, что большинство организаций имеют надежные меры предотвращения, большинство попыток предотвратить несанкционированный доступ в конечном итоге потерпят неудачу, предоставив скомпрометированным учетным данным свободный доступ к системам [2]. Как указано Collins et al. [3], «независимо от того, насколько бдительна организация против внутренней угрозы, если учетные записи организации могут быть скомпрометированы, у инсайдеров есть возможность обойти механизмы предотвращения атак» (стр.67). Учетные данные пользователя постоянно находятся под угрозой. Коллинз и соавт. [3] заявляют, что злоумышленники имеют много возможностей получить пароли. Эти возможности включают такие методы, как социальная инженерия, открытый обмен паролями и пароли, хранящиеся в текстовых файлах на компьютерах. Они также утверждают, что электронные письма на компьютерах, заметки в поле зрения и «просмотр с плеча» или наблюдение за тем, как пользователь вводит свой пароль, являются дополнительными векторами атак, способствующими взлому учетных данных. Как отмечают Song, Salem, Hershkop & Stolfo [4], доверие является фундаментальным фактором, на котором «основываются фундаментальные механизмы безопасности, направленные на предотвращение неправильного использования системы, утечку данных и применение политик безопасности» (стр.52). Ядро системы безопасности состоит из трех взаимосвязанных концепций: идентификация, аутентификация и авторизация [5]. Идентификация - это передача идентификатора пользователя системе безопасности, обычно предоставляемая в форме некоторого идентификатора пользователя, такого как адрес электронной почты или идентификатор единого входа [5]. Затем пользователь предоставляет подтверждение своей личности путем аутентификации (например, с помощью пароля), доказывая, что он является тем, на кого он претендует [5]. Авторизация - это последний шаг, предоставление привилегий аутентифицированному пользователю [5]. Чтобы системы аутентификации были полезны, они должны предоставить ответы на два важных вопроса: 1) кто является пользователем? 2) действительно ли пользователь, кем он себя представляет [5]. Уровень доверия в системе аутентификации зависит от степени доверия к используемым методам аутентификации. Таким образом, метод проверки не может быть доверенным, если методы проверки подлинности не являются полностью доверенными [5].

Процесс объединения нескольких факторов в единый процесс аутентификации называется многофакторной аутентификацией (MFA). Чем выше число факторов, используемых в системе аутентификации, тем сильнее эта система. «Реализации, использующие два разных фактора, как правило, считаются более сильными, чем те, которые используют только один фактор» [6].

Биометрические системы могут быть разбиты на две модальности: физиологическую и поведенческую. Каждый режим имеет свои преимущества и недостатки в зависимости от требований безопасности системы. Биометрические системы аутентификации используют физиологические или поведенческие черты пользователя. Физиологические черты - это особенности, с которыми мы рождаемся, а поведенческие черты - это особенности, которые мы изучаем - результат нашего взаимодействия с окружающей средой и природой [7]. Проверка состоит из измерений

биометрических характеристик человека [7]. Эти черты являются весьма отличительными, что позволяет их уникальность идентифицировать человека [8].

Системы, основанные на биометрии, не имеют общих проблем, связанных с паролями и системами на основе токенов, аспектом запоминания чего-либо. Как таковые, они предлагают наиболее безопасный и удобный подход [9]. «Биометрические подходы, основанные на физиологии, обеспечивают более надежную защиту, поскольку они очень уникальны для пользователей и их трудно воспроизвести» [7]. Показатели эффективности, используемые исследователями для биометрических систем, включают показатель ложных отклонений (FRR), коэффициент ложных приемов (FAR) и равный коэффициент ошибок (EER). Они определены Teh et al. [8] как:

Коэффициент ложного отклонения (FRR) относится к процентному соотношению между ложно отклоненными подлинными пользователями и общим числом подлинных пользователей, обращающихся к системе. Более низкий FRR подразумевает меньшее отклонение и более легкий доступ истинным пользователем. Коэффициент ложного принятия (FAR) - это процентное соотношение между ложно принятыми неавторизованными пользователями к общему количеству мошенников, обращающихся к системе. Меньший FAR указывает на меньшее количество принятых самозванцев. Равная частота ошибок (EER) используется для определения общей точности, а также для сравнительного измерения с другими системами. (стр. 4) Кроме того, EER - это точка, в которой частота ложных отклонений (FRR) и частота ложных утверждений (FAR) равны. Системы с более низким EER считаются более точными и точными.

