УДК 004.7.056.5 Вестник УрФО № 4(46) / 2022, с. 68–75

Захаров А.А., Шабалин А.М., Ханбеков Ш.И., Джалилзода Д.Б., Пономарев К.Ю

DOI: 10.14529/secur220408

ПРИМЕНЕНИЕ ГОЛОСОВОГО ПОМОЩНИКА В КАЧЕСТВЕ ВИРТУАЛЬНОГО КОНСУЛЬТАНТА ДЛЯ АДМИНИСТРИРОВАНИЯ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ[1]

В статье представлена технология создания интеллектуального голосового помощника для обеспечения информационной безопасности сетевой инфраструктуры локальных компьютерных сетей. Потребность в таком помощнике может возникнуть в организациях, предоставляющих хостинг небольшим сетевым инфраструктурам, например, для домашних телемедицинских стационаров или IT-стартапам, для которых вопросы, связанные с защитой информации, являются важными, а также при обучении студентов технологиям защиты сетевой инфраструктуры. Полученные результаты также имеют практическую значимость для решения задач обеспечения информационной безопасности лицами, совмещающими выполнение обязанностей администратора сети (NetOps) и администратора защиты (SecOps).

Ключевые слова: *виртуальный голосовой помощник, онтологии, распознавание речи, сетевая безопасность, системное администрирование, Cisco.*

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-47-720005

Zakharov A.A., Shabalin A.M., Khanbekov Sh.I., Dzhalilzoda D.B., Ponomarev K. Y.

USING A VOICE ASSISTANT AS A VIRTUAL CONSULTANT FOR ADMINISTRATION OF THE SECURITY OF THE LOCAL COMPUTER NETWORK INFRASTRUCTURE

The article presents the technology to create intellectual voice assistant for the tasks related to providing local area network information security. This technology may be found useful by organizations, offering hosting to small area network infrastructures, e.g. home health care telemedicine or IT-startups aimed at information security, or when teaching students how to protect the network infrastructure. The results obtained in this research also provide practical value in solving information security related tasks for employees occupied with network operations (NetOps) and security operations (SecOps) simultaneously.

Keywords: *virtual voice assistant, ontologies, speech recognition, network security, system administration, Cisco.*

Решение практических проблем обеспечения информационной безопасности (ИБ) системными администраторами во многом опирается на многолетний опыт работы с цифровой информацией, создающей следующие потенциальные риски:

• информация может быть раскрыта (конфиденциальность скомпрометирована);

• информация может быть модифицирована (целостность нарушена);

• информация может быть уничтожена или потеряна (доступность нарушена).

Указанные риски наносят ущерб как напрямую, непосредственно снижая стоимость цифрового актива, так и косвенно - ухудшая репутацию и приводя к юридическим последствиям. Организация может управлять рисками в повседневной деятельности. Стоимость ущерба от события риска ИБ обычно оценивается как произведение вероятности неблагоприятного события и отрицательной суммы стоимости ликвидации его последствий, происходящих в течение конкретного временного периода. Обычно мерой стоимости риска являются годовые убытки (Annual Loss Expectance, ALE). Ожидаемую стоимость ущерба можно уменьшить, например, за счет его страхования или снижения вероятности возникновения неблагоприятного события, а также, если событие произошло, путем минимизации последствий. Это позволяет определить ИБ как управленческий процесс, цель которого заключается в управлении (минимизации стоимости) информационными рисками для бизнеса.

В контексте решения задач обеспечения ИБ компьютерных сетей дополнительную сложность составляет то, что информация о частоте возникновения нежелательных явлений и об их последствиях обычно скрывается. То есть сведений об эффективности мер, которые можно предпринимать для предотвращения нежелательных явлений и/или смягчения последствий, обычно недостаточно или вообще не имеется, поскольку у организаций с проблемами в области ИБ отсутствуют мотивы для сообщения о них. При этом имеется множество стимулов для замалчивания этой информации. В конечном счете все это затрудняет оценку эффективности тех мер, которые в идеале должны обеспечить:

1) защиту телекоммуникационного оборудования и оконечных устройств (маршрутизаторов, коммутаторов, межсетевых экранов, серверов);

2) соблюдение требований регулятора и корпоративного регламента;

3) защиту от несанкционированного внутреннего или внешнего доступа к информации разной степени конфиденциальности (коммерческая тайна, персональные данные или бухгалтерская информация).

