Учреждение образования Белорусский
государственный университет информатики и
радиоэлектроники

УДК 004.054

Каплич
Андрей, Александрович

СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ БАНКОВСКОЙ СЕТИ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1–45 80 01 Системы и сети инфокоммуникаций
(информационные и коммуникационные технологии)

Научный руководитель
Кандидат технических наук,
ШЕВЧУК Оксана Геннадьевна

Минск 2021

ВВЕДЕНИЕ

Банковская деятельность всегда была связана с обработкой и хранением большого количества конфиденциальных данных. В первую очередь это персональные данные о клиентах, об их вкладах и обо всех осуществляемых операциях.

Данные о клиентах банков, их счета и операции интересны не только конкурентам, но и преступникам, которые для несанкционированного доступа к ним используют все возможные средства. Поэтому к банковским системам защиты конфиденциальной информации предъявляются особые требования, а именно полное исключения возможности понесения банком убытков или неполучения выгоды и обеспечения эффективной деятельности банка и качественной реализации им операций и сделок. Актуальной задачей является всесторонняя защита сервисов, сети и интересов банка.

Исходя из актуальности, целью работы является защита данных инфокоммуникационной сети банка.

Для достижения цели, необходимо решить следующие задачи:

– изучить список возможных угроз;
– проанализировать структуру банковской сети;
– разработать систему обнаружения и предотвращения вторжений.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 13 приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утвержденных Постановлением Совета Министров Республики Беларусь № 190 от 12 марта 2015 г. «Безопасность человека, общества, государства», а также пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «Обеспечение безопасности человека, общества, государства». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является защита данных в инфокоммуникационной сети банка.

Для достижения поставленной цели в диссертации решены следующие задачи:

- осуществить анализ возможных угроз на сеть банка;
- проанализировать структуру существующей банковской сети;
- разработать комплексную систему обнаружения и предотвращения вторжений для банковской сети.

Личный вклад соискателя ученой степени

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании выбранного программного обеспечения, оборудования и других решений, для обнаружения, проектирование системы обнаружения и предотвращения вторжений, оценке эффективности разработанной системы, обработке и анализе выбранных решений, формулировке выводов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем к.т.н. О.Г. Шевчук.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на 56-й научной конференции аспирантов, магистрантов и студентов БГУИР «Инфокоммуникации» (Минск, 2020) и на 57 научной конференции аспирантов, магистрантов и студентов БГУИР «Инфокоммуникации» (Минск, 2021).

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 тезиса в сборниках и материалах конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав с выводами по каждой главе, заключения, списока источников и графического материала.

Общий объем диссертационной работы составляет 81 страниц, из них 65 страниц текста, 42 рисунка на 14 страницах, 2 таблицы на 3 страницах, список использованных источников (13 наименований на одной странице), список публикаций автора по теме диссертации (2 наименование на 1 странице), графический материал.

Проверка на уникальность

Проверка на уникальность Проведена экспертиза диссертации Каплича Андрея Александровича «Система обнаружения и предотвращения вторжений банковской сети» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 08.04.2021 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 83 %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении дано краткое обоснование актуальности работы, сформулированы цель работы и задачи исследования.

В первой главе было рассмотрено понятие информационной безопасности, осуществлён анализ уязвимостей и угроз в корпоративной сети, в соответствии с моделью OSI и стека протоколов TCP/IP. Выявлены наиболее актуальные и опасные угрозы: социальная инженерия, отказ оборудования, программные угрозы, возможное повреждения данных, угрозы доступа.

На основе изученной литературе были проанализированные существующие угрозы и выделенные наиболее опасные из них. Все они были условно разделены на программные и технические

К техническим угрозам можно отнести: угрозу физической безопасности, которая подразумевает угрозу кражи данных преступниками или сотрудниками; повреждение и выход из строя оборудования и инженерных сетей; перепады напряжения; проблемы на стороне провайдера, например, проблемы с сетевым оборудованием; фишинг; социальная инженерия, с целью выявления учетных данных, паролей, например рассылка поддельных писем сотрудникам или звонки от мошенников, которые представляются сотрудниками банка с целью узнать конфиденциальные данные клиента; угрозу конфиденциальности, целостности передачи данных.

