УДК 005.94
DOI: 10.33764/2618-981X-2021-6-189-193

УПРАВЛЕНИЕ ЗНАНИЯМИ В КОНТЕКСТЕ 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

Знания об информационной безопасности являются одним из важных факторов в управлении информационной безопасностью, поскольку 70-80% инцидентов информационной безопасности происходит из-за халатности или неосведомленности сотрудников. В статье подчеркивается важность обмена знаниями в сфере информационной безопасности, выявлены препятствия на пути такого обмена знаниями.

Ключевые слова: информационная безопасность, проблемы управления информационной безопасностью, управление знаниями

KNOWLEDGE MANAGEMENT IN THE CONTEXT OF INFORMATION SECURITY

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

Knowledge of information security is one of important factors in information security management, since 70-80% of information security incidents occurred due to negligence or lack of awareness of employees. This article highlights the importance of sharing information security knowledge and identifies barriers to such sharing.

Keywords: information security, information security management problems, knowledge management

Введение

Информационная безопасность – важная проблема в современном мире. Управление информационной безопасностью не может осуществляться с помощью простого набора аппаратного и программного обеспечения, для этого требуется комплексная система. В повышении уровня информационной без-

опасности в организации важную роль играют сотрудники. Обмен знаниями всех типов улучшает организацию в целом, это способствует укреплению доверия между сотрудниками. Особый интерес в этой статье представляет обмен знаниями в сфере информационной безопасности. Обмен знаниями улучшает осведомленность об информационной безопасности, что важно, когда речь идет о предотвращении нарушений информационной безопасности. Поэтому организации должны уделять особое внимание обмену знаниями в сфере информационной безопасности, чтобы сделать знания доступными для всех, кто в них нуждается, и, в конечном итоге, улучшить информационную безопасность во всей организации.

Знания

Люди могут получать знания из своего окружения или из личного опыта [9]. В контексте информационной безопасности, люди могут получить знания в ходе обучающих мероприятий, но с большей вероятностью они получат необходимые знания от других сотрудников на рабочем месте.

Знание может быть неявным или явным [5]. Первое относится к знаниям, которые нелегко записать или выразить, что затрудняет обмен и сохранение знаний. Для сотрудников важно передавать неявные знания, связанные с информационной безопасностью, другим сотрудникам, чтобы получить формализованные знания. Явные знания могут быть выражены в числах и словах и могут быть записаны. Знания представляют наибольшую ценность, когда они связаны с другими релевантными и актуальными знаниями. При этом могут возникать новые знания, этот процесс называется «комбинацией» [7].

Знания в контексте информационной безопасности

Мария Бартнес и др. в своей работе [2] определяют информационную безопасность как набор процессов, политик и инструментов стратегического управления, необходимых для предотвращения, обнаружения, документирования и противодействия угрозам, которые подвергают информационные системы рискам, вызывающим ущерб, такой как потеря и кража информации. Флорес и др. [7] определяют обмен знаниями как явную или скрытую передачу ценностей, опыта, экспертных оценок и контекстной информации от одного человека к другому, что помогает этому человеку включать и оценивать новую информацию и опыт. Стэнтон Дж., Стэм К. и др. [10] предлагают двумерную модель поведения конечных пользователей в области безопасности. Первое – это опыт, и второе – намерение (доброжелательные намерения). В этой категории люди без знаний совершают простые ошибки, но знание ведет к осведомленности и гарантиям информационной безопасности. Кэтрин Парсонс совместно с другими исследователями [6] изучали человеческий фактор в информационной безопасности и пришли к выводу, что человеческие ошибки, связанные с отсутствием осведомленности и знаний об информационной без-

опасности, являются основными источниками нарушений информационной безопасности. Используя анкетирование и включив выборку из 500 сотрудников, авторы измерили уровень осведомленности сотрудников и пришли к выводу, что сотрудники с более низким уровнем осведомленности о безопасности подвергают свою организацию рискам нарушения информационной безопасности [6].

