

Д.А. Саяков, daniyar.sayakov@yandex.ru

Национальный исследовательский ядерный университет «МИФИ», г. Москва

ИДЕНТИФИКАЦИЯ АКТИВОВ НАЦИОНАЛЬНОЙ ЦИФРОВОЙ ВАЛЮТЫ И ВЫЯВЛЕНИЕ УГРОЗ

Обосновывается задача идентификации активов национальной цифровой валюты, и на ее основе разработка модели угроз и модели нарушителя имеет целью предсказать и смоделировать возможные угрозы и нарушения, которые могут нанести ущерб национальной цифровой валюте. Данная работа может быть использована в области кибербезопасности и разработке политик и стратегий для защиты национальных цифровых валют от противозаконных действий и несанкционированного доступа.

Ключевые слова: национальная цифровая валюта, идентификация активов цифровой валюты, разработка модели угроз, разработка модели нарушителя, защита национальной цифровой валюты

Описание архитектуры цифрового сома

Цифровая валюта имеет элементы наличных, безналичных денежных средств и криптовалюты, но ни под один не подходит целиком. Как и наличные, она выпускается государственным эмитентом (Национальным банком) в объеме, необходимом для монетарной политики конкретного государства. Но при этом цифровая валюта не имеет материального воплощения, а представляет собой цифровой код. В этом плане она похожа на классический банковский счет, где деньги лежат в виде записи в соответствующем реестре. Однако в отличие от банковского счета ответственность за сохранность средств на счете клиента несет не коммерческий банк, а опять-таки государственный регулятор рынка. С криптовалютами цифровую валюту роднит блокчейн, но крипто может эмитировать любой аноним, а не только государственный эмитент[1].

Переход на цифровую валюту не устраняет риски, связанные с выпуском наличной валюты, такие как инфляция и колебания курса. Когда цифровая валюта выпускается в обращение, один наличный сом будет изыматься из оборота. Однако появляется возможность проводить финансовые операции без посредников. Цифровые деньги переходят непосредственно с одного электронного кошелька на другой, минуя коммерческие банки. Такие переводы могут осуществляться даже без доступа к интернету и не требуют наличия банковского счета.

Полностью без коммерческих банков не обойтись, так как "цифровые кошельки" будут храниться на их серверах. Связано это с тем, чтобы снизить нагрузку на серверы национального банка, а также сократить расходы на приобретение или обновление оборудования. В случае DoS/DDoS атак время на совершение транзакции увеличится или произойдет сбой, что вызовет хаос среди пользователей и выведет из строя банковскую систему страны. Предполагается, что коммерческие банки не будут взимать комиссию за услуги по переводу денежных средств, на рисунке 1 показана схема работы цифровой валюты с участием коммерческих банков.

