УДК 004.056
DOI: 10.33764/2618-981X-2021-6-194-200

МНОГОУРОВНЕВАЯ АРХИТЕКТУРА СИСТЕМЫ УПРАВЛЕНИЯ ЗНАНИЯМИ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Амыртаа Кужугетович Монгуш
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (996)545-07-00, e-mail: amyrtaakuzhuget@mail.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Обеспечение информационной безопасности является серьезной проблемой, поскольку риски, связанные с безопасностью, могут сильно повлиять на активы организации. Для повышения уровня информационной безопасности предлагается использовать систему управления знаниями с многоуровневой архитектурой, с целью улучшения обмена знаниями и облегчения принятия решений, а также уменьшения зависимости от отдельных экспертов по информационной безопасности.

Ключевые слова: информационная безопасность, управление информационной безопасностью, управление знаниями, приобретение знаний, база знаний

MULTI-LEVEL ARCHITECTURE OF KNOWLEDGE MANAGEMENT SYSTEM TO IMPROVE INFORMATION SECURITY LEVEL

Amyrtaa K. Mongush
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (996)545-07-00, e-mail: amyrtaakuzhuget@mail.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of the Department of Physics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Information security is a major concern because security risks can greatly affect the assets of an organization. To increase the level of information security, it is proposed to use a knowledge management system with a multi-level architecture in order to improve knowledge exchange and facilitate decision-making, as well as reduce dependence on individual information security experts.

Keywords: information security; information security management; knowledge management; knowledge acquisition, knowledge base

Введение

Информационная безопасность является первостепенной задачей для организаций, поскольку большая часть организационной деятельности и бизнес-процессов во многом зависят от информационных и коммуникационных технологий.

Внедрение эффективной комплексной системы защиты информации в организации зависит, прежде всего, от двух факторов:

1) наличие защищенной информационной инфраструктуры, обеспечивающей целостность данных, унифицированных методов доступа к данным и информации и их поиска, эффективных процедур аутентификации и эффективного управления рисками;

2) наличие экосистемы, поддерживающей знания об информационной безопасности внутри организации, для разработки индивидуального набора процессов, политик и решений безопасности для защиты бизнеса в организации.

В то время как первый фактор широко исследовался специалистами по информационной безопасности, второму фактору уделялось мало внимания. В управлении информационной безопасностью очень важно использование знаний. Они необходимы для принятия рациональных решений относительно выбора политик и процедур информационной безопасности. Аспект управления знаниями в сфере информационной безопасности исследовался очень мало, и требуются дополнительные исследования, чтобы изучить более структурированные схемы и модели интеграции систем управления знаниями в управление информационной безопасностью.

Обмен знаниями

Во многих организациях методы защиты информации сосредоточены на технических решениях, и знания об информационной безопасности остаются скрытыми в памяти ограниченного числа специалистов. На сегодняшний день объем инцидентов, связанных с информационной безопасностью, и вызванных ими финансовых потерь продолжает увеличиваться, соответственно возрастает степень серьезности таких инцидентов. Все это ставит под сомнение реальную эффективность решений по информационной безопасности [1]. Причина неэффективности заключается в том, что информационная безопасность – это в первую очередь «проблема людей», а также техническая проблема. На основании этого считается, что управление информационной безопасностью – это наукоемкая деятельность, которая в настоящее время во многом зависит от опыта экспертов по информационной безопасности [11].

Управление знаниями оказывает положительное влияние на эффективность управления информационной безопасностью. Знание относится к кодифицированной информации с высокой долей добавленной ценности для человека, включая понимание, интерпретацию, контекст, опыт, мудрость и так далее [3]. Знание может быть явным и неявным. Явное знание выражено в виде

слов и цифр, и может передаваться в формализованном виде на носителях (документы, инструкции, книги и пр.). Неявное знание не формализуется, и может существовать лишь вместе с его обладателем – человеком или группой лиц. Оно связано с интуицией, прозрением, догадками, идеалами, ценностями. Этот вид знаний – основа индивидуальных действий и опыта [9].

Управление знаниями направлено на выявление, сбор, систематизацию знаний и предоставление их другим. Чтобы облегчить совместное использование и обмен знаниями, необходим формальный механизм для выявления и распространения знаний. Это облегчает принятие решений, увеличивает конкурентоспособность организации [7, 10].

Каждая организация имеет множество ценных знаний в рамках бизнес-процессов, которые необходимо хорошо задокументировать. Многие знания, используемые в процессах обеспечения информационной безопасности, хранятся как неявные знания внутри персонала. Если любой из этих сотрудников уволится с работы, то это приведет к серьезной угрозе для систем и процессов организации в целом [4]. Комплексный подход к этой проблеме облегчил бы действия по контролю над этим риском, например, посредством документирования знаний и обмена ими с помощью системы управления знаниями. В [6] Лю и др. утверждают, что организации могут улучшить информационную безопасность, сотрудничая и делясь знаниями о безопасности с другими фирмами. Примером организации обмена знаниями является центр мониторинга информационной безопасности, предназначенный для облегчения обмена информацией об угрозах и уязвимостях кибербезопасности. Этот центр обеспечивает нейтральный форум для взаимодействия между коллегами из членских организаций, чтобы понять и поделиться закрытыми деталями угроз и уязвимостей.