Условно, с точки зрения объектов защиты, информационную сеть можно разделить на две составляющие: 1) операционные системы, прикладное программное обеспечение и данные на хостах и серверах; 2) коммуникационная сеть для информационного взаимодействия внутренних и внешних пользователей (маршрутизаторы, коммутаторы и линии связи). Отметим, что по сравнению с сетевым оборудованием, операционные системы и прикладное программное обеспечение обновляются чаще, например, вследствие появления новых версий, тогда как коммуникационная сеть достаточно стабильна. Это послужило предпосылкой развития двух подходов к организации и поддержке безопасности информационной сети.

В том, что касается операционных систем и прикладного программного обеспечения на конечных устройствах как объектов защиты, необходимо отметить, что в настоящее время используются постоянно актуализируемые базы и одновременно платформ для сбора и распространения информации об уязвимостях. Базы содержат описания выявленных уязвимостей, оценку потенциального воздействия и (при наличии) способы их устранения. Можно выделить по крайней мере шесть популярных и поддерживаемых в актуальном состоянии подобных баз.

1. Common Vulnerabilities and Exposures (CVE) [1]. База хранит данные об общеизвестных уязвимостях информационной безопасности. Предназначена для применения в системах обнаружения и/или предотвращения атак, сканерах безопасности, при разработке сигнатурных правилах.

2. Exploit Database (ED) [2]. В данной базе реализован альтернативный подход к информации об уязвимостях программного обеспечения, а именно, осуществляется регистрация сценариев эксплуатации эксплойтов. Также в базе представлены примеры эксплуатации уязвимости.

3. National Vulnerability Database (NVD) [3]. База опирается на стандарты протокола (Security Content Automation Protocol – SCAP), которые определяют потенциальные уязвимости программного кода и его некорректные конфигурации.

4. Flexera – Secunia Advisory and Vulnerability Database SAaVD [4]. База обобщает доступную информацию об обнаруженных угрозах и уязвимостях ПО на основе агрегации данных из публичных источников.

5. Vulnerability Notes Database (VND) [5]. База агрегирует информацию о множестве сходных уязвимостей для определенных типов программного обеспечения.

6. Банк данных угроз безопасности информации «ФСТЭК России» [6]. Данная база считается ключевой в РФ. Принципиально важно, что «ФСТЭК России» поддерживает собственный реестр известных угроз информационной безопасности и уязвимостей программного обеспечения с 2014 года.

Определенная стабильность коммуникационной сети создает специфические условия для обеспечения ИБ. А именно, для настройки безопасности непосредственно на сетевых устройствах представляется целесообразным определить набор онтологий, связанных с безопасностью, например, NRL [7, 8] в качестве точного описания концепций безопасности информационной сети на различных уровнях детализации. Использование онтологий как спецификаций настройки безопасности позволяет создать базу семантических выражений для конфигурирования сетевого оборудования [9-11], а дополнительным преимуществом данного подхода является возможность анализа, накопления и повторного применения знаний о настройке сетевой безопасности, в том числе и в автоматическом режиме с помощью специализированных программных продуктов.

Отметим, что результатом использования онтологий в нашем случае является не только анализ ситуации с уровнем защищенности конкретной сети, но и создание базы знаний, выступающей в качестве одного из основных компонентов интеллектуального программного обеспечения для интерактивного администрирования с помощью голосового помощника [12]. Таким образом, цель настоящего исследования заключается в проектировании и разработке на основе онтологического подхода интеллектуального голосового помощника для обеспечения информационной

безопасности сетевой инфраструктуры локальных компьютерных сетей.

