УДК 004.056.53
DOI 10.33764/2618-981X-2024-8-2-183-187

Э. К. Сагилова[1], А. А. Христолюбова[2]*

Повышение осведомленности персонала в вопросах информационной безопасности как реализация личностно-ценностных и педагогических компетенций специалиста в области информационной безопасности

[1] Институт радиоэлектроники и информационных технологий – РТФ,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина», г. Екатеринбург, Российская Федерация
[2] Сибирский государственный автомобильно-дорожный университет (СибАДИ), г. Омск, Российская Федерация
* e-mail: sagilova.eila@yandex.ru

Аннотация. В статье рассматривается актуальность обладания специалистом в области информационной безопасности личностно-ценностными и педагогическими компетенциями и их связь по повышению осведомленности сотрудников предприятий в вопросах информационной безопасности как способа снижении рисков при утечке информации ограниченного доступа.

Ключевые слова: информационная безопасность, компетенции, управление информационной безопасностью, осведомленность персонала

E. K. Sagilova[1], A. A. Hristolyubova[2]*

Security Awareness Program as a Realization of Personality and Pedagogical Competence of a Specialist in Information Security

[1] Engineering School of Information Technologies, Telecommunications and Control Systems, Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N.Yeltsin», Ekaterinburg, Russian Federation
[2] Federal State Budget Educational Institution of Higher Education «The Siberian State Automobile and Highway University», Omsk, Russian Federation
* e-mail: sagilova.eila@yandex.ru

Abstract. The article examines the relevance of having a specialist in the field of information security with personal-value and pedagogical competencies and their relationship to increase awareness of enterprise employees in information security issues as a way to reduce risks in case of leakage of restricted access information.

Keywords: information security, competence, management of information security, security awareness program

Введение

Профессиональная сфера информационной безопасности амплифицирует не только аспекты компьютерной безопасности, но также включает в себя обеспечение безопасности коммуникаций, противодействие техническим формам

разведки и применение криптографических методов для защиты информации. Стандарты, предъявляемые к профессионалам в данной области, зависят от уникальных характеристик систем управления, информационных технологий и стратегий кадрового управления, применяемых внутри российских организаций. Это свидетельствует о том, что специалисты по информационной безопасности должны не только успешно выполнять свои трудовые обязанности в соответствии с профессиональными стандартами в области информационной безопасности, но и обладать педагогическими и ценностными качествами.

В [1] автор отмечает, что проблематика отсутствия достаточных педагогических компетенций начинает формироваться еще в ходе получения специалистами профессионального образования. Отмечается, что в структуре образовательных стандартов по направлению «Информационная безопасность» присутствует научно-педагогическая деятельность, однако соответствующей обязательной дисциплины не предусматривается.

Методы и материалы

Качественная подготовка персонала по вопросам безопасности информации значительно уменьшает риск случайных ошибок в обращении с конфиденциальными данными, что, в свою очередь, снижает вероятность несанкционированного доступа к ним. Любые грамотно выстроенные правила политики информационной безопасности, самые современные программные и технические средства защиты информации не будут эффективно выполнять свою задачу, если субъекты защиты информации – пользователи информационных систем недостаточно обучены безопасной работе с информацией.

Основной задачей исследования комплекса мотивационных факторов персонала является выявление интенсивности влияния различных факторов, определяющих отношение работников организации к действующим правилам информационной безопасности, а также изучение структуры мотивов к безопасности в зависимости от ценностных ориентаций работников исследуемых групп. В процессе исследования необходимо выявить влияние начального уровня осведомленности о правилах информационной безопасности на эффективность их выполнения, влияния уровня вознаграждения, а также влияния образования и квалификации на эффективность выполнения правил информационной безопасности.

При разработке исследования необходимо выделить ключевые причины, порождающие нарушения правил информационной безопасности, такие как:

– искажение правового сознания (правовой негативизм, правовой инфантилизм);

– неспособность сочувствовать, встать на сторону другого, низкий уровень эмпатичности личности;

– склонность разрешать конфликты насильственным путем;

– чрезмерная самооценка (видит в других только средство достижения своей цели);

– низкий заработок вследствие несправедливой оценки качеств работника;

– склонность работника к риску.

В работе [2] подчеркивается важность наличия высокого уровня эмоционального интеллекта у специалиста в области информационной безопасности. Среди желательных педагогических и личностно-ценностных навыков, которыми должен обладать специалист, можно выделить следующие: соблюдение этических норм в профессиональной деятельности, честность, ответственность, эмоциональная стабильность, умение контролировать свои поступки, умение сохранять конфиденциальность, бдительность, хорошие коммуникативные навыки и другие. Исследование показывает, что указанные личностные качества крайне важны для эффективной идентификации и оценки уязвимостей в области информационной безопасности.

Требования международного стандарта ГОСТ Р ИСО/МЭК 27001-2022 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» указывают на необходимость создания и поддержания в организации «атмосферы информационной безопасности». В целях решения этой задачи предлагается обучать работников правилам и требованиям, принятым на предприятии, обращать внимание на важность этих требований, повышать квалификацию ключевых пользователей информационных систем в области информационной безопасности. Таким образом, вышеперечисленные рекомендации выстраиваются в корпоративную систему повышения осведомленности персонала в вопросах информационной безопасности (аналог Security Awareness Program).

Для проведения наиболее эффективного внедрения программы повышения осведомленности персонала в вопросах информационной безопасности необходимо четко представлять задачу и ожидаемые результаты. В связи с относительно стабильной иерархией мотивов у взрослой категории работников мероприятия по обеспечению безопасности необходимо планировать, исходя из конкретной модели мотивов. Для этих целей служит специально разработанная программа (программа воспитательно-профилактической работы), частью которой является изучение мотивационных факторов групп персонала к выполнению правил информационной безопасности. Перед изучением мотивационных факторов групп персонала к выполнению правил информационной безопасности стоит учесть, что деление на законопослушных и нарушителей условно (очевидно, что все, хотя бы раз в жизни, нарушали установленные правила).

