УДК 004.031.2
DOI: 10.33764/2618-981X-2020-7-1-140-148

РАЗРАБОТКА КОМПЛЕКСНОЙ ОХРАННОЙ СИСТЕМЫ

Антон Александрович Юшманов
Новосибирский государственный технический университет, 630073, Росиия, г. Новосибирск, ул. пр. К. Маркса, 20, лаборант, тел. (913)717-87-64, e-mail: yushmanov.2014@stud.nstu.ru

В статье описан процесс разработки комплексной охранной системы на базе одноплатного компьютера NVIDIA Jetson Nano. Главной задачей системы является обеспечение профилированного доступа в помещение доверенным пользователям. В результате работы был спроектирован и реализован механизм распознавания лиц на основе сверточной нейронной сети. Обнаружение лица реализовано при помощи гистограмм направленных градиентов. Затем, данное лицо центрируется и обрабатывается обученной сверточной нейронной сетью, которая выдает характеристические признаки изображения, подаваемые классификатору изображений, который выделяет процент совпадение изображения с эталонными образами. В процессе реализации системы, был разработан интерфейс, позволяющий реализовать коплексную охранную систему, независимо от аппаратных компонент. Для обеспечения защиты помещения в систему были добавлены датчики дыма, открытия дверей и окон. Научная новизна работы заключается в инкапсуляции всего передаваемого трафика системы в оверлейные сети для обеспечения конфиденциальности.

Ключевые слова: нейронные сети, оверлейные сети, Tor, многоуровневое шифрование, VPN.

DEVELOP A COMPREHENSIVE SECURITY SYSTEM

Anton A. Yushmanov
Novosibirsk State Technical University, 20, Prospect K. Marx St., Novosibirsk, 630073, Russia, Laboratory Assistant, phone: (913)717-87-64, e-mail: yushmanov.2014@stud.nstu.ru

The article describes the process of developing an integrated security system based on a single-board NVIDIA Jetson Nano computer. The main objective of the system is to provide profiled access to the room for trusted users. As a result of the work, a face recognition mechanism based on the convolutional neural network was designed and implemented. Face detection is implemented using histograms of directional gradients. Then, the face is centered and processed by the trained convolutional neural network, out the characteristic features of the image supplied to the image classifier, which gives the percentage of image matching with the reference images. In the process of implementing the system, a framework was developed that allows implementing a complex security system, regardless of hardware components. To ensure the protection of the room, smoke detectors, opened doors and windows were added to the system. The scientific novelty of tht work is the encapsulation of all transmitted system traffic to overlay networks to ensure confidentiality.

Key words: neural networks, overlay networks, Tor, multi-level encryption, VPN.

Введение

Согласно статистике Генеральной Прокуратуры РФ, Россия занимает пятое место в мире по количеству краж со взломом. За год происходит около 400 тыс.

преступлений такого рода и нераскрытыми остаются более половины случаев. Вследствие чего вопросом об охране помещений задается все большее количество людей.

Однако, следует отметить, что многие охранные системы далеко не всегда могут предоставить даже минимальный уровень охраны помещения и профилирование доступа. Многие разработчики в своих устройствах обходятся камерой и ключом, без распознавания лиц, таким образом, создавая IP-домофоны, что обеспечивает контроль доступа в помещение, но не профилирование пользователей. При другом подходе, охранные системы снабжают каким-либо ключом. Когда пользователь, желающий войти, подходит к двери, от него требуют ключ, предоставляемый в самом лучшем случае через смартфон, либо через ключ-карту или ключ-брелок. В редких случаях при передаче ключа используется Wi-Fi, но в таком случае, даже при шифровании трафика средствами WPA2, если сеть не защищена от вторжений, и злоумышленник обнаружит ее и получит к ней доступ, то в таком случае он получит доступ к самой системе, например, уязвимость KRACK [12], уязвимости шифрования TKIP [13,14], уязвимости генератора случайных чисел при генерации ключа [15], в этом случае злоумышленник получит доступ к системе. Установка Wi-Fi адаптера будет слишком дорогой в сравнении с альтернативами, безопасность передачи ключа в таком случае будет намного выше, но и риск использования, первоначальной настройки и сопровождения намного выше.

В процессе разработки системы следующие задачи были основополагающими:

1. Проведение сравнительного анализа существующих популярных решений комплексных охранных систем, представленных на рынке;
2. Разработка классификатора изображений на основе нейронной сети, для распознания лиц. Тестирование разработанного классификатора;
3. Проектирование и реализация аппаратно-программного комплекса охранной системы;
4. Обеспечение информационной безопасности разрабатываемой системы;
5. Тестирование в автоматизированном режиме разрабатываемой системы и исследование ее в сравнении с существующими альтернативными решениями.

Постановка задачи

Целью работы являлась разработка комплексной охранной системы, способной обеспечить охрану помещения и предоставить доступ только доверенным лицам.