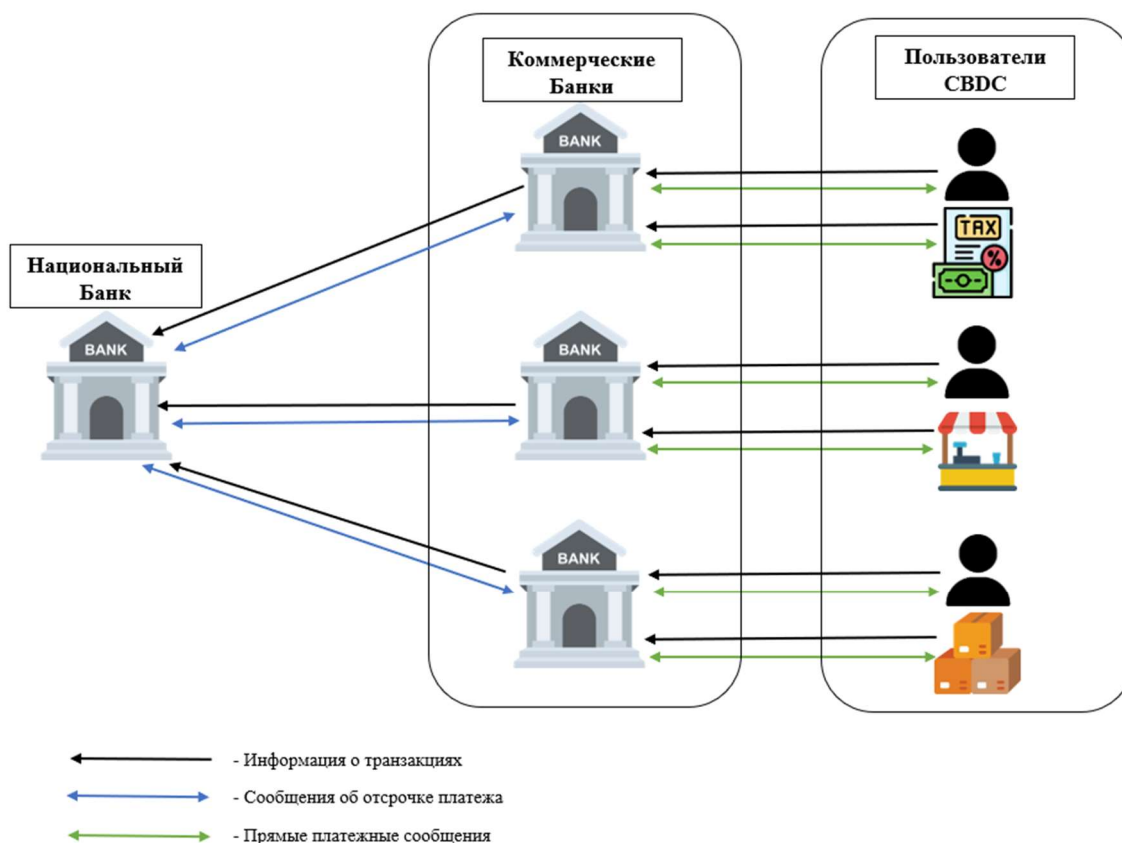


Рисунок 1 – Схема работы коммерческих банков с цифровой валютой (источник: рисунок автора)

Для пополнения своего кошелька кредитная организация направляет в Национальный банк запрос на эмиссию цифрового сома. Национальный банк списывает безналичные средства с корреспондентского счета кредитной организации и проводит эмиссию цифрового сома в эквивалентном объеме (рис.2).

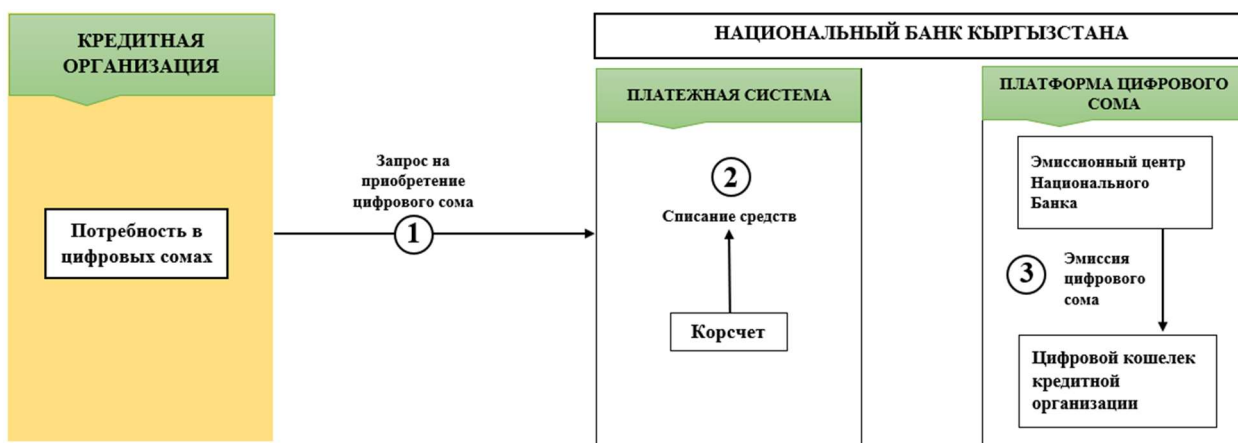


Рисунок 2 – Прототип схемы эмиссии цифрового сома (источник:

<https://rulaws.ru/acts/Kontseptsiya-tsifrovogo-rublya-%28podgotovlena-Bankom-Rossii%29/>, дата обращения: 30.11.2023)

1. Кредитная организация направляет запрос на пополнение своего счета цифровых сомов.
2. Национальный банк КР списывает средства с корсчета кредитной организации.