Система управления знаниями для информационной безопасности

В настоящее время создание в организации знаний об информационной безопасности остается разовым процессом. Организации либо нанимают дорогих внешних консультантов, либо зависят от экспертов по информационной безопасности, которые выстраивают свои собственные процессы создания личных знаний.

Во многих организациях потеря знаний из-за текучести кадров может стать большой проблемой. Если все важные данные хранятся внутри организации, то неожиданная текучесть кадров будет менее разрушительной для организации. Интеграция управления знаниями в управление информационной безопасностью может помочь в создании центрального репозитория для хранения и обмена информацией об информационной безопасности в организации [8]. Тем не менее, обязательно следует соблюдать стандарты по защите информации, чтобы разграничивать доступ в зависимости от ролей сотрудников. Система управления знаниями в информационной безопасности предназначена для поддержки управления информационной безопасностью на всех уровнях, как предложили Белсис

и др. [1]. Это могло бы уменьшить зависимость от внешних дорогих консультантов и экспертов по информационной безопасности, поскольку создание знаний происходит внутри организации.

Приобретение знаний

Приобретение знаний – важный шаг на пути к внедрению системы управления знаниями. Этот шаг заключается в настройке процесса приобретения знаний, цель которого – снабдить систему необходимыми знаниями. Приобретение знаний – это процесс, который направлен на передачу опыта решения проблем информационной безопасности, а также всей информации, связанной с информационной безопасностью организации. Эта передача осуществляется с помощью методов управления знаниями, которые анализируют задачи экспертов и их опыт и тщательно исследуют организационные документы, связанные с информационной безопасностью [2].

Приобретение знаний достигается посредством четырехступенчатого цикла: выявление, представление, внедрение и проверка (рис. 1).

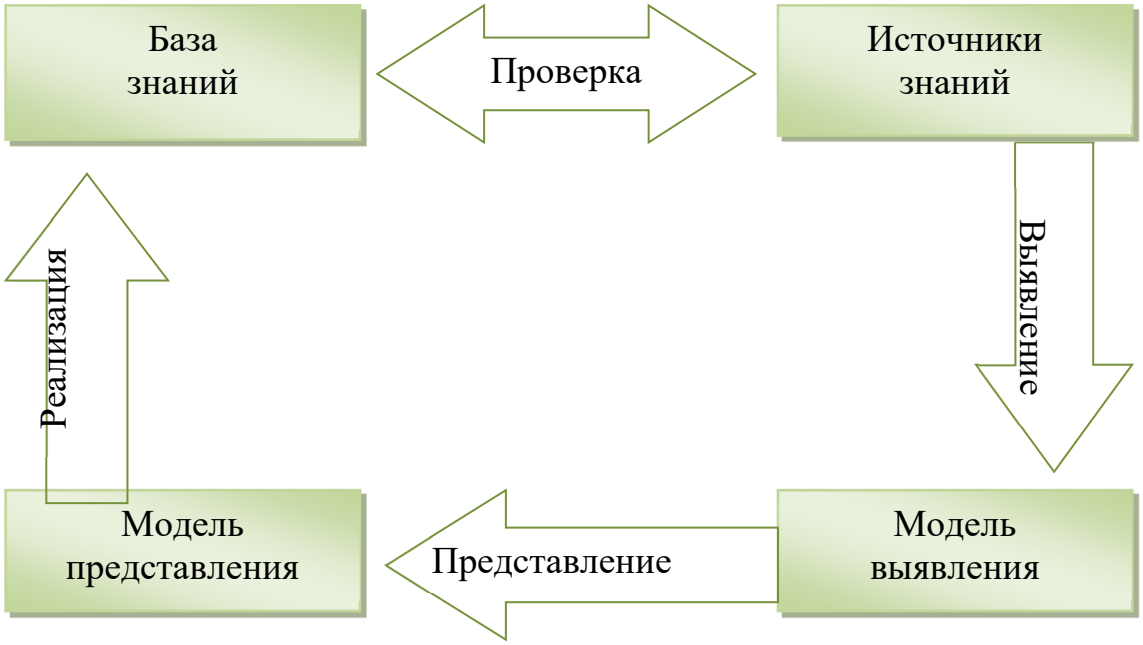

Рис. 1. Процесс приобретения знаний

Выявление – это идентификация данных, относящихся к информационной безопасности, используемых экспертами. Эти данные разбиты на категории, чтобы выделить процедуры, действия и правила, используемые в процессе принятия решения экспертом. Представление состоит в формализации знаний для последующей реализации. На этом этапе вырабатываются схемы действий, организующие действия эксперта. Кроме того, определяются стратегии решения проблем, используемые в процессе принятия решений. Реализация заключается в ко-

дировании опыта, приобретенного на двух предыдущих этапах, в базу, основанную на формализованных знаниях. На этапе проверки знания, закодированные в базе знаний, проверяются на актуальность и обновляются.