Системы аутентификации на основе голоса являются одной из самых успешных биологических систем безопасности. Коллекционирование - сбор голосовых биометрических данных является относительно простым и ненавязчивым для пользователя. В некоторых случаях пользователь может даже не знать, что происходит сбор данных. Процесс сбора данных полностью автоматизирован и стоит очень дешево.

Основываясь на возможностях, которые демонстрируют голосовые биометрии, они полезны во многих отраслях. Голосовая биометрия в основном хорошо подходит для проверки взаимодействия конечных пользователей с любыми устройствами ввода, такими как компьютеры, мобильные телефоны и т.д.

Голосовая биометрия - это метод аутентификации, который может предоставить недорогой, малозаметный вариант для развертывания систем CUA в организациях. Голосовая биометрия - это область биометрии, которая еще только зарождается и набирает обороты в качестве опции для аутентификации.

Безопасность.

Безопасность всей системы биометрической аутентификации является критической проблемой. Как указывает Грант [10], в отличие от предметов, основанных на знаниях или владении, после кражи биометрические данные никогда не могут быть отозваны или заменены. Jain et al. [11] подчеркивают, что «вопросы безопасности биометрической системы и конфиденциальности пользователей являются важными проблемами общественного восприятия, которые могут помешать успеху развертывания биометрической системы, если они не будут рассмотрены всесторонне» (стр. 99). Vielhauer, Dittmann и Katzenbeisser [12] отмечают, что «поскольку цифровые биометрические данные можно легко копировать без потери информации, манипулировать ими по желанию или подделывать без заметных следов, для противодействия этим угрозам необходимы решения безопасности». Подобно компьютерным и сетевым системам, важно, чтобы биометрические системы следовали требованиям безопасности конфиденциальности, целостности, подлинности,

неоспоримости и доступности [12]. Пять требований, поскольку они относятся к биометрии, согласно Vielhauer et al. [12] являются:

Конфиденциальность. Целостность. Подлинность. Безотказность. Доступность.

Безопасность во всем потоке биометрической обработки имеет огромное значение. Поток обработки обычно состоит из двух этапов. Первый этап, на котором формируются биометрические шаблоны, - это этап регистрации. «На этапе регистрации биометрическая система получает биометрический признак человека, извлекает из него набор характерных признаков и сохраняет извлеченный набор признаков в базе данных (часто называемый шаблоном) вместе с идентификатором, связывающим набор признаков с человеком» [11]. Второй этап, где происходит идентификация или аутентификация, - это этап распознавания. «На этапе распознавания система снова получает биометрический признак человека, извлекает из него набор функций и сравнивает этот набор функций с шаблонами в базе данных для определения соответствия или проверки заявленной личности» [11].

На этапе регистрации в некоторых местах возможны атаки на биометрические данные. Как видно из модели регистрации, рисунок 1, существует пять возможных точек атаки.

Рисунок 1. Точки уязвимости в биометрической модели регистрации.

Эти точки уязвимости при регистрации, как утверждают Shin, Seto и Shimizu [13], следующие:

1. Атака на сенсорный ввод фальшивых биометрических данных: спуфинг - это кража чужого идентификатора пользователя и пароля и притворство человека, вошедшего в сеть.

2. Атака на передачу данных с датчика на обработку извлечения признаков: биометрические данные, полученные с датчика, могут быть заменены атакой на сеть или шину.

3. Выполнение замены извлеченных данных объекта: вместо фактического объекта устанавливается произвольный объект.

4. Незаконное преобразование данных тела: данные тела могут быть заменены поддельными данными. Поскольку процессы извлечения признаков и сопоставления выполняются в одной и той же системе, выполнить эту атаку очень сложно.

5. Подделка хранимых данных. Незаконный пользователь может фальсифицировать данные шаблона, хранящиеся в базе данных, таким образом, что незаконный пользователь получает юридическое подтверждение и получает доступ, в то время как законный пользователь получает незаконное подтверждение и ему запрещается доступ.

Фаза распознавания страдает от тех же проблем во время процесса биометрического сбора, а именно: точки уязвимости 1,2 и 3. Кроме того, как видно на рисунке 2, при реализации процесса сопоставления возможны еще пять точек атаки.

Рисунок 2. Точки уязвимости в модели биометрического распознавания.

Эти точки уязвимости распознавания, как заявлено Shin et al.[13], являются:

6. Повторный ввод сохраненных биометрических данных: биометрические данные, которые остаются на сенсорных устройствах, могут автоматически вводиться снова без ввода данных пользователем.

7. Атака на передачу из хранилища данных шаблона в обработку сопоставления. Когда данные шаблона выбираются из базы данных для сопоставления с данными идентификации, данные шаблона могут быть незаконно изменены в канале связи.

