УДК 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Лебедева А.А., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *Человеческий фактор, информационная безопасность, культура информационной безопасности, политика безопасности, угрозы безопасности, осведомленность*

За последние два десятилетия наблюдается растущий интерес к вопросам связанным с человеком проблемами в сфере информационной безопасности. Пользователи, являющиеся сотрудниками компаний, признаются наиболее уязвимым звеном из-за множества угроз, которые могут потенциально повлиять на их безопасность. Данная статья представляет основные направления исследованияобеспечения безопасности информации. Подробно рассматриваются основные угрозы, связанные с целостностью и конфиденциальностью информации в организации, а также предлагаются эффективные меры по их противодействию.

Один из основных аспектов изучения человеческого фактора в информационной безопасности организации заключается в анализе поведенческих факторов, которые оказывают влияние на соблюдение политик безопасности сотрудниками. Также важным направлением исследований является анализ особенностей личности сотрудников, которые могут быть связаны с их склонностью к совершению киберпреступлений.

Одним из аспектов готовности к информационной безопасности является использование и регулярное обновление антивирусных приложений. Важным фактором также является готовность к резервированию данных и защите корпоративной сети [1].

Важным направлением исследований – как актуальное поведение может отличаться от их заявленных намерений, что представляет реальную опасность для информационной безопасности организации. Такие факторы, как нежелание соблюдать политику безопасности, лень или недостаточная мотивация, могут стать причиной утечки информации [5].

Одним из главных вопросов, требующих разрешения, является эффективный поиск методов увеличения заинтересованности сотрудников в вопросах информационной безопасности, что будет мотивировать их использовать соответствующие техники и следовать правилам безопасности на рабочем месте. Проблема изучения внутренней угрозы остается одним из наиболее известных аспектов человеческого фактора.

Так, согласно широко известным статистическим данным, более 75 % случаев нарушений в работе системы безопасности организации являются результатом инсайдерской деятельности. В этом смысле большаяугроза информационной безопасности находится не за пределами периметра безопасности, а в беспечных или злонамеренных действиях внутренних пользователей, таких как сотрудники или другие участники с доступом к ресурсам информации предприятия [2].

Другое направление исследований обращается к угрозам извне. В частности, отмечается, что технологии безопасности могут быть без труда преодолены при атаке неподготовленного пользователя с использованием техник социальной инженерии [4].

Компания Ideco 21 ноября 2023 года подвела итоги произошедших за год изменений на рынке информационной безопасности в России. С каждым годом в России происходит все больше краж данных из баз компаний: только в первом квартале 2023 уже было отмечено около 40 масштабных утечек персональных сведений. За первое полугодие 2023 года, число кибератак в отношении отечественных предприятий составило более 85 000 прецедентов, сравнивая с показателями того же периода 2022 года – 50000 случаев. Такая тенденция сильно изменила жизнь, как крупных компаний, так и малых и средних предприятий, заставляя внедрять актуальные технологии для защиты от хакеров.

Меры противодействия, предлагаемые исследователями, в общем случае включают три основных аспекта:

1) технологии и техники;

2) политики и практики;

3) образование и обучение.

При этом могут быть задействованы следующие превентивные меры:

1) психологические оценочные тесты для мониторинга сотрудников организации с целью определения наличия или отсутствия у них предпосылок к осуществлению инсайдерской деятельности;

2) скрининг безопасности, включающий в себя проверку бэкграунда и биографических данных сотрудников, их мотивацию, и др.;

3) правовые и организационные методы, включающие установление как политик и руководств, так и санкций за их несоблюдение [2].

Рекомендуемые для решения проблемы разрыва между знанием и поведением сотрудников в сфере информационной безопасности, в своюочередь, включают:

1) наказания;

2) инструкции по ситуационной этике;

3) повышение уровня осведомленности.

Для эффективного повышения качества политики безопасности организации рекомендуется усиление процедур безопасности, направленных на ситуационные факторы. Это позволит им иметь необходимые ресурсы для внедрения установленных процедур по повышению безопасности. Также следует улучшить внутреннюю согласованность между целями безопасности компании и ее практиками [6].

Особенно важным является комплексное обучение и информирование сотрудников организации. Такое обучение должно включать учебные курсы, практические семинары и презентации, посвященные безопасности при использовании интернет-ресурсов и корпоративных почтовых ящиков. Мотивационные постеры, предметы канцелярии и ролевые игры могут быть использованы для поддержки обучения.

Безопасное управление информационными системами продолжает сохранять решающее значение для финансового и репутационного благополучия предприятия. И хотя большинство организаций давно и успешно используют релевантные задаче технологии, проблема обеспечения информационной безопасности стоит все столь же остро по причине влияния человеческого фактора. Как следствие, область изучения поведенческих аспектов будет оставаться актуальной и все так же привлекать повышенный интерес к изучению и имплементации методов эффективного управления информационной безопасностью организации [3].

Библиографический список:

1. Актуальные киберугрозы: итоги 2020 года / PositiveTechnologies [2021]. [Электронный ресурс]. - Режим доступа: https://www.ptsecurity.com

2. Утечки информации ограниченного доступа: отчет за 9 месяцев 2020 г. / Экспертно-аналитический центр InfoWatch. [2020]. [Электронный ресурс]. - Режим доступа: https://d-russia.ru

3. «Лаборатория Касперского»: половина киберинцидентов происходит из-за человеческого фактора / Агентство международной информации Trend. [2017]. [Электронный ресурс]. - Режим доступа: https://www.trend.az

4. Гончаренко, Г. Ю. Компьютерная психология или универсальный подход к уязвимостям конфиденциальной информации / Г. Ю. Гончаренко, И. К. Ермаков, Д. А. Ермолатий, К. В. Пителинский // Вопросы защиты информации. - 2018. - № 4 (123). - С. 62-68.

5. Маркова, Д. Г. Человеческий фактор в информационной безопасности / Д. Г. Маркова // Известия тульского государственного университета. Технические науки. - 2018. - № 10. - С. 149-152.

6. Голубев, С. В. Актуальные вопросы информационной безопасности / С. В. Голубев, С. А. Голбуева // Материалы научно-практической конференции «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения». - Ульяновский ГАУ. – 2022. – С. 552-557.

INFORMATION SECURITY AND THE HUMAN FACTOR

Lebedeva A.A.
Scientific supervisor – Golubev S.V.
FSBEI HE Ulyanovsk SAU

Keywords: *Human factor, information security, information security culture, socio-organizational and psychological aspects, security policy, security threats, awareness*

Over the past two decades, there has been a growing interest in issues related to humans and socio-organizational problems in the field of information security. Users who are employees of companies are recognized as the most vulnerable link due to the many threats that can potentially affect their security. This article presents the main directions of research on the socio-organizational and psychological aspects of information security. The main threats related to the integrity and confidentiality of information in the organization are considered in detail, and effective measures to counter them are proposed.