В качестве рекомендации авторы определили целостный подход к обучению сотрудников, в котором особое внимание уделяется знаниям и отношению, как способу решения этой проблемы. Однако Чжан Т. в своей работе «Срок действия знаний в обучении по вопросам безопасности» [11] утверждает, что знания в этой области быстро устаревают, и их необходимо постоянно обновлять. Авторы работы [3] утверждают, что культивирование культуры информационной безопасности, которая подразумевает, что обмен знаниями стал обязательным, является лучшим подходом к учету человеческого фактора в информационной безопасности.

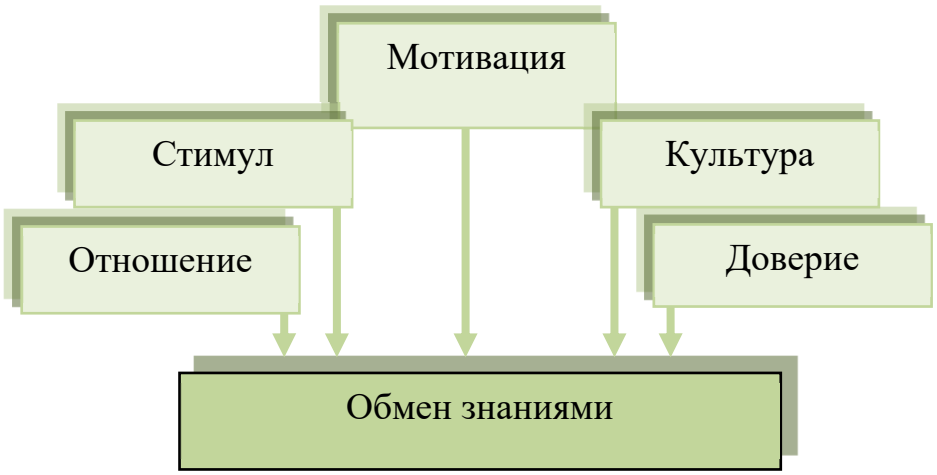
Обмен знаниями в сфере информационной безопасности

Обмен знаниями имеет важнейшее значение в сфере информационной безопасности. Сафа и фон Солмс [8], изучая эффективную модель, которая могла снизить негативное влияние человеческого фактора на информационную безопасность, пришли к выводу, что обмен знаниями, опытом и совместная работа в области информационной безопасности положительно влияют на желание сотрудников соблюдать руководящие принципы информационной безопасности. В работе [1] сообщается, что люди делились бы знаниями, если бы ожидали получить взамен что-то ценное, то есть при передаче знаний важна взаимность. Авторы предлагают использовать теорию детерминации – удовлетворение потребностей сотрудников (стимул) для максимального обмена, такой обмен необходим для улучшения и повышения осведомленности сотрудников об информационной безопасности организации.

Данг-Фам Д. и Нхома М. изучали, почему люди дают советы по информационной безопасности другим, и они пришли к выводу, что основными препятствиями для обмена знаниями об информационной безопасности является личные отношения и недостаток доверия между сотрудниками [4]. Роша Флорес В., Антонсен Э. и Экстедт М. исследовали влияние культурных факторов на обмен знаниями в области информационной безопасности, результаты показывают, что когда речь заходит о характере обмена, стоит учитывать национальные и культурные факторы [7]. Они пришли к выводу, что наиболее серьезным препятствием для обмена знаниями в области безопасности является культура. Авторы работы [9] Феледи Д., Фенц С. и Лехнер Л. исследовали эффективность сотрудничества между участниками в процессе обмена знаниями, они определили, что основным препятствием для обмена знаниями о безопасности является отсутствие мотивации со стороны сотрудников.