8. Замена порогового значения: политика суждения может быть незаконно изменена, и пороговое значение для степени сходства может быть установлено на новое значение, чтобы получить ожидаемый результат.

9. Атака на процесс сопоставления: процесс сопоставления может быть атакован, и результат сопоставления может быть заменен произвольной оценкой.

10. Подстановка данных окончательного решения: результат оценки аутентификации может быть заменен.

Существует несколько вопросов, которые следует учитывать организациям при изучении использования биометрической аутентификации. Две важные проблемы, связанные с безопасностью, включают уязвимости биометрической обработки и хранение биометрических шаблонов. Поток обработки, состоящий из фазы регистрации, когда система узнает о пользователе, и фазы распознавания, где происходит проверка входящих биометрических данных по существующим шаблонам, имеют несколько точек уязвимости. Атаки происходят в этих точках с помощью таких методов, как подмена датчика, атаки с переносом данных, атаки с повторением, изменение политики оценки и манипулирование данными шаблона.

Место хранения. Как было показано в предыдущем разделе, безопасность хранения данных, как тип хранимых данных, так и местонахождение этих данных: является ключевой проблемой при разработке биометрической системы. Как указывает Грант [10], нарушение ОРМ выявило более 5,6 миллиона необработанных отпечатков пальцев. «Технологии защиты шаблонов направлены на предотвращение прогнозирования необработанных биометрических данных из шаблонов и предотвращение повторного использования утечек шаблонов неавторизованными пользователями» [13]. «Защита биометрических шаблонов является сложной проблемой и остается одним из главных препятствий на пути широкого распространения биометрической аутентификации» [15].

Выводы

Голосовая биометрия может предоставить организациям средства для улучшения существующих систем аутентификации для обеспечения дополнительной защиты от внутренних угроз. Технология получения и различения поведенческих биометрических признаков была успешно доказана. Хотя технология доказала свою эффективность, существует много проблемных вопросов, которые возникают у систем

биометрической аутентификации. Конфиденциальность, по-видимому, является проблемой номер один, которая делает внедрение системы поведенческой биометрической аутентификации неудачной. Юридические проблемы, связанные с использованием и хранением биометрических данных, являются дополнительными рисками, которые организации должны учитывать при определении того, является ли биометрическая система жизнеспособной для их нужд. Поскольку в мире существует так много разных законов о биометрии, система, внедренная в одной стране, может вступать в противоречие с существующими нормативными актами в другой. Необходимо провести дополнительные исследования, чтобы изучить способы использования голосовых биометрических признаков, которые не нарушают законы о конфиденциальности. Еще одна проблема, связанная с голосовыми биометриками, заключается в их естественной тенденции меняться со временем.

Кроме того, отсутствие отраслевых стандартов в отношении того, как биометрия должна регистрироваться, храниться и внедряться, является еще одной проблемой, которую должны рассмотреть организации. Поток биометрического захвата чреват уязвимыми точками, открытыми для атаки, а проблема хранения имеет множество аспектов. Где и как биометрические шаблоны хранятся и защищаются, - это разнообразная тема, освещаемая в многочисленных технических документах и биометрических журналах. Чтобы голосовая биометрия получила широкое распространение на корпоративном рынке в качестве жизнеспособного метода аутентификации, необходимо провести дополнительные исследования в реальном мире, чтобы поддержать создание отраслевых стандартов.

Благодарность.

Данная работа была поддержана Министерством образования и науки Республики Казахстан. IRN AP05131207 Разработка технологий мультязычного автоматического распознавания речи с использованием глубоких нейронных сетей.

