Секция «Проблемы финансовых расследований и экономической безопасности»

Проблемы безопасности и оценка рисков в рамках деятельности аудиторской компании Deloitte

Научный руководитель – Ниязбекова Шакизада Утеулиевна

Егорова А.В.[1], *Молодчиков А.А.*[1]

1 - Московский университет имени С.Ю. Витте, Факультет экономики и финансов, Кафедра финансов и кредита, Москва, Россия

Deloitte (DLT) - международная компания по предоставлению консультационных и аудиторских услуг.

Смарт-контракты определяются как юридически обязательные контракты, новые средства контроля кибербезопасности необходимо для обеспечения хранения и хранения данных в безопасной обстановке. Но большинство существующих видов стандартов кибербезопасности также будут по-прежнему применяться. [1]

Любой код, разработанный для безопасности смарт-контрактов должен придерживаться лучших практик безопасности и должен регулярно пересматриваться, чтобы гарантировать, что вновь открывшиеся проблемы безопасности отсутствуют в устаревшем коде. [2]

DLT также представляет проблемы интеграции с аппаратными модулями безопасности (HSM[1]) для хранения ключей и генерации, и инфраструктура безопасности как виртуальные частные сети (VPN[2]). Этот интерфейс как правило, защищен с помощью учетных данных сети системы (связанная с корпоративным каталогом) или пользовательским механизмом аутентификации пароля.

Интеграция с точки зрения данных это относительно просто через стандартные интерфейсы программирования, предполагая, что интеграция данных происходит в установленные рамки и стандарты безопасности процесса ETL[3]. Уязвимостью смарт-контракта может быть риск несанкционированного доступа к системе записи данных, аудита безопасности и базы правил аудита кода для известных уязвимостей и потенциальные дыры в безопасности должны стать частью области аудита для блокчейнов. Следовательно, проблемы безопасности и оценки рисков аудита будут критическим видом деятельности при проведении аудита клиента с блокчейн-реализациями. [1]

Безопасность ключей имеет решающее значение. Двадцать шесть нарушений (см. табл. 1), связанные с кражей или несанкционированным контролем эти ключи могут иметь серьезные последствия для платформы с применением ДОТ[4]. [3]

Альтернативный подход заключается в обеспечении того, чтобы все данные, записанные в цепочку, шифруются. Когда ключи шифрования для "забытых" данных уничтожаются, данные выводятся нечитаемыми. Если этот подход принят, шифрование должно реализовываться с самого начала, позже осуществление вряд ли возможно. Другие угрозы включают авансы в квантовых вычислениях, которые отображают ядро криптографические компоненты, устаревшие или поврежденные целостность данных, зашифрованных скомпрометированных алгоритмов. [4]

Принципы управления технологическими рисками, ИКТ[5] элементы управления могут быть разбиты на пять различных областей деятельности: система; управление безопасностью развитие и Управление изменениями; информация обработка; коммуникационные сети; управление поставщиками технологических услуг. [5]

1 HSM (hardware security module) — специализированный вычислитель, который выполняет различные криптографические операции.

2 VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

3 ETL (от англ. Extract, Transform, Load — дословно «извлечение, преобразование, загрузка») — один из основных процессов в управлении хранилищами данных.

4 ДОТ - дистанционные образовательные технологии.

5 Информационно-коммуникационные технологии.

Источники и литература

1) https://www2.deloitte.com/ru/ru.html
2) Аналитический отчет «Шесть принципов контроля и управления для блокчен-решений, используемых при оказании финансовых услуг» (“Six Control Principles for Financial Services Blockchains. October 2017”, Deloitte).
3) https://lektsii.org/8-20438.html
4) Коротков А.П. Преступления в сфере экономической деятельности как угроза экономической безопасности России. - М.: ПРИОР, 2006.
5) Молчанов А.В. Экономическая безопасность финансовой системы России на современном этапе: сб. тр. – М.: аЭБ МВД России, 2007.

Иллюстрации

Таблица 1

№	Наименование метода
1	Метод следования "За дураком"
2	Метод "За хвост"
3	Метод "Компьютерный абордаж"
4	Метод "Неспешного выбора"
5	Метод "Поиск бреши"
6	Метод "Люк"
7	Метод "Маскарад"
8	Метод "Мистификация"
9	Метод "Аварийный"
10	Метод "Склад без стен"
11	Методы манипуляции
12	Манипуляция с пультом управления
13	"Троянский конь"
14	"Логическая бомба"
15	"Временная бомба"
15	"Асинхронная атака"
16	Моделирование
17	Реверсивная модель
18	"Воздушный змей"
19	Взлом" изнутри
20	Взлом" извне
21	Хищение информации
22	Хищение услуг

Рис. 1. Таблица 1.