К программным угрозам относятся: несанкционированный доступ, ошибки ПО, разведка сети, а именно когда злоумышленник сканирует сети для выявления уязвимостей и слабых месте, для последующих атак; сниффер пакетов; сканирование портов; анализ пакетов; парольные атаки, например брутфорс – атака методом подбора паролей; вирусные угрозы (трояны, черви и др.); атака MitM, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами; неактуальные версии ПО; DDoS атаки.

Во второй главе проведен комплексный анализ ИТ-инфраструктуры банка, а именно в рамках одного кабинета и филиала, а также общая структура сети банка. Было рассмотрено программное обеспечение, используемое в банке и серверная инфраструктуру, с развёрнутыми операционными системами.

В роли центрального узла сети кабинета или филиала выступает коммутатор фирмы Cisco (см. рисунок 1). Рабочее место сотрудника оборудовано персональным компьютером и IP-телефоном. Сотрудники компании в качестве корпоративного рабочего устройства также используют ноутбук и могут подключаться к корпоративной сети через Wi-fi. Кабинет

оборудован сетевым принтерам с общим доступом для каждого сотрудника, что позволяет печатать документы с любого устройства. Доступ к Интернету осуществляется через маршрутизатор.

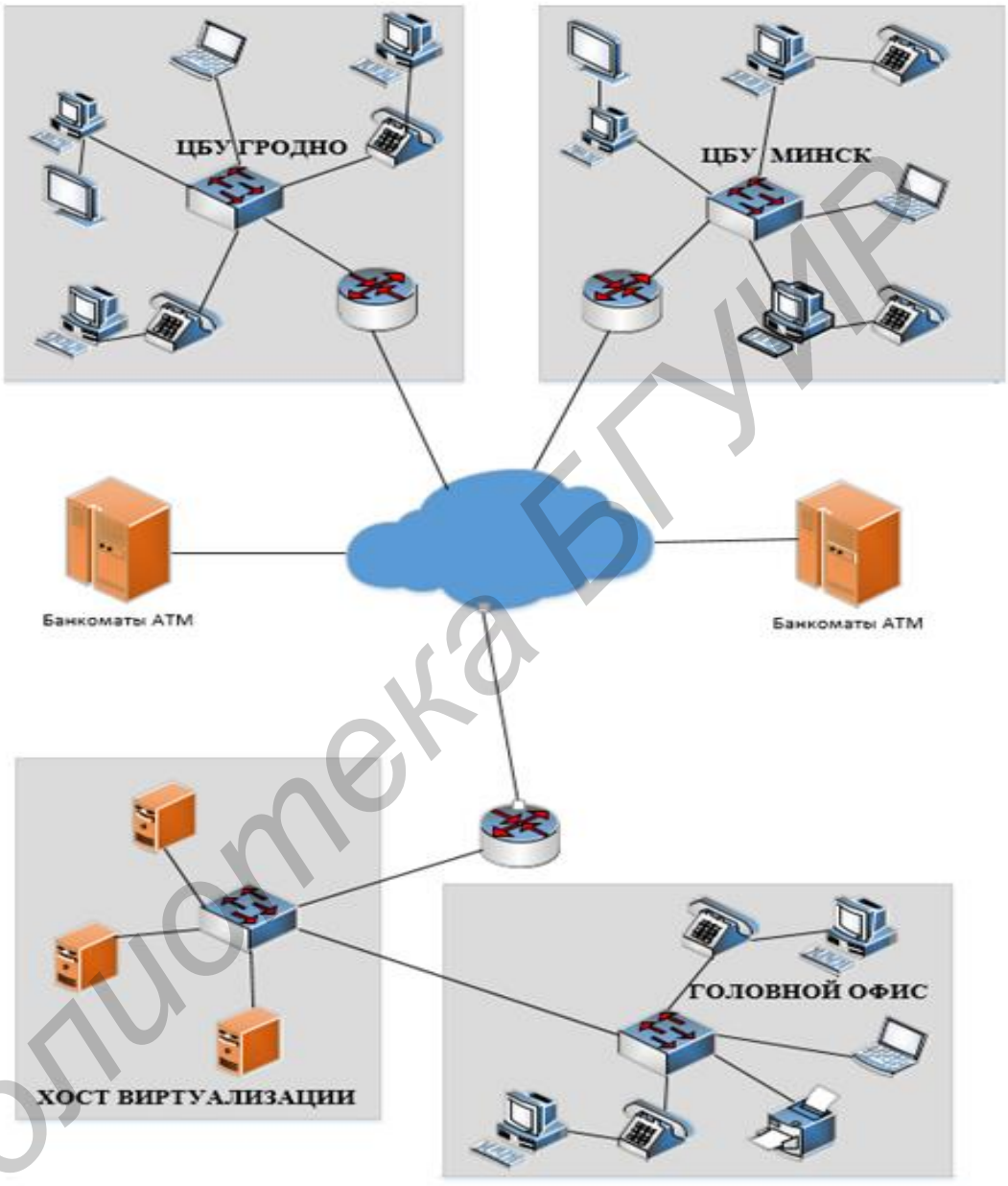

Рисунок 1 – Структурная схема сети банка

Аналогичная схема применяется во всех офисах, с небольшими модификациями, в зависимости от помещения и выполняемых задач, например инфраструктура филиала, имеет незначительные отличия с офисной, но в целом имеет похожую схему. В ней присутствует табло для отображения курса валют, которое представляет собой мини-ПК, подключенный к телевизору, а также терминал электронной очереди.

Так как для функционирования банка необходима работа множества отделов. Сеть банка включает в себя офисы для сотрудников, банкоматы, ЦОД и филиалы, для обслуживания клиентов в разных районах Минска и Республике Беларусь, а именно филиалы, которые находятся в Бресте, Гомеле, Могилеве, Витебске и Гродно (см. рисунок 2).

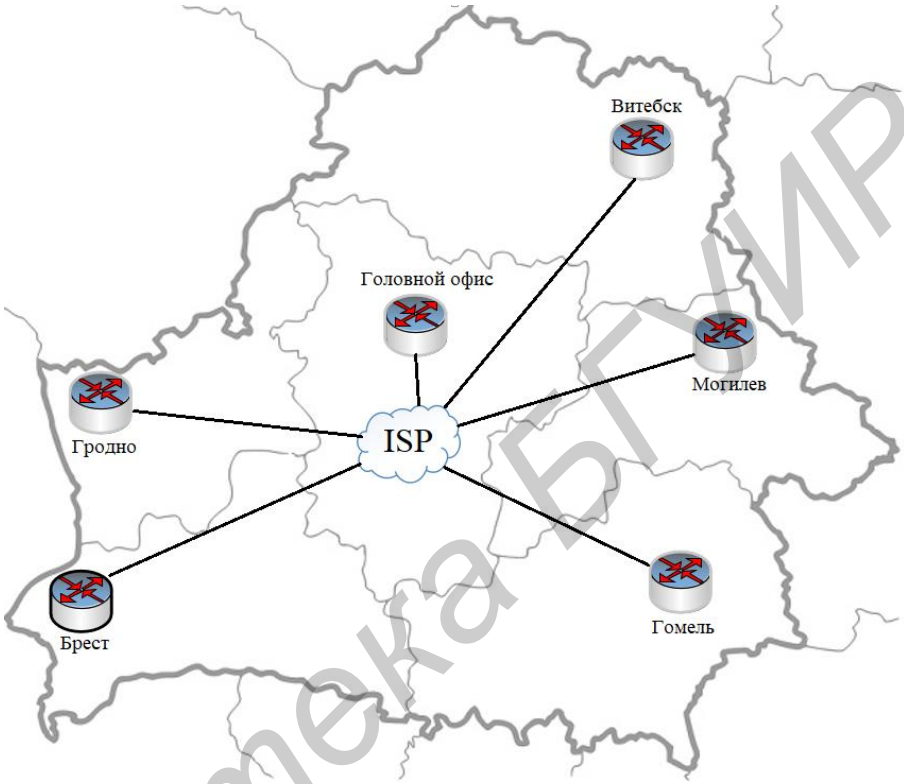

Рисунок 2 – Схема подключения региональных филиалов.

