УДК 004.056

ОЦЕНКА ЗАЩИЩЕННОСТИ ЦИФРОВЫХ ДВОЙНИКОВ ПАЦИЕНТОВ

Ласкус Е.О. (Университет ИТМО)
Научный руководитель – доцент (квалификационная категория «ординарный доцент») Коржук В.М.
(Университет ИТМО)

Введение. Цифровой двойник — это «система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием (при наличии изделия) и (или) его составными частями», то есть виртуальная копия какого-либо объекта, которая достоверно воспроизводит все происходящие на оригинальном объекте процессы в режиме реального времени, так что в каждый момент времени параметры состояния цифрового двойника соответствуют параметрам состояния физического объекта [1]. Несмотря на распространенное применение цифровых двойников [2], в настоящее время до конца не сформирован единообразный подход к формированию модели угроз цифровых двойников, не разрешены правовые отношения между требованиями к защите персональных данных и врачебной тайны, не регламентирован порядок оценки рисков цифровых двойников; что позволяет говорить об актуальности данной работы.

Основная часть. Для оценки защищенности цифровых двойников пациентов было решено применить модель зрелости безопасности интернета вещей с использованием иерархии практик обеспечения безопасности (security practices) [3]. Практикой обеспечения безопасности, к примеру, является реализация контроля доступа, защита данных при их хранении и передаче или управление обновлениями безопасности. Системный подход к выбору вариантов защиты поддерживается группированием практик по ожидаемому эффекту от их применения.

Для определения защищенности выполняются следующие шаги:

1) Определить потребность компании в повышении безопасности объекта.

1.1) Определить, насколько угрозы различного типа атак актуальны для предприятия:

1.2) Определить масштаб возможных репутационных, финансовых потерь и юридические риски для компании и её сотрудников в случае успешной кибератаки на системы реализации цифровых двойников.

1.3) Определить набор необходимых к реализации требований по безопасности от регуляторов и оценить риски их невыполнения.

2) Сформулировать цели безопасности, достижение которых необходимо для бесперебойного функционирования системы цифровых двойников и получения запланированной прибыли.

2.1) Обеспечить выполнение обязательных требований регулятора.

2.2) Защитить наиболее важные для бизнес- и технологического процесса организации информационные системы и системы автоматизации от потенциальных атак.

2.3) Защитить системы предприятия, необходимые для обеспечения безопасности сотрудников и защиты окружающей среды, от любых возможных воздействий со стороны потенциальных злоумышленников.

2.4) Защититься от юридических рисков, связанных с возможной недостаточной защитой от новых и технически сложных угроз.

2.5) Переложить финансовые риски, от угроз, от которых защита не была предусмотрена, на третью сторону (например, на страховую компанию).

3) Установить сроки реализации для каждой из сформулированных целей безопасности.

4) Определить, какие ресурсы компания готова выделить на достижение поставленных целей безопасности, спланировать выделение ресурсов для достижения поставленных целей в заданные сроки.

5) Выбрать процессы, меры и средства реализации сформулированных целей безопасности в установленные сроки с учётом спланированного выделения бюджета.
6) Определить приоритеты, дорожную карту внедрения выбранных мер и спланировать выделение ресурсов на каждую из мер.
7) Рассчитать коэффициенты важности подсистем значимых и незначимых объектов. Расчет значений этих коэффициентов выполняется на основе мнения группы экспертов.
8) Провести контроль реализации требований членами экспертной группы, осуществляющими аудит ИБ. В процессе анкетирования оценивается выполнение/не выполнение требований.
9) Вычисление значений показателей уровня защищенности цифровых двойников пациентов.

Использование модели зрелости позволяет оптимизировать постановку задачи безопасности, то есть определить уровень «достаточной безопасности», провести оценку и планирование объема работ, которые необходимо провести для её достижения с требуемой детализацией, начиная с уровня доменов безопасности вплоть до отдельных практик.

Выводы. Проведен анализ возможности применения модели зрелости безопасности интернета вещей и на её основе разработана методика оценки защищенности информационных систем цифровых двойников пациентов. В дальнейшем планируется провести апробацию результатов в реальных условиях.

Список использованных источников:

1. ГОСТ Р 57700.37-2021 «Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения»;
2. Цифровые технологии в российской экономике / К.О. Вишневский, Л.М. Гохберг , В.В. Дементьев и др.; под ред. Л.М. Гохберга ; Нац. исслед . ун т «Высшая школа экономики». М.: НИУ ВШЭ, 2021. 116 с. 400 экз. ISBN 978 5 7598 2199 1;
3. IoT Security Maturity Model (SMM). Description and Intended Us. An Industrial Internet Consortium White Paper. Version 1.2 – 2020-05-05. Sandy Carielli (Entrust Datacard), Matt Eble (Praetorian), Frederick Hirsch (Fujitsu), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft)

Ласкус Е.О. (автор) Подпись

Коржук В.М. (научный руководитель) Подпись