1. Wood P., Nahorney B., Chandrasekar K., Wallace S., & Haley K. (2016, апрель). Отчет Symantec об угрозе интернет-безопасность. <https://www.symantec.com/21-2016-en.pdf>.
2. Voris J., Jermyn, J., Boggs N. & Stolfo S. (2015, апрель). Материалы восьмого европейского семинара по системной безопасности.
3. Collins M., Theis M., Trzeciak R., Strozer J., Clark J., Costa D., Moore A. (2016). Руководство по здравому смыслу для уменьшения внутренних угроз. 5-е издание (CMU / SEI-2016-TR-015). Получено с <http://resources.sei.cmu.edu/library/asset-view.cfm?>
4. Song Y., Salem M., Hershkop S., & Stolfo S. (2013, май). Биометрия поведения пользователя на уровне системы с использованием функций Фишера и моделей гауссовых смесей. Семинары по безопасности и конфиденциальности (SPW), 2013 IEEE., С. 52-59.
5. Idrus S., Cherrier E., Rosenberger C., & Schwartzmann, J. (2013). Обзор методов аутентификации. Австралийский журнал фундаментальных и прикладных наук, 7 (5), 95-107. Инсайдерская информация об угрозе. (2016).
6. Grassi, Garcia & Fenton Дж. (2017, 30 января). ПРОЕКТ NIST специальная публикация 800-63-3. Получено с <https://pages.nist.gov/800-63-3/sp800-63-3.html>.
7. Саид К. (2017). Новые направления в поведенческой биометрии. Бока-Ратон, штат Флорида: Тейлор и Фрэнсис Групп, ООО.
8. Teh P., Teoh A. & Yue S. (2013, 8 29). Обзор динамики нажатия клавиш биометрии. (Ф. Фернандес де Вега и Д. Ян, ред.) The Scientific World Journal, 2013.
9. Saevanee Н. (2014). Непрерывная аутентификация пользователя с использованием мультимодальной биометрии. Получено с <https://pearl.plymouth.ac.uk/bitstream/handle/10026>.
10. Грант Дж. (2016). Безопасная биометрическая аутентификация: фундаментальный строительный блок для достижения надежных облачных сервисов. Корпорация Майкрософт.
11. Jain A., Nandakumar K. & Ross A. (2016). 50 лет биометрических исследований: достижения, проблемы и возможности, 80-105.

12. Vielhauer C., Dittmann J. & Katzenbeisser S. (2013). Вопросы проектирования безопасных биометрических систем и биометрии в зашифрованном домене. В П. Кампизи, Безопасность и конфиденциальность в биометрии (стр. 25-43). Лондон: Спрингер.
13. Shin S., Seto Y. & Shimizu S. (2016). Исследование отменяемой биометрии в повышении безопасности системы биометрической аутентификации с использованием анализа дерева отказов. Международный журнал аффективной инженерии, 351-359.
14. Lourdes C. & Tibor K. (2016). Получение биометрической информации, вопросы конфиденциальности на рабочем месте: мониторинг и безопасность. Материалы 8-го Международного Инженерного Симпозиума в Банки.
15. Roeschlin M., Sluganovic I., Martinovic I., Tsudik G., & Rasmussen K. (2016, 24 октября). Генерация секретных ключей из биометрических измерений сопротивления тела. WPES '16 (стр. 59-69). Вена, Австрия: ACM. DOI: 10.1145 / 2994620,2994626

Прудий А.В., Соломыкин П.В., Бондаренко И.А., Прохоров А.О.
Концепция цифрового двойника процесса, бестраншейной прокладки
коммуникаций

*Шахтинский автодорожный институт (филиал) Южно-Российского государственного политехнического Университета (НПИ) имени М.И. Платова
(Россия, Новочеркасск)*

doi:10.18411/sciencepublic-12-06-2020-05

idsp: sciencepublic-12-06-2020-05

Аннотация

В статье представлена концепция цифрового двойника процесса бестраншейной прокладки коммуникаций. В работе рассмотрены основные положения, анализ внедрения системы и её оптимизирование. Также проанализирована концепция цифровых двойников на сегодняшний день.

Ключевые слова: бестраншейная прокладка, горизонтальное направленное бурение, инженерные коммуникации, подземное строительство, городское подземное пространство, грунт, физико-механические свойства, методы прокладки, скважина, мониторинг, алгоритмы управления.

Abstract

The article presents the concept of a digital double of the process of trenchless laying of communications. The paper considers the main provisions, analysis of the implementation of the system and its optimization. The concept of digital doubles for today is also analyzed.

Keywords: trenchless pipelaying, horizontal directional drilling, infrastructure, underground development, utility structure, subgrade, soil test, pipe-jacking, pipe pushing, down hole, geotechnical monitoring, control algorithms.

Распоряжением правительства РФ от 28 июля 2017 г. №1632-р утверждена Программа «Цифровая экономика Российской Федерации» в целях реализации Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" настоящая Программа направлена на создание условий для развития общества знаний в Российской Федерации, повышение благосостояния и качества жизни граждан нашей страны путем повышения доступности и качества товаров и услуг, произведенных в цифровой экономике с использованием современных цифровых технологий, повышения степени информированности и цифровой грамотности, улучшения доступности и качества государственных услуг для граждан, а также безопасности как внутри страны, так и за ее пределами.

В рамках реализации данной программы планируется повсеместное внедрение цифровых двойников. Цифровой двойник (англ. *Digital Twin*) - цифровая копия