Прототип кроссплатформенного программного решения «NEVA (Network Engineer Voice Assistant)» (Голосовой Помощник Сетевого Инженера) содержит голосовой (VUI) и графический (GUI) интерфейсы, взаимодействующие друг с другом через специальный программный интерфейс (API), запускаемый на рабочей станции системного администратора, который служит связующим звеном всех программных компонентов (модулей) голосового помощника и предоставляет приложению доступ к компьютерной сети организации.

Функциональные возможности голосового помощника распределены между его модулями. Архитектура приложения представлена на рисунке 1.

За синтез входящей текстовой информа-

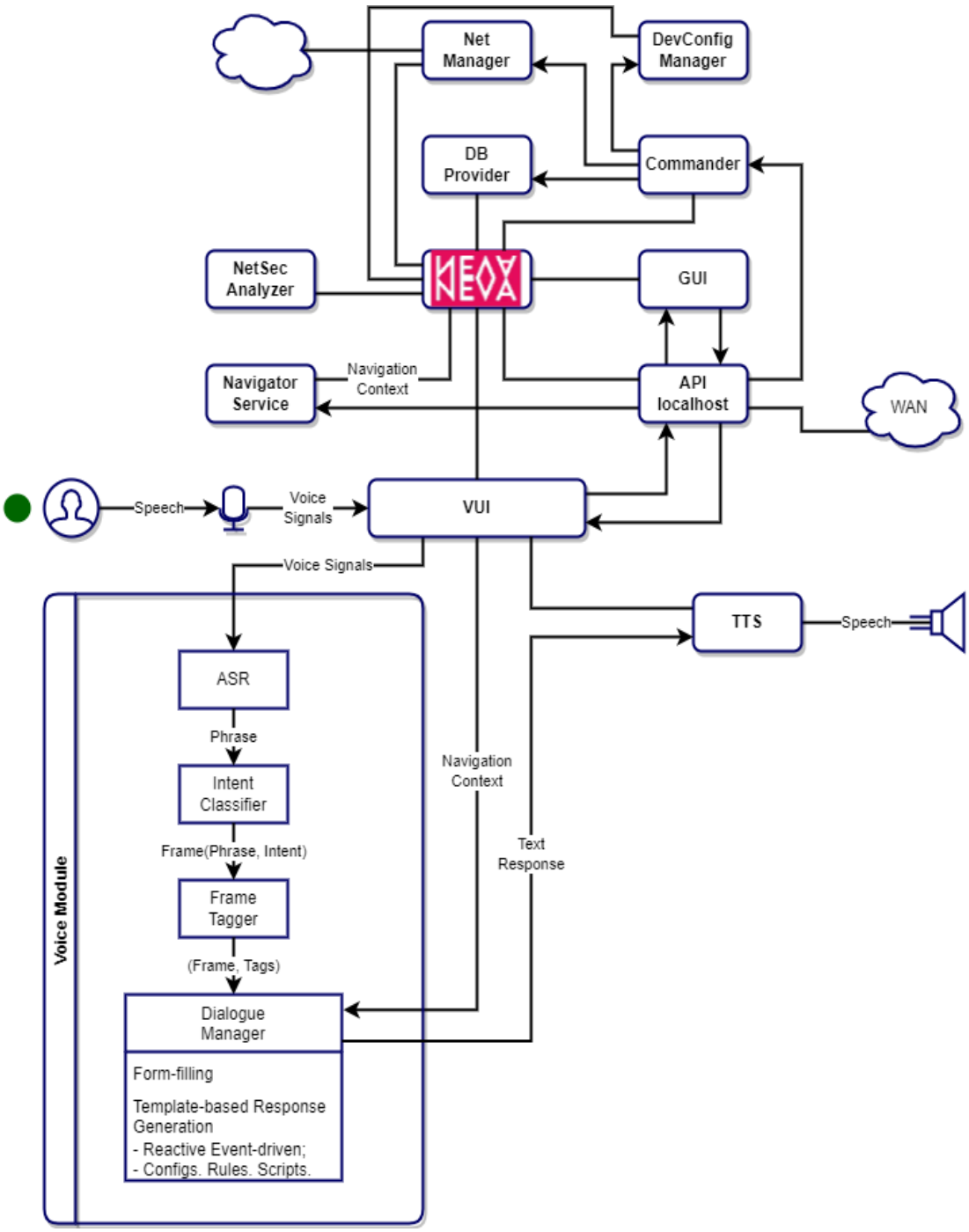

Рис. 1. Архитектура виртуального голосового помощника

ции в речь и последующее озвучивание отвечает сервис «TTS» (Text-to-Speech). Следует отметить, что существует потребность в предоставлении пользователю возможности регулирования скорости озвучивания информации.

Графический интерфейс служит для визуализации сведений, с которыми работают и программа, и системный администратор. Интерфейс состоит из двух частей: основного окна и окна диалога. Окно диалога показывает взаимодействие системного администратора с голосовым помощником (в привычном и удобном для восприятия пользователя виде), а основное окно отвечает за предоставление иной информации.

В приложении присутствует также сервис навигации (Navigator Service), хранящий сведения о контексте происходящих событий и выполняющихся процессов, которые предоставлены системным администратором или операционной системой и которыми руководствуются модули приложения в ходе работы программы (в том числе модули, отвечающие за процессы принятия решений).

За сетевое взаимодействие с коммуникационными устройствами компьютерной сети отвечает модуль «Net Manager» или «Менеджер Сети», позволяющий управлять сетевым оборудованием подключенной компьютерной сети через специальные консольные команды, перечень которых зависит от установленной операционной системы на сетевом устройстве. Модуль также взаимодействует (при необходимости) с конфигурационными и иными файлами, хранящимися в памяти сетевых устройств, через модуль «DevConfig Manager» или «Менеджер Настроек Устройств» для получения сведений по решению актуальных задач.