3. Национальный банк КР зачисляет цифровые сомы на счет кредитной организации в объеме средств, списанных с корсчета.



Рисунок 3 – Прототип схемы пополнения кошелька клиентом (источник:

<https://rulaws.ru/acts/Kontsepsiya-tsifrovogo-rublya-%28podgotovlena-Bankom-Rossii%29/>, дата обращения: 30.11.2023)

1. Клиент через мобильное приложение кредитной организации отправляет запрос на пополнение своего цифрового кошелька.
2. Кредитная организация выполняет процедуры, предусмотренные законодательством в сфере ПОД/ФТ/ФРОМУ, валютным законодательством, и списывает средства со счета клиента.
3. Кредитная организация зачисляет цифровые сомы со своего кошелька на кошелек клиента.
4. Платформа цифрового сома направляет клиенту через мобильное приложение кредитной организации уведомление о зачислении цифровых сомов на его кошелек.

Аналогично представленной схеме на рисунке 3 цифровые сомы могут перемещаться со счета одного клиента на счет другого.

Прототип платформы цифрового сома

В прототипе платформы цифрового сома будет предусмотрено подключение участников со следующими функциями:

- Национальный банк – оператор платформы цифрового сома и эмитент цифрового сома.
- Кредитные организации – участники платформы цифрового сома, выполняющие платежи по поручениям своих клиентов на платформе цифрового сома.
- Физические и юридические лица – пользователи платформы цифрового сома, получающие доступ к своим кошелькам на платформе цифрового сома через кредитные организации.