На сетевом уровне филиалы подключены к общей сети с помощью двух провайдеров через два разных кабеля по 12 Мбит/с. Для большей отказоустойчивости используется аварийное переключение – передача функциональной нагрузки на резервный компонент компьютерной сети, в случае сбоя или нарушения функционирования основного провайдера. Услуги связи предоставляются двумя провайдерами – А1 и МТС. Приоритетный провайдер – МТС, так как он арендует канал у Белтелекома, метрика которого меньше, чем у А1, где метрика больше из-за аренды у Деловой сети. При недоступности сети МТС, используется А1.

В третей главе были проанализированы все актуальные уязвимости и угрозы, была составлена следующая схема обнаружения и предотвращения вторжений. (см. рисунок 3).

Рисунок 3 – Схема обнаружения и предотвращения вторжений.

С точки зрения физических угроз, можно выделить угрозу выхода из строя оборудования и угрозы, которые могут исходить от самих пользователей. При незначительной поломке оборудования, например, сервера приложений, клиенты теряют доступ к приложению и не могут совершать необходимые операции. Что касается угроз, со стороны пользователей, наиболее распространенным и эффективным методом проникновения в инфраструктуру банка являются фишинговые атаки, например, рассылка электронных писем в адрес сотрудников или клиентов банка.

К угрозам можно также отнести прослушивание сетевого трафика нелегитимными пользователями, доступ к файлам и данным сотрудников отдела пользователями, которые не относятся к данному отделу и снижение пропускной способности ЛВС, в следствие большого количества широковещательных запросов.

Использование ненадлежащего или устаревшего сетевого и серверного оборудования, может также повлечь за собой ряд проблем, например, широковещательный шторм или коллизии в канале связи.

Инфраструктура банка, как и любого другого предприятия, часто подвергается различным программным угрозам. Основные из них это атаки на локальную сеть, например, DDos, спуффинг, разведка сети и вирусные угрозы, такие как черви, трояны, вирусы шифрования.

Определенную опасность несут угрозы доступа, а именно незащищенный удаленный доступ и доступ между отдельными сегментами сети. При ненадлежащей защите, злоумышленник может перехватить трафик, при удаленном соединении, тем самым конфиденциальные данные окажутся под угрозой компрометации.

Существует необходимость обеспечения безопасной авторизация и аутентификации в банковской сети, а также удобное и централизованное управление ими. Использование локальной базы данных для авторизации в крупной сети нецелесообразно из-за большого количество пользователей.

Вопросы резервирования информационных систем, в том числе резервного копирования данных и восстановления деятельности при сбоях и чрезвычайных ситуациях – одни из самых важных для кредитных и не кредитных финансовых организаций. Необходимо обеспечивать непрерывность бизнес–процессов и защиту информации от природных и техногенных катастроф, действий злоумышленников.

Для организации сети банка на основе представленной комплексной системы, используются решения, представленные на рисунке 4.