За принятие решений отвечает модуль «Commander» или «Командующий Модуль», которому на вход подаются все необходимые данные для инициализации той или иной операции.

Онтологии по настройке определенных технологий размещаются в базах данных, которые хранятся локально или централизованно на выделенных серверах в виде таблиц данных. Приложение работает с этими данными в формате JSON через сериализацию объектов, предоставляемых системе управления базами данных (СУБД). Нами рекомендуется использование свободной объектно-реляционной СУБД «PostgreSQL», которая имеет широкий спектр возможностей. Мостом между СУБД и компонентами приложения служит модуль «DB Provider» или «Провайдер Баз Данных». Онтологии состоят из перечня правил, программных сценариев, справочной информации и ссылок на входные шлюзы для взаимодействия с собственными анализирующими средствами.

За предоставление пользователю сведений рекомендательного характера на основе анализа активных конфигураций коммуникационных устройств, подключенных к компьютерной сети, отвечает модуль «NetSec Analyzer», или «Модуль Анализа Безопасности Сети», в котором дополнительно предусмотрена возможность анализа степени защищенности сети путем применения ряда соответствующих инструментов с открытым исходным кодом (Open Source) от сторонних производителей (Third-Party), а также – собственные средства анализа. Кроме того, данный модуль руководствуется онтологиями по безопасной настройке сетевых технологий, обеспечиваемыми модулем «DB Provider».

В качестве примера нами рассматривается алгоритм настройки безопасности протокола SSH для работы системного администратора в локальной сети [13]. Предполагается, что в модельной компьютерной сети выполнены следующие минимальные настройки:

- все узлы в сети имеют IP-связность;
- на коммутационных устройствах предварительно настроен протокол telnet.

Моделируемая топология в среде эмуляции GNS3 компьютерной сети, построенной на коммуникационном оборудовании компании Cisco, представлена на рисунке 2.

Программа реагирует на команды, начинающиеся с обращения: «Нева, …». Так, при словах системного администратора – «Нева, включи поддержку SSH версии 2» – сначала речь передается на службе автоматического распознавания речи (Automatic Speech Recognition, ASR), которая потом превращает его в текст: «Нева, включи поддержку эсэсаш версии два».