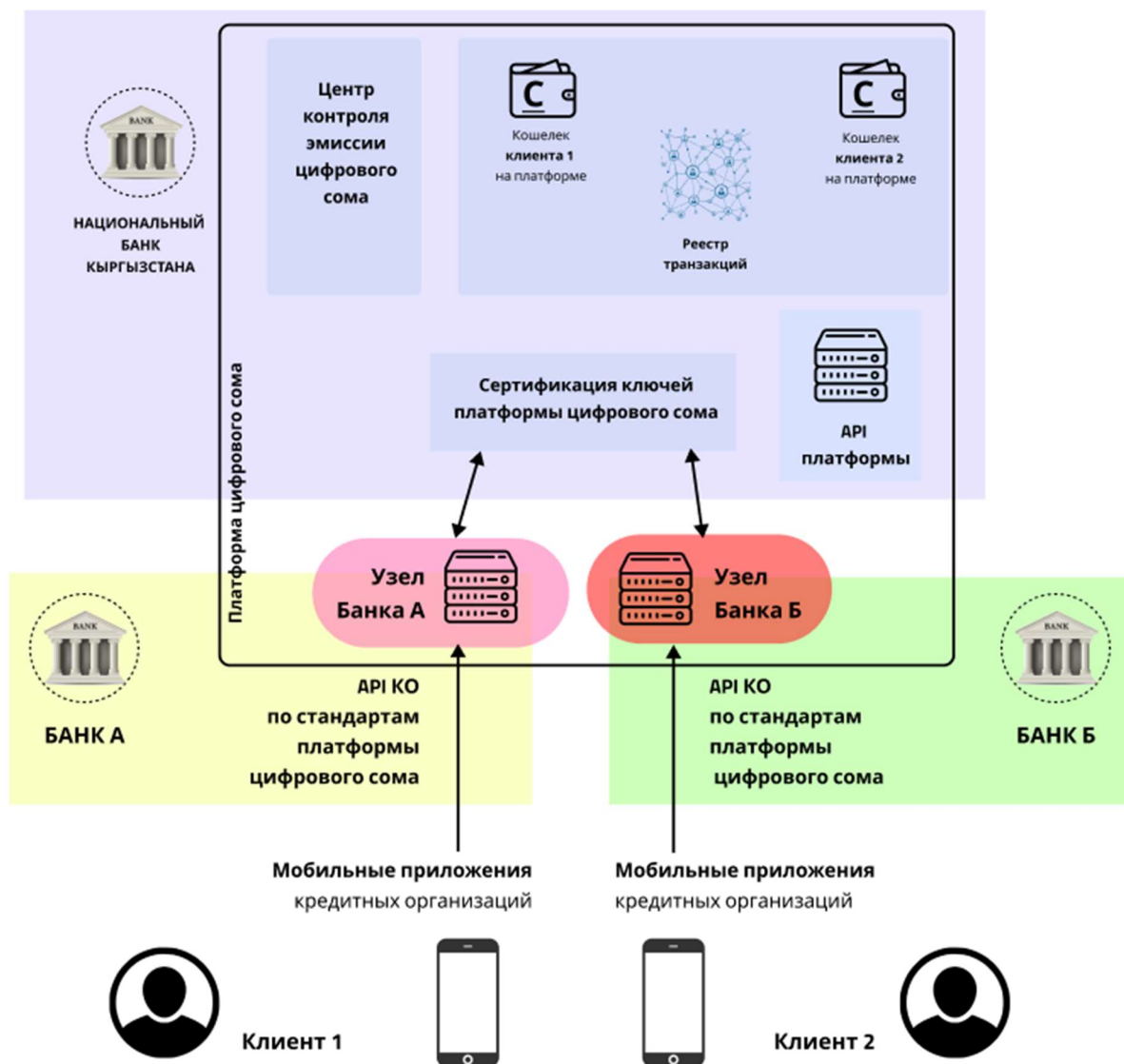


Рисунок 4 – Прототип архитектуры цифрового сома (источник: <https://rulaws.ru/acts/Kontseptsiya-tsifrovogo-rublya-%28podgotovlena-Bankom-Rossii%29/>, дата обращения: 30.11.2023)

На рисунке 5 представлена угроза целостности данных в канале передачи цифрового сома.

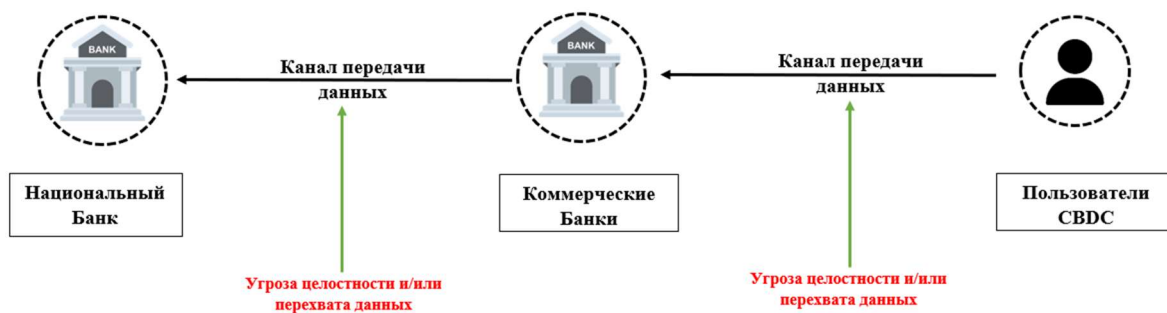
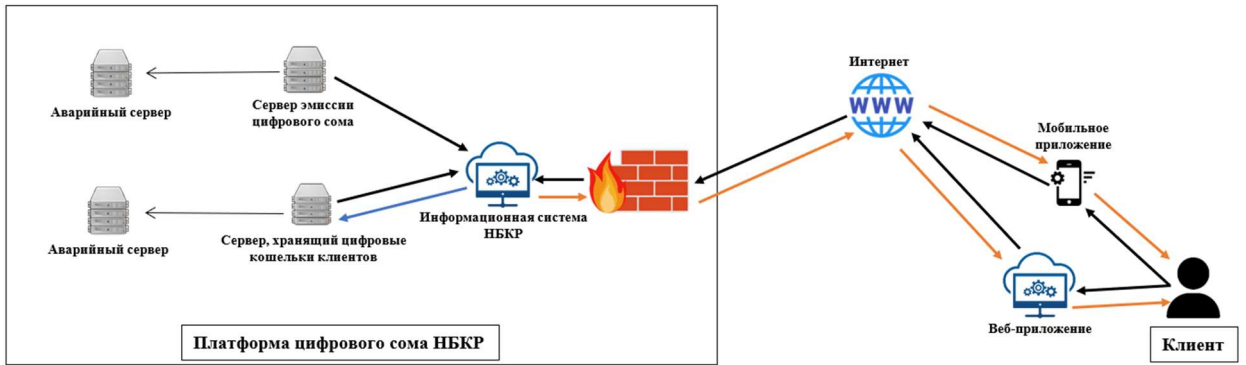


