Бурдастых Юлия Николаевна
студентка
Дюмина Светлана Васильевна
канд. пед. наук, доцент, преподаватель
ФГБОУ ВО «Юго-Западный
государственный университет»
г. Курск, Курская область

АНАЛИЗ ПСИХОЛОГИЧЕСКИХ ФАКТОРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *в данной статье были классифицированы человеческие факторы, являющиеся источниками реализации угроз. Также указаны меры их ликвидации.*

Ключевые слова*: психологический фактор, угроза, безопасность, автоматизированная система, человеческий фактор, персональные данные.*

Говоря о психологических аспектах, специалисты обычно выделяют две формы его негативного выражения. Например, Андрей Прозоров, руководитель экспертного направления Solar Security, охарактеризовывает их следующим образом: «Первая – ошибки и халатность персонала, вторая – личная мотивация, которая может сказываться на принимаемых решениях». Наиболее уязвимым компонентом в информационной безопасности считается человек, как основной элемент автоматизированной информационной системы. Психологический фактор оказывает большое воздействие на обеспечение безопасности объекта защиты в целом.

Исходя из практики были сформированы основные факторы, которые оказывают серьезное влияние на поведение сотрудников безопасности, и меры по их ликвидации.

1. Недостаток мотивации

Мотивировать персонал в сфере безопасности не просто. Безопасность – это понятие, которое очень трудно оценить количественно, соблюдение правил не

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

приносит дополнительный доход, а лишь сокращает расходы. Поэтому мотивация сотрудников может быть достигнута тремя путями: наказание за нарушение, информирование и поощрение за выполнение правил.

2. Недостаток осведомленности в области защиты информации

Недостаток осведомленности ликвидируется с помощью информирования. Источником информирования являются инструктажи, они могут быть вводными, дополнительными, периодическими. Очень важно, чтобы сама форма подачи инструктажа была доступной. Обязателен также контроль усвояемости информации в виде контрольного тестирования.

3. Убеждение

Мало убедить сотрудников в важности поддержания уровня безопасности, нужно научить их безопасным методам работы. Правила должны быть выполнимы, просты, понятны, лучше, если по каждому вопросу будет составлена краткая памятка. И конечно же, самое доходчивое объяснение – объяснение на примерах, стоит показать, что будет, если пропадет вся клиентская база либо годовой отчет, бюджет предприятия, что будет, если в здание проникнет злоумышленник или ограбят кассу. Это должно впечатлить сотрудников.

4. Неграмотное пользование технологиями

Неграмотное пользование технологиями может привести к различным опасностям в области компьютерной безопасности. Их можно систематизировать несколькими методами: превышение полномочий, промах, халатность, социальная инженерия, несанкционированный доступ и т. д. Рассмотрим неудачный пример из жизни. «В вооруженных силах Украины (ВСУ) для доступа на сервера автоматизированной системы управления войсками «Днипро» использовались пароли admin и 123456. Об этом сообщает агентство УНИАН со ссылкой на журналиста Александра Дубинского» Отмечается, что такая защита просуществовала не один год и позволяла посторонним людям сканировать информацию об украинских военных. Напомню, что персональные данные военных с недавних пор приравнивают к государственной тайне. Таким образом, без особых навыков по информационной безопасности можно свободно иметь доступ к программно-

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

аппаратным средствам защиты, а соответственно к огромному массиву секретной информации вооруженных сил.

Вывод

Информационная безопасность – понятие мнимое, обманчивое, призрачное не имеющее материального выражения. Поэтому не стоит думать, что высокий уровень безопасности зависит только от качества аппаратного средства защиты. Наоборот от того, как будут учтены в информационных процессах психологические установки сотрудников зависит уровень защищенности информации. В данной статье была предпринята попытка собрать и внятно классифицировать человеческие факторы, вызывающие трудности безопасности для их дальнейшего преодоления.

Список литературы

1. [Электронный ресурс]. – Режим доступа: http://texno.group/news/show-23

2. [Электронный ресурс]. – Режим доступа: http://www.s-director.ru/magazine/magdocs/view/96.html

3. [Электронный ресурс]. – Режим доступа: http://bishelp.ru/business/motivirovanie-sotrudnikov-na-obshchuyu-bezopasnost-kompanii

4. [Электронный ресурс]. – Режим доступа: https://docplayer.ru/58008869-Udk-331–5-metody-raboty-s-personalom-v-ramkah-sistemy-zashchity-informacii.html

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)