Исследователи [3] выделяют существенное значение непрерывности процессов повышения осознанности персонала в контексте обеспечения безопасности информации. Однако часто собственных ресурсов в организации может не хватать, что приводит к оказанию таких услуг специализированными организациями. В случае привлечения к решению поставленной задачи специализированной сторонней организации может возникнуть трудность, заключающаяся в том, что поставщики услуг и решений по обучению специалистов и повышению осве-

домленности персонала в области информационной безопасности недостаточно учитывают особенности организационной структуры и комплекса мотивационных факторов выполнения правил информационной безопасности персонала конкретной организации.

Результаты

Мероприятия, направленные на повышение осознанности сотрудников в области безопасности информации, должны базироваться на результатах исследования комплекса мотивационных факторов и ориентироваться на стимулирование положительных мотивов в каждой референтной группе сотрудников.

- мотив самоутверждения (повышение статуса, позитивная оценка личности);
- мотив идентификации с другим человеком;
- мотив власти;
- мотив интереса к процессу и содержанию деятельности;
- просоциальные мотивы (общественная значимость);
- мотивы угрозы наказания.

Большое значение для эффективности программы повышения осведомленности персонала в вопросах информационной безопасности имеют форма и представление агитационных и обучающих материалов. Содержание данных информационных материалов также должно разрабатываться индивидуально с учетом особенностей организационной культуры.

Обсуждение

В исследовании [1] приведен анализ программ подготовки специалистов в области корпоративной и информационной безопасности в странах Европы и США. Результаты показали, что лишь некоторые из этих программ включают педагогические и этические компоненты. Европейская стандартизированная модель цифровой грамотности для граждан выделяет важность развития не только навыков работы с информацией и данными, но также акцентирует внимание на формировании компетенций в области безопасности, охватывающих защиту персональных данных, здоровья человека и сохранение окружающей среды. Этот подход направлен на уменьшение вероятности возникновения компьютерных инцидентов из-за недостаточного уровня осведомленности пользователей [4].

Ожидается, что, специалисты в этой области должны не только обладать умениями преподавания информационных технологий и безопасности, но также эффективно участвовать в процессах предотвращения и устранения инцидентов информационной безопасности, вызванных человеческим фактором. Работодатели ожидают, что специалисты будут способствовать формированию личностно-ценностных компетенций у других сотрудников организации для более эффективного управления рисками в области информационной безопасности.

Современные отечественные образовательные стандарты подготовки специалистов в области информационной безопасности третьего поколения (или их

проекты) практически не содержат функциональных блоков, развивающих педагогические и личностно-ценностные компетенции [5, 6].

Заключение

Таким образом, в комплексе компетенций, которыми должен владеть специалист в области информационной безопасности, крайне востребованы педагогические и личностно-ценностные компетенции. Потребности потенциального специалиста в области информационной безопасности включают в себя не только внутренние механизмы моральной мотивации, но и способность эффективно взаимодействовать с индивидами, обладающими разнообразными ценностными системами. Кроме того, важно владеть навыками убеждения и воздействия для успешной передачи позитивных стимулов в области безопасного обращения с конфиденциальной информацией. При этом все эти компетенции должны быть подкреплены реальными технологиями и навыками в различных областях гуманитарных знаний: педагогике, социологии, юриспруденции, социальной психологии и т.д. Тем не менее, опыт показывает, что обладание специалистом в области информационной безопасности исключительно педагогическими компетенциями не позволяет ему качественно реализовывать свои задачи, если он не имеет убежденности в правильности политики информационной безопасности, вовлеченность в процессы обеспечения безопасности информации обеспечивается его личностно-ценностными компетенциями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Астахова, Л. В. Педагогическая компетенция будущего специалиста по защите информации в вузе: проблема развития и понятие / Л. В. Астахова // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. – 2014. – Т. 6, № 1. – С. 69–76. – EDN RYPUMB.

2. Астахова, Л. В. Эмоциональная компетентность будущего специалиста по защите информации: понятие и педагогические условия развития / Л. В. Астахова // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. – 2021. – Т. 13, № 2. – С. 88–95. – DOI 10.14529/ped210208. – EDN TPUUVN.

3. Вилкова, А. В. Проблемы непрерывного обучения персонала информационной безопасности / А. В. Вилкова, В. М. Литвишков, Б. А. Швырев // Уголовно-исполнительная система: право, экономика, управление. – 2019. – № 5. – С. 37–40. – DOI 10.18572/2072-4438-2019-5-37-40. – EDN HBMQJB.

4. Соколова, Е. И. Цифровые компетенции и новые технологии в образовании: по материалам документов европейской комиссии / Е. И. Соколова // Непрерывное образование: XXI век. – 2020. – № 2(30). – С. 121–133. – DOI 10.15393/j5.art.2020.5693. – EDN YIHRIU.

5. Васильева, Д. С. Модель компетентности специалиста по информационной безопасности в современных условиях / Д. С. Васильева, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2020. – Т. 6, № 1. – С. 53–59. – DOI 10.33764/2618-981X-2020-6-1-53-59. – EDN NRRKLT.

6. Воробьев, Е. Г. К вопросу разработки профессиональных стандартов в области информационной безопасности / Е. Г. Воробьев, А. К. Племянников // Методы и технические средства обеспечения безопасности информации. – 2015. – № 24. – С. 168-176. – EDN YPUVBB.