Факторы, влияющие на обмен знаниями

В нескольких исследованиях рассматривались преимущества обмена знаниями в организации, особенно в области осведомленности об информационной безопасности. На рисунке отображены факторы, влияющие на обмен знаниями, подтвержденные исследованиями. Наиболее значительными препятствиями являются: отсутствие мотивации, недостаток доверия, отсутствие систем стимулов и вознаграждений, отсутствие организационной культуры.



Факторы, влияющие на обмен знаниями

Различные исследования по обмену знаниями в области информационной безопасности проводились в разных частях мира, и на азиатском континенте было проведено наибольшее количество исследований. Возможное объяснение этого может заключаться в том, что на азиатском континенте высокий уровень риска для информационной безопасности, что требует большего внимания к безопасности и попыток повысить осведомленность сотрудников.

Текущее исследование выявило преимущества обмена знаниями в организационной среде, особенно с точки зрения осведомленности об информационной безопасности. Результаты анализа литературы в этой области показывают, что недостаток доверия, мотивации и культуры являются большими препятствиями для обмена знаниями. В большинстве исследований не предлагалось эффективных решений для устранения этих препятствий.

Заключение

Исследования обмена знаниями в сфере информационной безопасности показывают, что обмен знаниями положительно влияет на осведомленность сотрудников об информационной безопасности, снижает риски, улучшает процесс принятия решений и повышает эффективность работы. Однако на обмен знаниями влияют многие факторы, такие как доверие, мотивация, куль-

тура и отношение. Также была выявлена важность процессов стимулирования организации в поощрении обмена знаниями в контексте информационной безопасности.

Когда мы принимаем во внимание тот факт, что хакеры широко и активно делятся знаниями между собой, мы должны обращать внимание на обмен знаниями в сфере информационной безопасности внутри организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алахмари С., Рено К., Оморония И. Модель для описания и максимизации обмена знаниями о безопасности для повышения осведомленности о кибербезопасности // 16-я Европейская, Средиземноморская и Ближневосточная конференция по информационным системам. – 2020.– С. 376-390.

2. Бартнес М, Гьере Э. А., Роша Флорес В. Геймификация осведомленности и обучения информационной безопасности // 3-я Международная конференция по безопасности и конфиденциальности информационных систем. – 2017. – С. 59-70.

3. Гказа Н., фон Зольмс Р. Культура кибербезопасности: неопределенная проблема // Международная конференция ИФИП по образованию в области информационной безопасности. – 2017. – С. 98-109.

4. Гугунова П. И., Кашевник А. М. Коллективное информационное взаимодействие участников экспертных сетей: анализ современного состояния исследований // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – № 5 (17). – С. 859-871.

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

6. Парсонс К., Калик Д, Паттинсон М., Бутавичюс М., Маккормак А., Зваанс Т. Опросник по человеческим аспектам информационной безопасности: Две дополнительные проверочные исследования // Компьютеры и безопасность. – 2017. – № 66. – С. 40-51.

7. Роша Флорес В., Антонсен Э., Экстедт М. Обмен знаниями в области информационной безопасности в организациях: исследование влияния поведенческого управления информационной безопасностью и национальной культуры // Компьютеры и безопасность. – 2014. – № 43. – С. 90-110.

8. Сафа Н. С., Сольмс Р. В., Фурнелл С. Модель соответствия политики информационной безопасности в организациях // Компьютеры и безопасность. – 2016. – № 56. – С. 70-82.

9. Феледи Д., Фенц С., Лехнер Л. На пути к обмену знаниями в области информационной безопасности через Интернет // Технический отчет по информационной безопасности. – 2013. – № 4 (17). – С. 199-209.

10. Стэнтон Дж., Стэм К., Мастранджело П., Джолтон Дж. А. Анализ поведения безопасности конечных пользователей // Компьютеры и безопасность. – 2005. – № 2 (24). – С. 124-133.

11. Чжан Т. Истечение срока знаний в обучении по вопросам безопасности // 13-я ежегодная конференция ассоциации цифровой криминалистики, безопасности и права. – 2018. – С. 197-211.