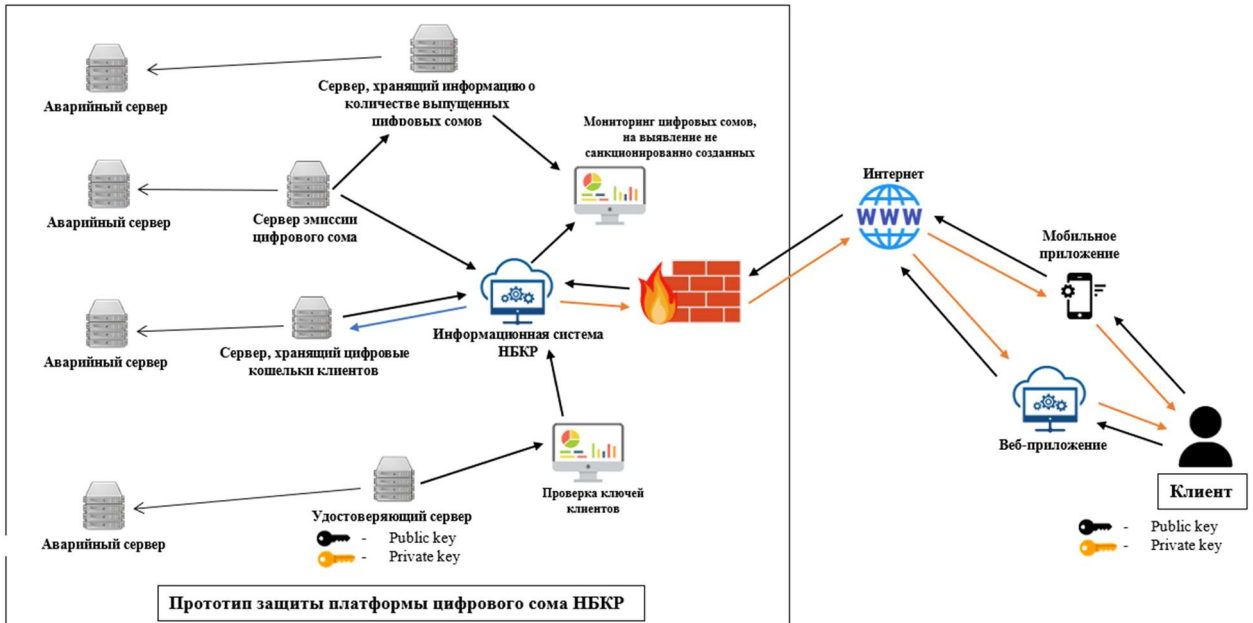
Рисунок 5 – Угроза целостности данных, передаваемых по каналу передачи платформы цифрового сома (источник: рисунок автора)



- ← - создание резервной копии данных
- - передача данных на информационную систему НБКР цифрового сома
- - обновление данных цифрового кошелька клиента
- - обновление информации о счете цифрового кошелька клиента