Далее данный текст попадает в сервис «Классификатор интентов», задача которого – определить «намерения» пользователя относительно выполнения их программой. Классификатор интентов – машинообучаемая сущность, для которой заранее определяются все ключевые триггерные фразы, помогающие классифицировать намерение пользователя. Создаются определенные ключевые ка-

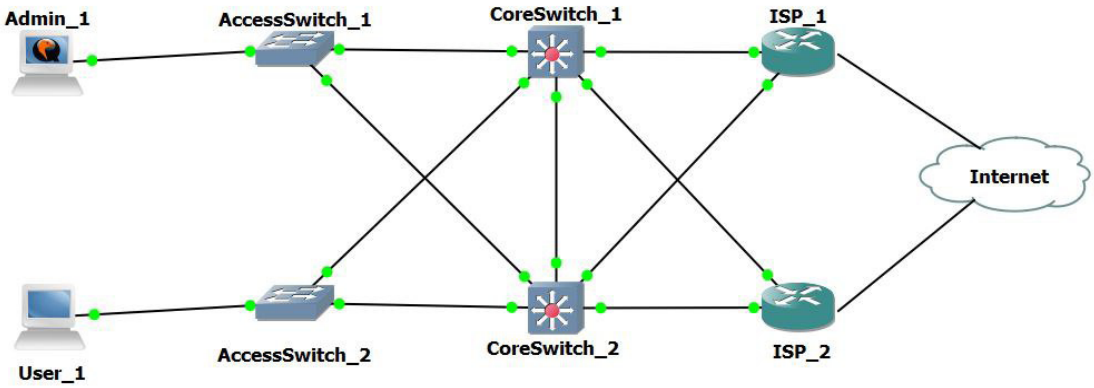

Рис. 2. Топология компьютерной сети

Рис. 3. Пример взаимодействия с голосовым помощником

тегории запросов, которые задействуются в ходе работы программы как важнейшие составляющие процесса принятия ею решений. Например, для вышеуказанного текста системой определяется категория запроса «setup_ssh_pragma_permit_version» по ключевым фразам «включи», «эсэсаш», «версии».

Данный запрос попадает в модуль «Менеджер диалогов», который отвечает пользователю сгенерированными на основе шаблонов голосовыми фразами, взаимодействуя с модулем синтеза речи, и, самое главное, принимает решения. Процесс принятия решений должен быть предсказуемым, так что не может быть, по нашему мнению, основан на машинном обучении (в целях безопасности). А потому основу модуля составляют правила, сценарии и конфигурационные файлы. Здесь нами реализована концепция «форм-филлинг», состоящая в том, что системный администратор своими репликами как бы заполняет некую виртуальную форму и, по мере заполнения им всех обязательных полей, задачу можно решить, применив необходимое действие. При этом менеджер следит за событиями, которые происходят в процессе взаимодействия пользователя с программой, а также – программы с коммуникационными устройствами, что конструирует логику диалога и влияет на процесс принятия решений. Поскольку данный запрос администратора после его семантического тегирования не включал информации о том, на каком сетевом оборудовании администратор хочет изменить конфигурацию, менеджер диалогов после заполнения соответствующей виртуальной формы может запросить недостающую информацию у пользователя (например, имя или тип устройства) или предоставить опцию изменения для текущего активного се-

тевого оборудования, на который системный администратор ранее произвел навигационный переход.

Указанный выше пример диалога между системным администратором и голосовым помощником продемонстрирован на рисунке 3.

Таким образом, мы считаем, что применение технологий, использующих виртуального голосового помощника на основе онтологий в системном администрировании безопасных компьютерных сетей, очень эффективно и способствует повышению уровня компетенций, необходимых системному администратору для организации приемлемого уровня защиты в небольшой локальной компьютерной сети.

Литература

1. Common Vulnerabilities and Exposures: сайт / The MITRE Corporation. – 1999 –. – URL: https://cve.mitre.org/ (дата обращения: 14.11.2022). – Текст: электронный.

