Пырнова Ольга Александровна,

студентка 2-го курса,

Зарипова Римма Солтановна,

канд. техн. наук, доцент,

ФГБОУ ВО «Казанский государственный энергетический университет»,

г. Казань, Республика Татарстан, Россия

КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

В статье обращается внимание на важность культуры информационной безопасности и необходимость проведения дополнительных исследований, чтобы обеспечить всеобъемлющую основу создания культуры информационной безопасности в рамках организации.

Ключевые слова: информационная безопасность, защита информации.

Информация очень ценна для любой организации, и на ее защиту привлекают множество средств. Организации тратят миллиарды на работу с информацией, включая расходы на очистку и потерю данных, ответственность и потерю доверия клиентов. Одной из основных угроз для обеспечения безопасной среды для информационных активов в организации являются действия и поведение сотрудников при обращении с информацией. Недавнее исследование о нарушении данных указывает на то, что инсайдеры могут стоять за многими нарушениями, будь то намеренно или непреднамеренно. Ряд подобных исследований заключает, что инсайдеры представляют угрозу для защиты информации. Многочисленные исследования продолжают предполагать, что отношение людей и недостаточная осведомлённость о проблемах безопасности являются одними из самых важных факторов, влияющих на инциденты в сфере безопасности. Опрос, проведённый PWC, показал, что человеческая ошибка (а не технология) становится причиной большинства нарушений безопасности. Решением этой проблемы является создание культуры, обеспечивающей безопасность, в которой сотрудники должны быть более осведомлены о рисках и их обязанностях, что позволит им действовать разумно и безопасно. Культура, ориентированная на обеспечение

информационной безопасности, минимизирует риски для информационных активов и уменьшит риск ненадлежащего поведения сотрудников и вредного взаимодействия с информационными активами организации. Культура информационной безопасности определяется как способ, которым все это делается в организации для защиты информационных активов. В последнее время культура информационной безопасности все чаще рассматривается как способ внедрения методов обеспечения безопасности в организации [1]. Многие исследователи обратили внимание на важность и потребность в культуре информационной безопасности внутри организаций для управления рисками безопасности информационных активов.

Культура информационной безопасности – это субкультура организации, которая поддерживает все действия таким образом, что информационная безопасность становится естественным аспектом повседневной деятельности каждого сотрудника. Корпоративная культура руководит деятельностью организации и ее сотрудников, ограничивая деятельность и поведение сотрудников и предписывая, что организация и ее сотрудники должны, могут или не могут делать. Культура организации влияет на поведение сотрудников, поэтому ее следует использовать для установления поведения сотрудников в области информационной безопасности. Исследователи определяют культуру информационной безопасности по-разному. Некоторые исследователи рассматривают культуру информационной безопасности как цель, которая должна быть достигнута путем создания культуры, которая должна поддерживать все действия таким образом, чтобы информационная безопасность становилась естественным аспектом в повседневной деятельности каждого сотрудника. Другие рассматривают культуру информационной безопасности во время работы сотрудников и организации в целом в соответствии с принципами информационной безопасности. Культура информационной безопасности развивается в результате взаимодействия сотрудников с элементами управления информационной безопасностью, такими как пароли, карты доступа или антивирусное программное обеспечение.

Культура информационной безопасности включает в себя все социально-культурные меры, которые поддерживают технические методы безопасности информации [2].

Для улучшения культуры информационной безопасности существуют рекомендации, которых стоит придерживаться в организациях. Руководству нужно назначить команду или человека, которые возмут на себя ответственность за привитие правильного пути в отношении информационной безопасности. На индивидуальном уровне работникам необходимо руководствоваться тем, какое поведение является приемлемым, а какое – нет. Организации необходимо внедрить такие процедуры, как просветительские сессии и учебные программы для поддержки и передачи политики информационной безопасности. Это побудит сотрудников придерживаться политики информационной безопасности, тем самым прививая правильное поведение, которое необходимо для приемлемой культуры информационной безопасности. Из вышесказанного следует, что в культуре информационной безопасности существует много вопросов, которые необходимо решить в отношении этой культуры. Исходя из исследований, организации могут внедрять методы информационной безопасности в рамках своей повседневной деятельности в организации, которая со временем станет частью культуры информационной безопасности организации [3]. Культура информационной безопасности организации должна быть улучшена за счет человеческого поведения.

СПИСОК ЛИТЕРАТУРЫ

1. Бикмухаметов И.И. Кибертерроризм как угроза информационной безопасности / И.И. Бикмухаметов, Р.С. Зарипова // Аллея науки. – 2018. – Т.1. – №2(18). – С. 266-268.

2. Шакиров А.А. Обеспечение информационной безопасности организаций / А.А. Шакиров, Р.С. Зарипова // Аллея науки. – 2018. – Т.3. – №1(17). – С.841-843.

3. Шакиров А.А. Актуальность обеспечения информационной безопасности в условиях цифровой экономики / Шакиров А.А., Зарипова Р.С. / Инновационное развитие экономики. Будущее России: Сборник материалов V Всероссийской (национальной) научно-практической конференции. – 2018. – С. 257-260.