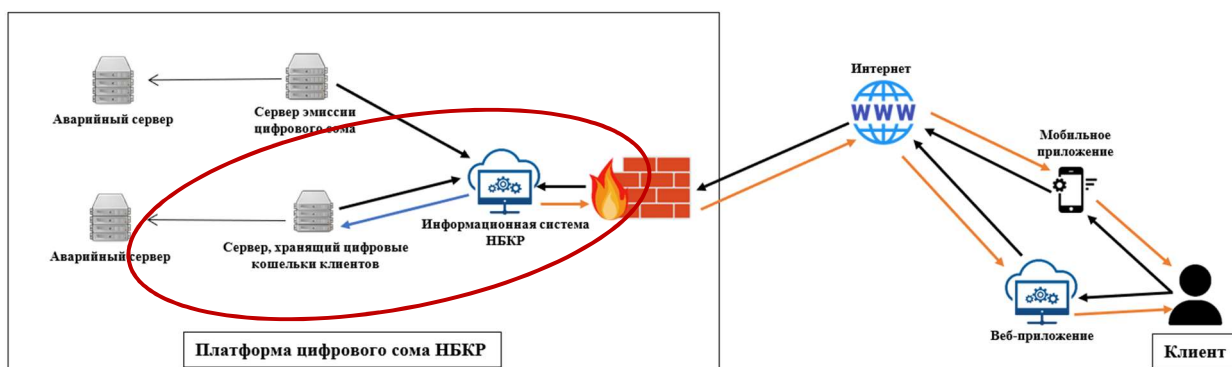
Рисунок 6 – Прототип схемы работы клиента с платформой цифрового сома (источник: рисунок автора)

На рисунке 6 показаны основные компоненты для работы платформы цифрового сома [2].



- ← - создание резервной копии данных
- - передача данных на информационную систему НБКР цифрового сома
- - обновление данных цифрового кошелька клиента
- - обновление информации о счете цифрового кошелька клиента

Рисунок 7 – Прототип схемы защиты платформы цифрового сома (источник: рисунок автора)



- ← - создание резервной копии данных
- - передача данных на информационную систему НБКР цифрового сома
- - обновление данных цифрового кошелька клиента
- - обновление информации о счете цифрового кошелька клиента

Рисунок 8 – Рассмотрение схемы платформы цифрового сома для идентификации активов (источник: рисунок автора)

Классификация обрабатываемой информации на платформе цифрового сома

На платформе цифрового сома обрабатывается информация ограниченного доступа.

В категорию «информация ограниченного доступа» включена следующая информация:

- Информация о коде (ПО). Свойства ИБ (в порядке приоритета): К, Ц, Д;
- Информация о цифровых кошельках клиентов. Свойства ИБ (в порядке приоритета): К, Ц, Д;
- Информация о пользователях. Свойства ИБ (в порядке приоритета): К, Ц, Д.

Инфраструктура ИС платформы цифрового сома

Инфраструктура ИС цифрового сома включает в себя следующие элементы:

- ПК сотрудников;
- Маршрутизатор Mercusys MR50G;
- Сервер (процессор IntelXeonGold 6128);
- ОС Astra GNU/Linux;

Для аппаратного актива процессор Intel Xeon Gold 6128 были выявлены следующие уязвимости:

- BDU:2023-00942;
- BDU:2020-05478;
- BDU:2020-00180;
- BDU:2020-00130.

Для программного актива ОС Astra GNU/Linux были выявлены следующие уязвимости:

- BDU:2021-00101;
- BDU:2021-05090.

Для телекоммуникационного актива Mercusys MR50G была выявлена следующая уязвимость:

- Отсутствие аутентификации на точке доступа Wi-Fi вследствие ошибки конфигурации сетевого оборудования.

Анализ угроз ИБ ИС платформы цифрового сома

На основе выявленных уязвимостей активов среды обработки информационных активов, а также рекомендаций документов:

- «РС БР ИББС 2.2-2009. Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы

Российской Федерации. Методика оценки рисков нарушения информационной безопасности» [6];

- Методика оценки угроз безопасности информации. Документ утвержден ФСТЭК России 05.02.2021», – будет сформирован предварительный перечень угроз ИБ ИС платформы цифрового сома[7].

Далее, основываясь на рекомендациях следующих документов:

- Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн). Документ утвержден приказом ФСТЭК России от 14 февраля 2008 г.[7];
- Методика определения актуальных угроз безопасности информации в информационных системах. Проект документа ФСТЭК России (2015 г.), были выявлены актуальные угрозы ИБ ИС платформы цифрового сома[7].