2. Exploit Database: сайт / OffSec Services Limited. – 2009 –. – URL: https://www.exploit-db.com/ (дата обращения: 14.11.2022). – Текст: электронный.

3. National Vulnerability Database (NVD): сайт. – Gaithersburg. –. – URL: https://nvd.nist.gov/ (дата обращения: 14.11.2022). – Текст: электронный.

4. Secunia Advisories: сайт / Flexera. – Chicago. – . – URL: https://community.flexera.com/t5/Secunia-Advisories/ct-p/advisories (дата обращения: 14.11.2022). – Текст: электронный.

5. Vulnerability Notes Database: сайт / Carnegie Mellon University. – Pittsburgh. – . – URL: https://www.kb.cert.org/vuls/ (дата обращения: 14.11.2022). – Текст: электронный.

6. Банк данных угроз безопасности информации: сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва. – . – URL: https://bdu.fstec.ru/ (дата обращения: 14.11.2022). – Текст: электронный.

7. Kim A., Luo J., Kang M. Security ontology for annotating resources //OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". – Springer, Berlin, Heidelberg, 2005. – С. 1483-1499.

8. Котенко И. В., Полубелова О. В., Чечулин А. А. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода //Информатика и автоматизация. – 2013. – №. 26. – С. 26-39.

9. Мирзагитов А. А., Пальчунов Д. Е. Методы разработки онтологии по информационной безопасности, основанные на прецедентном подходе //Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2013. – Т. 11. – №. 3. – С. 37-46.

10. Гаршина В. В., Степанцов В. А. Онтологический подход для анализа рисков безопасности информационных систем //Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 3 (29). – С. 18-22.

11. Загорулько Ю. А. Моделирование робота, управляемого речевыми сигналами //Известия Томского политехнического университета. Инжиниринг георесурсов. – 2011. – Т. 319. – №. 5. – С. 98-102.

12. Актаева А.У., Ниязова Р., Сералиева А., Сарсенбаева Ж., Даутов А., Кусаинова У, Жартанов С. КОГНИТИВНЫЕ ТЕХНОЛОГИИ ОНТОЛОГИИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. URL: http://ceur-ws.org/Vol-2064/paper01.pdf (дата обращения 14.11.2022).

13. Shabalin, A. M. Development of a Set of Procedures for Providing Remote Access to a Corporate Computer Network by means of the SSH Protocol (Using the Example of the CISCO IOS Operating System) / A. M. Shabalin, E. A. Kaliberda // Dynamics of Systems, Mechanisms and Machines, Dynamics: 15th International IEEE Scientific and Technical Conference, Omsk, 09–11 ноября 2021 года. – IEEE: Institute of Electrical and Electronics Engineers Inc., 2021. – DOI 10.1109/Dynamics52735.2021.9653723. – EDN OBZZYO.

References

1. Common Vulnerabilities and Exposures: sayt / The MITRE Corporation. – 1999 –. – URL: https://cve.mitre.org/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

2. Exploit Database: sayt / OffSec Services Limited. – 2009 –. – URL: https://www.exploit-db.com/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

3. National Vulnerability Database (NVD): sayt. – Gaithersburg. – . – URL: https://nvd.nist.gov/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

4. Secunia Advisories: sayt / Flexera. – Chicago. – . – URL: https://community.flexera.com/t5/Secunia-Advisories/ct-p/advisories (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

5. Vulnerability Notes Database : sayt / Carnegie Mellon University. – Pittsburgh. – . – URL: https://www.kb.cert.org/vuls/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

6. Bank dannykh ugroz bezopasnosti informatsii: sayt / FAU «GNIII PTZI FSTEK Rossii». – Moskva. – . – URL: https://bdu.fstec.ru/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

7. Kim A., Luo J., Kang M. Security ontology for annotating resources //OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". – Springer, Berlin, Heidelberg, 2005. – C. 1483-1499.