Архитектура управления знаниями

Знания полезны для организации, когда у нее есть формальные или неформальные механизмы преобразования неявных знаний в явные. Архитектура управления знаниями используется для построения системы управления знаниями, которая позволяет фиксировать и совместно использовать знания об информационной безопасности, чтобы эффективно реагировать на инциденты информационной безопасности и уменьшить зависимость от экспертов по информационной безопасности [5]. Архитектура системы управления знаниями включает четыре основных уровня: пользователь знаний, интерфейс знаний, описание знаний и ресурсы знаний (рис. 2).

Рис. 2. Архитектура системы управления знаниями

Пользователь знаний описывает «нужных людей», которым следует приобрести знания в области информационной безопасности, чтобы поддерживать конфиденциальность, целостность и доступность системы.

Интерфейс знаний детализирует «правильную информацию», которая должна быть передана каждому пользователю знаний для поддержания безопасности си-

стемы и для принятия эффективных решений относительно безопасности информационной системы. Взаимосвязь между пользователями знаний и интерфейсом знаний должна быть тщательно определена, поскольку она должна позволять только «правильному» пользователю знаний получить доступ к «правильной» информации по информационной безопасности, на основе типов знаний, и роли пользователя в организации. В зависимости от роли пользователя в организации будут отображаться конкретные знания. Другими словами, для интерфейса знаний будет назначен ряд ролей пользователей, которые могут получить к нему доступ.

Описание знаний предоставляет необходимые элементы для классификации знаний, которые могут быть процедурными (как), декларативными (что) или условными (утверждение, когда и какие отношения). Этот уровень включает: онтологии (представляют собой концептуальные описания домена безопасности); схемы действий (определяют последовательность действий, которые необходимо выполнить для решения проблемы, связанной с информационной безопасностью); правила (описывают соответствие между фактами безопасности и действиями, которые необходимо предпринять для решения проблемы безопасности); стратегии разрешения (объединяют различные правила, действия, методы и эвристики для решения проблемы безопасности или определения метода предотвращения угроз безопасности).

Уровень ресурсов знаний включает ресурсы, из которых собирается и получается информация, связанная с безопасностью. Этот уровень имеет дело с базами данных организации, которые могут быть внутренними по отношению к организации или внешними. Знания будут также извлечены из коллективной памяти организации, определенной из прошлого опыта и событий, которые влияют на текущую деятельность организации. Эта информация находится в локальной сети. К ресурсам также можно получить удаленный доступ в сети, доступ к ним осуществляется с помощью определенных доступных служб, которые позволяют уровню ресурсов искать, получать доступ и извлекать их.

Заключение

Опыт в сфере информационной безопасности очень важен для обеспечения информационной безопасности организации от угроз, которые становятся очень частыми и сложными. Решения защиты системы от угроз не всегда можно найти в книгах и руководствах, большинство из них приобретено благодаря опыту и практике. Система управления знаниями с многоуровневой архитектурой позволяет поддерживать передачу практических знаний от экспертов по информационной безопасности в систему управления знаниями, которая будет использоваться многими участниками, участвующими в обеспечении информационной безопасности организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Белсис П., Коколакис С., Киунтузис Э. Безопасность информационных систем с точки зрения управления знаниями // Управление информацией и компьютерная безопасность. – 2005. – №13 (3). – С. 189-202.

2. Берри Дж. На пути к структуре коллективного разума // Международная конференция по управлению цифровыми знаниями. – 2010. – С. 454-459.

3. Глейзер Т., Паллас Ф. Информационная безопасность и управление знаниями: решения через аналогии // Электронный журнал ССРН. – 2007. – С. 1–17.

4. Джианетто К. Преимущества управления знаниями [Электронный ресурс]. URL: https://www.elitarium.ru/preimushhestva_upravlenija_znanijami/ (дата обращения: 22.03.2021).

5. Кеш С., Ратнасингам П. Архитектура знаний для ИТ-безопасности, Коммуникации ACM. – 2007. – № 50 (7). – С. 103–108.

6. Лю Д., Джи Ю., Мукерджи В. Обмен знаниями и инвестиционные решения в информационной безопасности // Системы поддержки принятия решений. – 2011. – № 52 (1). – С. 95-107.

7. Матвеев А. Ю. Введение в процесс управления знаниями // Бизнес-образование в экономике знаний. – 2016. – № 3 (5). – С. 46-50.

8. Мусило Ю., Мусило А., Вейнс Д., Биффло С. Архитектура систем коллективного интеллекта // 12-я рабочая конференция ИФИП по архитектуре программного обеспечения (WICSA). – 2015. – С. 1-11.

9. Нонака И., Такеучи Х. Компания – создатель знания: зарождение и развитие инноваций в Японских фирмах. – М. : Олимп-Бизнес, 2011. – 384 с.

10. Филяк П. Ю. Обеспечение информационной безопасности с помощью технологии управления знаниями «BRAIN» // Информация и безопасность. – 2016. – Т. 19. – № 2. – С. 238-243.

11. Шедден П., Шиперс Р., Смит В., Ахмад А. Включение знаний с точки зрения перспективы при оценке рисков безопасности // Журнал систем управления информацией и знаниями. – 2011. – № 41 (2). – С. 152-166.