Стоит отметить, что профилирование доступа в системе можно реализовать различными способами. Разработанная система считывает биометрические данные пользователя, используя камеру. Фотографии эталонных образов содержатся в базе данных, лицо считывают камерой и затем обрабатываются модулем Python, который для обработки использует фотографии пользователей, в качестве эталонных образов. В случае, если пользователь не может показать лицо,

либо это новый пользователь, еще не добавленный в базу, предусмотрена аутентификация пользователя через пин-код с клавиатуры.

Пример работы алгоритма представлен на рис. 1. Следующий этап – идентификация лица. Для этого происходит построение нормализации лица, оно центрируется таким образом, чтобы губы и глаза всегда находились на одном и том же месте в изображении, независимо от того, как повернуто лицо. Для этого генерируется маска из 68-ми антропометрических точек, после наложения которой, происходит центрирование. После чего полученное отцентрированное изображение обрабатывается сверточной нейронной сетью и на выходе получается 128 характеристик, на основе которых SVM-классификатор (англ. Support-vector machine) генерирует центр совпадения эталонных образов с подаваемым изображением.

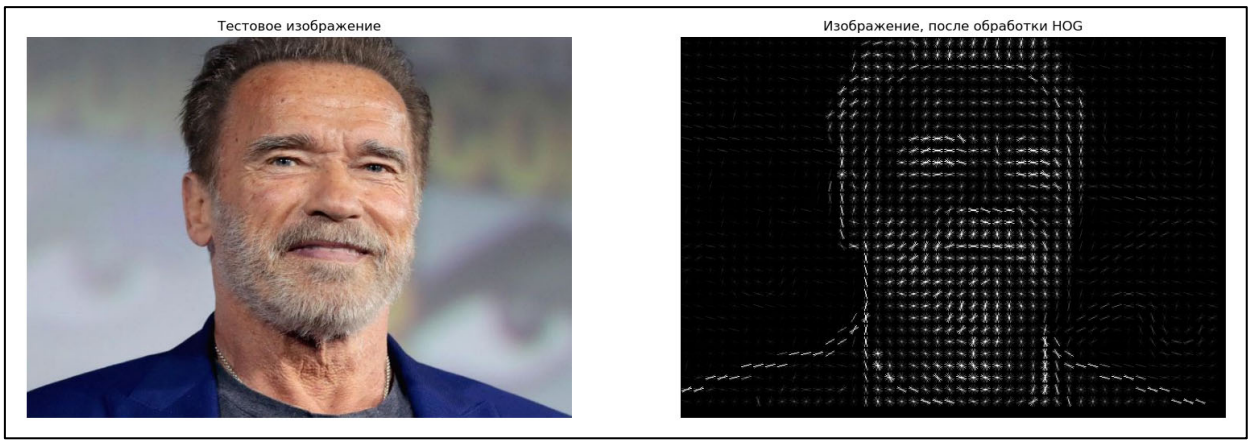

Рис. 1. Результат работы обнаружения лица, используя алгоритм HOG

Взаимодействие администратора с системой происходит через WEB-интерфейс. Администратор связывается с WEB-сервером, реализованном с использованием технологий Nginx и Apache. Затем переходит к работе с самой системой.

Практическая значимость работы заключается в возможности использования системы для разграничения доступа на различные объекты.

Сравнительный анализ существующих решений

Из аналогов разработанной системы можно выделить ISS SecurOS. Это крупный проект, который выходит за рамки только лишь охраны помещений, среди них можно найти распознавание номеров автотранспорта, видеостены, интеллектуальную систему предотвращения ДТП и т.д. Но у них также имеется разработанная система контроля доступа в помещение ISS SecurOS Face. Система похожа на разработанную в данной работе, но лишь в плане контроля доступа по лицу и общему принципу работы. Принцип работы системы ISS SecurOS Face: запись лица с камеры отправляется на сервер, где проходит обработку, заносится в архив и затем отправляется оператору. В спецификациях системы указано, что вероятность распознавания лица, составляет 80 % [16]. Также следует указать, что никаких дополнительных датчиков для охраны помещения си-

стемой не предусмотрено. При этом цена крайне высока. Расценки на лицензии модуля захвата лиц есть от трех сотен тысяч рублей до пяти миллионов в зависимости от количества человек в базе [17]. В цену не входит установка и настройка оборудования системы, только лицензия на возможность использования соответствующего ПО. Такой модуль подойдет крупным компаниям, которые могут себе позволить подобное, и которых устраивает точность в 80 %, но для небольших и средних бизнес-проектов, не говоря о простых квартирах, такой ценник крайне высок.

