DOI: 10.58168/CISMP2024_44-47
УДК 004.56

РАЗВИТИЕ КОМПЕТЕНЦИЙ СОТРУДНИКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СОКРАЩЕНИЯ РИСКОВ ВНУТРЕННИХ УГРОЗ

Ю.Ю. Громов[1], П.И. Карасев[2], Ф.М. Пыршев[1]

[1]ФГБОУ ВО «Тамбовский государственный технический университет»
[2]МИРЭА - Российский технологический университет

Аннотация. В эпоху цифровизации бизнес-процессов информационная безопасность становится критически важным аспектом устойчивого развития и конкурентоспособности предприятий. Защита информационных активов от несанкционированного доступа, вредоносных атак, утечек данных и других угроз требует комплексного подхода, включая технические средства защиты, обучение персонала основам информационной безопасности и разработку эффективных политик безопасности. Статья анализирует роль человеческого фактора в обеспечении информационной безопасности и подчеркивает важность систематического обучения и повышения осведомленности персонала по вопросам информационной безопасности. Авторы рассматривают различные методы обучения, включая онлайн-курсы, корпоративные тренинги, симуляцию фишинга и обучение на примерах из реальной жизни. Статья также подчеркивает преимущества обучения сотрудников, включая повышение уровня осведомленности, улучшение навыков, создание атмосферы ответственности и доверия, снижение вероятности возникновения внутренних угроз и улучшение репутации компании.

Ключевые слова: информационная безопасность, обучение сотрудников, человеческий фактор, внутренние угрозы, повышение осведомленности.

DEVELOPMENT OF EMPLOYEE COMPETENCIES IN INFORMATION SECURITY TO REDUCE THE RISKS OF INTERNAL THREATS

Y.Y. Gromov [1], P.I. Karasev[2], F.M. Pyrshev[1]
[1]Tambov State Technical University
[2]MIREA - Russian Technological University

Abstract. In today's digital age, information technology plays a crucial role in all aspects of business operations. As a result, information security has become an essential component for protecting data and ensuring the stability of businesses. Information security risks are not only associated with external threats but also with human error within organizations. Training employees in information security fundamentals is a vital strategy to minimize potential risks and prevent security incidents caused by unintentional or erroneous actions. This article discusses methods for training and educating employees on information security principles, as well as the impact of these efforts on reducing internal risks to organizations.

Keywords: information security, employee training, human factor, internal threats, awareness raising.

В эпоху цифровизации бизнес-процессов и постоянного роста объемов цифровой информации, информационная безопасность выходит на передний план как один из приоритетных аспектов устойчивого развития и конкурентоспособности предприятий [1]. Защита информационных активов от несанкционированного доступа, вредоносных атак, утечек данных и других угроз становится не просто задачей IT-отдела, но стратегической задачей управления на всех уровнях организации. Помимо технических средств защиты, значительную роль в обеспечении информационной безопасности играет человеческий фактор. Ошибки сотрудников, неосведомленность в вопросах безопасности или непреднамеренные действия могут стать причиной серьезных инцидентов, влекущих за собой финансовые потери и потерю репутации компании. Таким образом, систематическое обучение и повышение осведомленности персонала по вопросам информационной безопасности являются неотъемлемыми элементами стратегии защиты информационных ресурсов предприятия.

В современном обществе, информация становится одним из ключевых активов для любой организации или индивида. Защита этой информации является критически важной для поддержания конфиденциальности, целостности и доступности данных [2]. Обучение сотрудников имеет решающее значение для защиты данных. Правильное обучение поможет выстроить первую линию обороны от утечек информации, кражи данных и других видов атак.

Обучение помогает повысить осведомлённость сотрудников о возможных угрозах, научить их распознавать подозрительные ситуации и действия, а также правильно реагировать на них.

Краткий обзор основных угроз информационной безопасности, связанных с человеческим фактором

Человеческий фактор играет значительную роль в обеспечении информационной безопасности [3]. Ошибки сотрудников, недостаточная осведомленность о принципах безопасности и целенаправленные вредоносные действия внутренних лиц могут стать причиной серьезных угроз для организаций. Среди ключевых угроз, связанных с человеческим фактором, выделяют:

Социальная инженерия: Манипулирование людьми для получения конфиденциальной информации.