8. Kotenko I. V., Polubelova O. V., Chechulin A. A. Postroenie modeli dannykh dlya sistemy modelirovaniya setevykh atak na osnove ontologicheskogo podkhoda //Informatika i avtomatizatsiya. – 2013. – №. 26. – S. 26-39.

9. Mirzagitov A. A., Pal'chunov D. E. Metody razrabotki ontologii po informatsionnoy bezopasnosti, osnovannye na pretsedentnom podkhode //Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnye tekhnologii. – 2013. – T. 11. – №. 3. – S. 37-46.

10. Garshina V. V., Stepantsov V. A. Ontologicheskiy podkhod dlya analiza riskov bezopasnosti informatsionnykh sistem //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2018. – №. 3 (29). – S. 18-22.

11. Zagorul'ko Yu. A. Modelirovanie robota, upravlyaemogo rechevymi signalami //Izvestiya Tomskogo politekhnicheskogo universiteta. Inzhiniring georesursov. – 2011. – T. 319. – №. 5. – S. 98-102.

12. Aktaeva A.U., Niyazova R., Seralieva A., Sarsenbaeva Zh., Dautov A., Kusainova U, Zhartanov S. KOGNITIVNYE TEKhNOLOGII ONTOLOGII V SISTEMAKh INFORMATsIONNOY BEZOPASNOSTI. URL: http://ceur-ws.org/Vol-2064/paper01.pdf (data obrashcheniya 14.11.2022).

13. Shabalin, A. M. Development of a Set of Procedures for Providing Remote Access to a Corporate Computer Network by means of the SSH Protocol (Using the Example of the CISCO IOS Operating System) / A. M. Shabalin, E. A. Kaliberda // Dynamics of Systems, Mechanisms and Machines, Dynamics: 15th International IEEE Scientific and Technical Conference, Omsk, 09–11 noyabrya 2021 goda. – IEEE: Institute of Electrical and Electronics Engineers Inc., 2021. – DOI 10.1109/Dynamics52735.2021.9653723. – EDN OBZZYO.

ЗАХАРОВ Александр Анатольевич, доктор технических наук, профессор, заведующий базовой кафедрой безопасности информационных технологий умного города, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: a.a.zakharov@utmn.ru

ШАБАЛИН Андрей Михайлович, кандидат педагогических наук, доцент, доцент кафедры информационной безопасности, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: a.m.shabalin@utmn.ru

ХАНБЕКОВ Шамиль Ирекович, аспирант 2 курса, ассистент кафедры информационной безопасности, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: s.i.khanbekov@utmn.ru

ДЖАЛИЛЗОДА Дунё Бехруз, ведущий инженер-программист, МКУ «Тюменьгортранс». 625019, г. Тюмень ул. Республики, 200. E-mail: d.jalilzoda@vk.com

ПОНОМАРЕВ Кирилл Юрьевич, Руководитель группы .NET ООО «АйТиТуДжи. 109544, г. Москва, ул. Большая Андреевская, 17. E-mail: drmckay-kirill@yandex.ru

ZAKHAROV Aleksandr Anatol'evich, doctor of technical sciences, professor, head of Base department of smart city technologies information security, Tyumen state university. 625003, Tyumen, Volodarskogo street, 6. E-mail: a.a.zakharov@utmn.ru

SHABALIN Andrey Mikhaylovich, candidate of pedagogical sciences, docent of Department of information security, Tyumen State University. 625003, Tyumen, Volodarskogo street, 6. E-mail: a.m.shabalin@utmn.ru

KHANBEKOV Shamil Irekovich, 2nd year graduate student, assistant of Department of information security, Tyumen State University. 625003, Tyumen, Volodarskogo street, 6. E-mail: s.i.khanbekov@utmn.ru

DZHALILZODA Dune Bekhruz, leading software engineer. 625019, Tyumen, st. Republic, 2 MKU "Tyumengortrans". E-mail: d.jalilzoda@vk.com

PONOMAREV Kirill Yuryevich, Head of the .NET group of LLC ITToGi. 109544, Moscow, Bolshaya Andreevskaya street, 17. E-mail: drmckay-kirill@yandex.ru