УДК 004.056.5

ВАЖНОСТЬ ОБУЧЕНИЯ СОТРУДНИКОВ ОСНОВАМ ЦИФРОВОЙ БЕЗОПАСНОСТИ

Д. А. Ахрем

студент, Брестский государственный технический университет, г. Брест, Беларусь, doraakhrem@gmail.com

Научный руководитель **В. В. Зазерская**

кандидат экономических наук, доцент, декан экономического факультета Брестского государственного технического университета, г. Брест, Беларусь, zazerskaya@mail.ru

Обучение персонала цифровой безопасности помогает сотрудникам защищать данные и ИТ-системы от киберугроз. Программа обучения должна охватывать многие аспекты кибербезопасности, чтобы дать сотрудникам комплексный набор навыков для безопасного управления данными и использования средств ИКТ при обеспечении когнитивных, коммуникативных и организационных задач с соблюдением норм информационной безопасности.

Ключевые слова: кибербезопасность, сотрудники, ИТ, данные.

IMPORTANCE OF TRAINING EMPLOYEES IN THE BASICS OF DIGITAL SECURITY

D. A. Akhrem

student, Brest State Technical University, Brest, Belarus, doraakhrem@gmail.com

Supervisor **V. V. Zazerskaya**

PhD in economic sciences, associate professor, dean of the faculty of economics at Brest State Technical University, Brest, Belarus, zazerskaya@mail.ru

Digital security training helps employees protect data and IT systems from cyberthreats. The training program should cover multiple aspects of cybersecurity to provide employees with a comprehensive set of skills for secure data management and the use of ICT tools while supporting cognitive, communication, and organizational tasks in compliance with information security regulations.

Keywords: cybersecurity, employees, IT, data.

Обучение по повышению осведомленности в вопросах безопасности является важным инструментом для компаний и организаций, которые хотят эффективно защитить свои данные, сократить количество инцидентов, связанных с человеческим фактором, сократить расходы на реагирование и обеспечить понимание сотрудниками того, как ответственно обращаться с клиентскими данными и безопасно работать в сети. Согласно отчету «Лаборатории Касперского» за 2024 год, если сотрудники осведомлены и понимают, что им нужно делать в случае инцидента безопасности, тем меньше вероятность того, что злоумышленник проникнет в инфраструктуру компании. Эти программы, разработанные и реализуемые экспертами в области

ИТ и безопасности, имеют общую цель – попытаться помочь в борьбе с человеческими ошибками, которые приводят к утечкам данных и краже информации и, в итоге, могут привести к финансовым потерям и репутационному ущербу для компании [1].

Обучение по повышению осведомленности в вопросах безопасности – это образовательная программа, которая может принимать различные формы. Однако все программы имеют одну конечную цель: снабдить сотрудников компании знаниями и навыками, необходимыми для защиты данных и конфиденциальной информации организации от взлома, фишинга и других нарушений, что, в свою очередь, защитит ИТ-инфраструктуру компании. Обучение кибербезопасности включает в себя множество различных аспектов, и хорошая программа должна охватывать многие из них, чтобы дать сотрудникам комплексный набор навыков для безопасного управления данными и онлайн-активностью [1].

По закону некоторые компании обязаны соблюдать определенные отраслевые правила, такие как: общий регламент по защите данных (GDPR) или даже Закон о переносимости и подотчетности медицинского страхования (HIPAA), и в рамках этих примеров они должны проводить обучение по кибербезопасности для сотрудников. Обычно это происходит один или два раза в год, чтобы держать сотрудников в курсе последних проблем кибербезопасности, которые постоянно развиваются [1].

Для компаний с небольшим штатом до 15–20 человек может быть достаточно индивидуального инструктажа или личной встречи, посвященной кибербезопасности. Для средних и крупных предприятий, особенно тех, которые имеют филиалы по всей стране, важно использовать эффективные инструменты обучения персонала. Например: «используйте примеры реальные ситуации из прошлого или из текущего опыта организации. Это поможет сотрудникам лучше понять, какие ошибки могут привести к утечке данных или другим проблемам, и как их избежать, оповещайте сотрудников об угрозах безопасности данных в форме информационных бюллетеней, электронных рассылок или встреч с экспертами в области безопасности данных, организуйте практические упражнения в обучающие программы (симуляцию фишинговых атак, проверку сложности паролей и прочие сценарии), чтобы сотрудники могли непосредственно применить свои знания и навыки» [2].

Помимо внедрения технологических мер защиты информации, необходимо создавать условия и развивать культуру информационной и цифровой безопасности в организации. Личная культура цифровой безопасности способствует адаптации установок в корпоративной культуре. Для этого необходимо выстроить доверительные отношения с сотрудниками с целью минимизации их предубеждений по поводу конфиденциальности данных и обеспечить знаниями для противодействия угрозам информационной безопасности. Для мотивации сотрудников к обучению и пониманию различных аспектов использования программного обеспечения и работы в Интернете используют пример из реальной, повседневной жизни. Все боятся, что у них уведут профиль в Instagram, выгрузят из электронной почты копии паспорта или обнулят счёт в банке. Чтобы не допустить этого, на базовом уровне достаточно понимать, каким должен быть надёжный пароль, необходимость двухфакторной аутентификации. Если сотрудник привыкнет следить за собственной кибербезопасностью и осознает важность простейших правил, то уже не станет чинить препятствия при их внедрении на корпоративном уровне [3].

По статистике, наиболее распространенной причиной кибератак является человеческая ошибка. Вот почему обучение сотрудников кибергигиене является основой всех основ информационной безопасности компании. Независимо от того, насколько продвинутые антивирусы установлены, независимо от того, насколько профессионален отдел информационной безопасности, одна небольшая ошибка обычного менеджера – и база данных компании оказывается в руках злоумышленников или вредоносная программа проникает в сеть компании.

Регулярные занятия по кибербезопасности не только предотвращают подобные инциденты, но также могут помочь повысить осведомленность об угрозах и укрепить культуру безопасности организации [4].

Библиографические ссылки

1. Отчёт «Лаборатории Касперского» за 2024 год. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-security-awareness-training (дата обращения: 19.09.2025).

2. Примеры обучения сотрудников кибербезопасности. URL: https://rt-solar.ru/products/solar_dozor/blog/3817/ (дата обращения: 19.09.2025).

3. На страже периметра. Как обучить сотрудников основам кибербезопасности. URL: https://potok.io/blog/hr-howto/cybersecurity-education/. (дата обращения: 19.09.2025).

4. Необходимость обучения кибергигиене в современном цифровом мире. URL: https://1csoft.ru/publications/neobkhodimost-obucheniya-kibergigiene-v-sovremennom-tsifrovom-mire. (дата обращения: 19.09.2025).