Фишинг: Получение доступа к личным данным через мошеннические сообщения.

Несанкционированный доступ: Доступ к информационным системам без разрешения.

Внутренние угрозы: Действия сотрудников, направленные на нанесение ущерба информационной системе организации.

Защита от этих и других угроз требует комплексного подхода, включая технические средства защиты, обучение персонала основам информационной безопасности и разработку эффективных политик безопасности [4].

Методы обучения сотрудников по информационной безопасности: Онлайн-курсы и вебинары: это удобный и доступный способ обучения, который позволяет сотрудникам проходить обучение в удобное для них время и место. Онлайн-курсы могут содержать интерактивные модули, тесты и практические задания для закрепления знаний.

Корпоративные тренинги и семинары: Организация корпоративных тренингов по информационной безопасности позволяет привлечь специалистов извне для проведения обучения, а также создать более интерактивную и адаптированную программу для конкретной компании.

Симуляция фишинга: Проведение атак позволяет сотрудникам наглядно увидеть, как могут выглядеть реальные угрозы, и научиться правильно реагировать на них.

Обучение на примерах из реальной жизни: Один из наиболее эффективных способов обучения сотрудников основам информационной безопасности — это использование примеров из реальной жизни. Рассказы о случаях утечки данных или кибератак позволяют сотрудникам лучше понять последствия небрежного отношения к информационной безопасности.

Тестирование знаний и навыков: Проведение тестирования знаний и навыков после завершения обучения позволяет оценить эффективность обучающей программы и выявить слабые места, которые требуют дополнительного внимания.

Преимущества обучения сотрудников:

Повышение уровня осведомленности сотрудников о возможных угрозах и рисках в сфере информационной безопасности.

Улучшение навыков сотрудников по защите конфиденциальных данных и предотвращению утечек информации.

Создание атмосферы ответственности и доверия в компании, где каждый работник понимает важность обеспечения безопасности данных.

Снижение вероятности возникновения внутренних угроз со стороны сотрудников, как намеренных, так и случайных.

Улучшение репутации компании и повышение доверия клиентов и партнеров благодаря эффективным мерам по обеспечению информационной безопасности.

Сокращение потенциальных финансовых потерь и репутационных убытков, связанных с утечками данных или кибератаками.

Повышение профессионального уровня сотрудников и развитие их компетенций в области информационной безопасности.

Обеспечение соответствия компании требованиям законодательства и стандартам безопасности данных.

Выводы

В заключении, можно сделать вывод. Обучение и повышение осведомленности сотрудников в области информационной безопасности является ключевым аспектом защиты организации от внутренних и внешних угроз. Важно подходить к процессу обучения комплексно, сочетая различные

методы и инструменты для охвата широкого круга тем и сценариев. Эффективное обучение должно включать как теоретические аспекты безопасности, так и практические упражнения, моделирующие реальные угрозы и ситуации. Использование игровых элементов и реалистичных симуляций может значительно усилить вовлеченность и интерес сотрудников, повышая эффективность учебного процесса. Наконец, регулярное тестирование и обновление знаний помогут поддерживать высокий уровень осведомленности и готовности сотрудников к действиям в условиях изменяющейся информационной среды.

Список литературы

1. Васильков А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков. – Москва: ФОРУМ: ИНФРА-М, 2013. – 368 с.

2. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. – Санкт-Петербург: СПбНИУИТМО, 2014. – 173 с.

3 Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. – Москва: Горячая линия – Телеком, 2001. – 148 с.

4. Мельников В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. – Москва: Финансы и статистика, 2003. – 368 с.

References

1. Vasilkov A.V. Security and access control in information systems / A.V. Vasilkov. Moscow: FORUM: INFRA-M, 2013. – 368 p.

2. Zhigulin G.P. Organizational and legal provision of information security / G.P. Zhigulin. St. Petersburg: St. Petersburg State University ITMO, 2014. – 173 p.

3. Malyuk A.A., Pazizin S.V., Pogozhin N.S. Introduction to information security in automated systems. Moscow: Hotline – Telecom, 2001. – 148 p.

4. Melnikov V.V. Information security in automated systems / V.V. Melnikov. Moscow: Finance and Statistics, 2003. – 368 p.