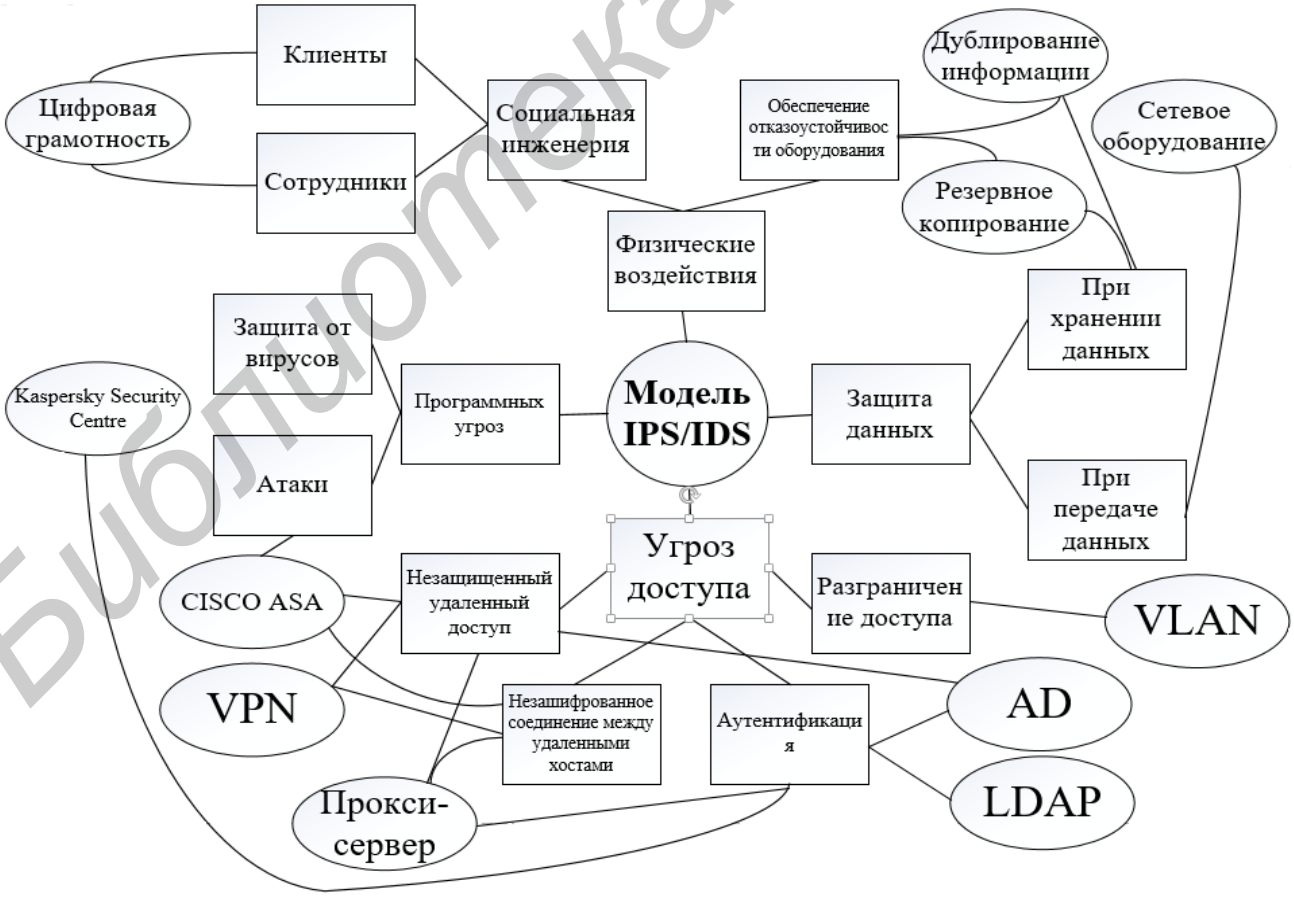

Рисунок 4 – Система обнаружения и предотвращения вторжений на основе выбранных решений

Как видно из рисунка 4, для обеспечения отказоустойчивости используется дублирование всех критичных подсистем, что позволяет сервисам функционировать, даже если из строя выходит один из компонентов. А для защиты от социальной инженерии используется тщательный вводный инструктаж, посвященный информационной безопасности для сотрудников и информирование клиентов о возможных угрозах безопасности и хищения данных мошенниками.

Проблема разграничения сети доступа и данных в сети, решается путем использования виртуальных локальных компьютерных сетей (VLAN).