Информационный актив ИА-1 обрабатывается в следующих активах среды обработки информационных активов:

- телекоммуникационный актив Mercusys MR50G, для которого были выявлены следующие уязвимости: отсутствие аутентификации на точке доступа Wi-Fi вследствие ошибки конфигурации сетевого оборудования. Антропогенный (внешний нарушитель), эксплуатируя данную уязвимость, может реализовать следующий перечень угроз:
 - a. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне из-за отсутствия аутентификации на точке доступа Wi-Fi. Реализация данной угрозы приведет к нарушению конфиденциальности информационного актива. Ущерб от реализации данной угрозы для организации – репутационный (снижение престижа).
 - b. Угроза нарушения целостности данных вследствие деятельности внешнего нарушителя в контролируемой зоне из-за отсутствия аутентификации на точке доступа Wi-Fi. Ущерб от реализации данной угрозы следующий: для информационного актива – нарушение целостности; для ИТ-сервиса – нарушение доступности, для организации – экономический (потеря конкурентного преимущества).
 - c. Угроза нарушения доступности данных из-за сбоя или отказа сетевого оборудования вследствие деятельности внешнего нарушителя в контролируемой зоне из-за отсутствия аутентификации на точке доступа Wi-Fi. Ущерб от реализации данной угрозы следующий: для информационного актива – нарушение доступности; для актива среды обработки информационного актива – нарушение доступности; для ИТ-сервиса – нарушение доступности, для организации – экономический (потеря конкурентного преимущества, закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) и технологический (необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций));
- аппаратный актив Intel Xeon Gold 6128, для которого была выявлена следующая уязвимость: BDU:2023-00942 Уязвимость функции spectre_v2_select_mitigation() ядра операционной системы Linux связана с ошибками работы процессоров Intel при обработке инструкции RET после завершения работы виртуальной машины. Антропогенный (внешний нарушитель), эксплуатируя данную уязвимость, может реализовать следующую угрозу:
 - a. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне связана с ошибками работы процессоров Intel при обработке инструкции RET. Реализация данной угрозы

- приведет к нарушению конфиденциальности информационного актива. Ущерб от реализации данной угрозы для организации – репутационный (снижение престижа).
- аппаратный актив Intel Xeon Gold 6128, для которого была выявлена следующая уязвимость: BDU:2020-05478 Уязвимость процессоров Intel связана с недостатками разграничения доступа. Антропогенный (внешний нарушитель), эксплуатируя данную уязвимость, может реализовать следующую угрозу:
 - а. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне связана с недостатками разграничения доступа в процессоре Intel. Реализация данной угрозы приведет к нарушению конфиденциальности информационного актива. Ущерб от реализации данной угрозы для организации – репутационный (снижение престижа).
 - аппаратный актив Intel Xeon Gold 6128, для которого была выявлена следующая уязвимость: BDU:2020-00180 Уязвимость микропрограммного обеспечения процессоров Intel Xeon связана с недостаточной проверкой необычных или исключительных состояний. Антропогенный (внешний нарушитель), эксплуатируя данную уязвимость, может реализовать следующую угрозу:
 - а. Угроза нарушения доступности данных вследствие деятельности внешнего нарушителя в контролируемой зоне из-за недостаточной проверки состояний процессоров Intel Xeon. Ущерб от реализации данной угрозы следующий: для информационного актива – нарушение доступности; для актива среды обработки информационного актива – нарушение доступности; для ИТ-сервиса – нарушение доступности, для организации – экономический (потеря конкурентного преимущества, закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) и технологический (необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций));
 - аппаратный актив Intel Xeon Gold 6128, для которого была выявлена следующая уязвимость: BDU:2020-00130 Уязвимость реализации технологии Intel Transactional Synchronization Extension (TSX) микропрограммного обеспечения процессоров Intel связана с отсутствием защиты служебных данных. Антропогенный (внешний нарушитель), эксплуатируя данную уязвимость, может реализовать следующую угрозу:
 - а. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне связана с отсутствием защиты служебных данных процессоров Intel. Реализация данной угрозы приведет к нарушению конфиденциальности информационного актива. Ущерб от реализации данной угрозы для организации – репутационный (снижение престижа).
 - программного актива ОС Astra GNU/Linux, для которого была выявлена следующая уязвимость: BDU:2021-00101 Уязвимость функции `nsm_drop_privileges` (`support/nsm/file.c` пакета NFS утилит `nfs-utils`) связана с неправильным присвоением стандартных разрешений. Антропогенный (внешний нарушитель), эксплуатируя данную уязвимость, может реализовать следующую угрозу:
 - а. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне, связанная с неправильным присвоением стандартных разрешений. Реализация данной угрозы приведет к нарушению конфиденциальности информационного актива. Ущерб от реализации данной угрозы для организации – репутационный (снижение престижа).

- программного актива ОС Astra GNU/Linux, для которого была выявлена следующая уязвимость: BDU:2021-05090 Уязвимость компонента string.c пакета criu операционной системы Debian GNU/Linux вызвана целочисленным переполнением. Антропогенный (внешний нарушитель), эксплуатируя данную уязвимость, может реализовать следующую угрозу:

- а. Угроза нарушения доступности данных вследствие деятельности внешнего нарушителя в контролируемой зоне, позволяющая нарушителю вызвать переполнение стека в ОС DebianGNU/Linux. Ущерб от реализации данной угрозы следующий: для информационного актива – нарушение доступности; для актива среды обработки информационного актива – нарушение доступности; для ИТ-сервиса – нарушение доступности, для организации – экономический (потеря конкурентного преимущества, закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) и технологический (необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций));

По результатам проведенного анализа угроз ИБ ИС платформы цифрового сома был получен предварительный перечень угроз ИБ ИС, в состав которого вошли 11 угроз, представленные ниже:

1. ТУ-1. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне из-за отсутствия аутентификации на точке доступа Wi-Fi.
2. ТУ-2. Угроза нарушения целостности данных вследствие деятельности внешнего нарушителя в контролируемой зоне из-за отсутствия аутентификации на точке доступа Wi-Fi.
3. ТУ-3. Угроза нарушения доступности данных из-за сбоя или отказа сетевого оборудования вследствие деятельности внешнего нарушителя в контролируемой зоне из-за отсутствия аутентификации на точке доступа Wi-Fi.
4. ТУ-4. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне связана с ошибками работы процессоров Intel при обработке инструкции RET.
5. ТУ-5. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне связана с недостатками разграничения доступа в процессоре Intel.
6. ТУ-6. Угроза нарушения доступности данных вследствие деятельности внешнего нарушителя в контролируемой зоне из-за недостаточной проверки состояний процессоров IntelXeon.
7. ТУ-7. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне связана с отсутствием защиты служебных данных процессоров Intel.
8. ТУ-8. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне, связанная с неправильным присвоением стандартных разрешений.
9. ТУ-9. Угроза нарушения доступности данных вследствие деятельности внешнего нарушителя в контролируемой зоне, позволяющая нарушителю вызвать переполнение стека в ОС DebianGNU/Linux.
10. ТУ-10. Угроза нарушения конфиденциальности данных вследствие деятельности внешнего нарушителя в контролируемой зоне, связанная с недостаточной проверкой входных данных, позволяющая нарушителю выполнить произвольные команды.
11. ТУ-11. Угроза нарушения доступности данных вследствие деятельности внешнего нарушителя в контролируемой зоне, позволяющая нарушителю вызвать отказ в обслуживании.

Список использованной литературы

1. **Цифровой юань:** новая финансовая реальность или тайное оружие Китая? - .- URL: <https://tass.ru/ekonomika/12218193> (дата обращения: 26.10.2023). Текст: электронный.
2. Сколько стоит открыть криптобиржу - . –URL: <https://vc.ru/crypto/347319-skolko-stoit-otkryt-kriptobirzhu> (дата обращения: 03.12.2023). Текст: электронный
3. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
4. ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
5. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.
6. РС БР ИББС 2.0-2007. Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0.
7. Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн)». Документ утвержден приказом ФСТЭК России от 14 февраля 2008 г.