Широковещательный шторм или коллизии, могут быть исключены использованием следующего оборудования – маршрутизатор Cisco 2911 и коммутатором Cisco Catalyst 2960, которые используются в инфраструктуре банка.

Используемая программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации от программных угроз.

Последствия, которые несут угрозы доступа предотвращаются с помощью технологии VPN, межсетевого экрана Cisco 5500 и прокси-сервера. В качестве программного продукта, для удаленного подключения используется Cisco AnnyConnect. Эта реализация, совместно с используемым межсетевым экраном Cisco ASA 5500 предлагает гибкие технологии VPN для любого сценария подключения. Данный выпуск обеспечивает удобный в управлении сетевой доступ в режиме полного туннелирования.

Все это позволяет устанавливать по общедоступным сетям хорошо защищенные подключения к мобильным пользователям, удаленным объектам, подрядчикам и бизнес–партнерам. Затраты, связанные с развертыванием и эксплуатацией VPN, снижаются за счет устранения потребности во вспомогательном оборудовании для масштабирования и обеспечения безопасности.

Использование Active Directory, совместно с LDAP, является неотъемлемой частью архитектуры банковской сети, позволяя ИТ–специалистам лучше контролировать доступ и безопасность. AD – это централизованная стандартная система, позволяющая системным администраторам автоматически управлять доменами, учетными записями пользователей и устройствами (компьютерами, принтерами и т.д.) в сети.

Так как данные клиентов являются самой важной частью банка и приоритетным направлением, необходима их полая сохранность, несмотря на любые условия и происшествия. Для обеспечения сохранности данных используется способ резервного копирования «3–2–1», которое гласит, что для

обеспечения надежного хранения данных, необходимо иметь как минимум три резервные копии, которые должны быть сохранены в двух различных физических форматах хранения, причем одна из копий, должна быть передана на хранение вне офиса.

ЗАКЛЮЧЕНИЕ

В диссертационной работе предложена комплексная система обнаружения и предотвращения вторжений в инфокоммуникационную сеть банка, которая позволяет всесторонне защищать данные пользователей и клиентов. В процессе работы был осуществлён глубокий анализ угроз не только со стороны пользователя, а также со стороны программного обеспечения и внештатных ситуаций.

Было рассмотрено понятие информационной безопасности, осуществлён анализ уязвимостей и угроз в корпоративной сети, в соответствии с моделью OSI и стека протоколов TCP/IP. Выявлены наиболее актуальные и опасные угрозы: социальная инженерия, отказ оборудования, программные угрозы, возможное повреждения данных, угрозы доступа.

Проведен комплексный анализ ИТ-инфраструктуры банка, а именно в рамках одного кабинета и филиала, а также общая структура сети банка. Было рассмотрено программное обеспечение, используемое в банке и серверная инфраструктуру, с развёрнутыми операционными системами.

Разработанная комплексная система обнаружения и предотвращения вторжений, может быть использована в сети банка, либо же сети больших организаций, где необходима всесторонняя защита данных. Для маленьких организаций данная система дорогостояща и избыточна.

Список публикаций автора

1–А. Каплич, А. А. Волоконно-оптические технологии в сетях гостиничных комплексов / Каплич А.А. // 56-я научная конференция аспирантов, магистрантов и студентов БГУИР : тезисы докладов 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР. Минск, 21-24 апреля 2020 г. / редкол. : В. Ю. Цветков [и др.]. – Минск : БГУИР, 2020. –С. 54.

2–А. Каплич, А. А. Система обнаружения и предотвращения вторжений IPS/IDS / Каплич. А. А. // 57-я научная конференция аспирантов, магистрантов и студентов БГУИР : тезисы докладов 57-ой научной конференции аспирантов, магистрантов и студентов БГУИР. Минск, 19-23 апреля 2021 г. / редкол. : В. Ю. Цветков [и др.]. – Минск : БГУИР, 2021. –С.27.