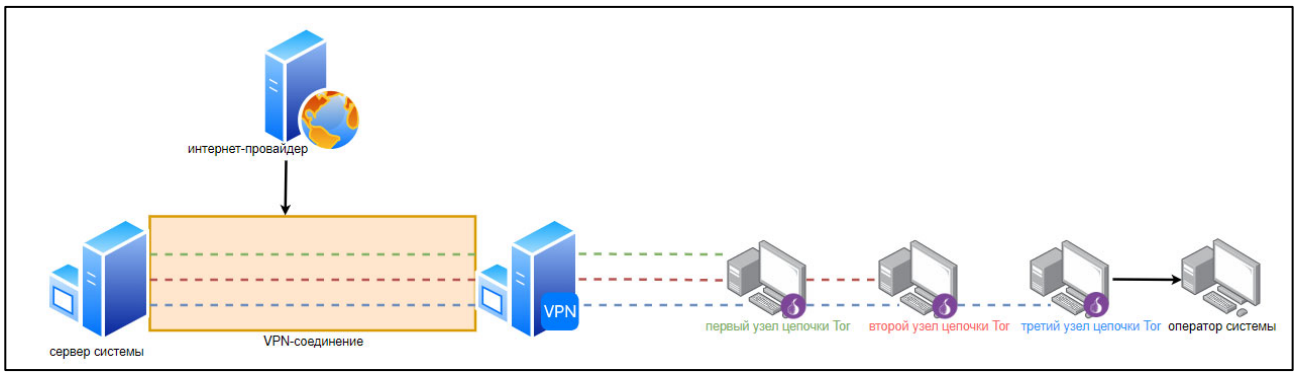

Рис. 2. Процесс сетевого взаимодействия системы

В ходе анализа также было выяснено, что многие решения построены с использованием технологий, построенных на архитектуре MIPS (англ. Microprocessor without Interlocked Pipeline Stages, «Микропроцессор без блокировок в конвейере»). Архитектура появилась в 1985 году и занимала крупную долю рынка. На данной архитектуре производилось большое количество процессоров как для ПК (Персональный Компьютер), так и для встраиваемых систем до начала двухтысячных годов. Но, с появлением ОС Windows NT v4.0, в которой оставили поддержку только для процессоров Alpha и Intel, одновременный с этим выпуск революционного процессора Intel Pentium и полный переход компании SGI на архитектуры Itanium и IA32 окончательно вывели MIPS с рынка.

Главные производители MIPS-процессоров последних лет: Broadcom и Cavium Networks. Broadcom не производили MIPS-процессоры с 2006-го года, а Cavium перешли на производство процессоров на архитектуре ARM v8.

У многих современных ОС отсутствует поддержка MIPS-архитектуры, из-за чего предлагаемые решения часто используют устаревшие ОС и ПО, в которых еще не закрыты определенные уязвимости.

Энергоэффективность MIPS-процессоров не так высока, например, в сравнении с соверменными ARM-процессорами и даже некоторыми процессорами x86. Можно рассмотреть один из последних MIPS-процессоров компании Байкал 2015-го года Baikal-T1, который активно применяется до сих пор, и одноплатный компьютер NVIDIA Jetson Nano, выпущенный в 2019-ом году. В таком случае энергопотребление процессора Baikal-T1 составляет 5 Вт, а энергопотребление всего одноплатного компьютера Jetson Nano без периферии составляет от 15 Вт,

при этом в нем стоит процессор с чуть большей тактовой частотой 1400 МГц, чем Baikal-T1. Но основные вычисления разрабатываемой системы планируется проводить не на процессоре, а на 128 ядерном GPU, которые предоставляет Jetson, что в десятки раз увеличит производительность системы при параллелизации программы. Многие современные ARM-процессоры имеют низкое энергопотребление. Например, Qualcomm Snapdragon 845 2017-го года потребляет лишь 4,38 Вт при работе в реальных системах, а Qualcomm Snapdragon 835 2016-го года 3,79 Вт при работе в сматрфоне Galaxy S8. При этом частота 845-го составляет 2800 МГц, а 835-го 2450 МГц. Также у 845-го имеется кэш L3 2 Мб. Данные процессоры по характеристикам лучше, чем Baikal-T1, имеют ARM архитектуру и также являются RISC-процессорами (англ. Reduced Instruction Set Computer, «компьютер с набором коротких (простых, быстрых) команд»).

Разработка комплексной охранной системы

На рис. 3 представлена блок-схема функционирования разрабатываемого интерфейса комплексной охранной системы. В блок-схеме представлены этапы, через которые система должна пройти, прежде чем начать работу в штатном режиме работы, и сам алгоритм работы штатного режима системы, независимо от того, какое оборудование было выбрано для реализации ее работы.

Учитывая требования, наиболее рентабельным вариантом является одноплатный компьютер. В зависимости от модели характеристики разнятся, но одноплатные компьютеры портативны, потребляют малое количество электроэнергии, поддерживают автономную работу вне электросети, используя портативный аккумулятор для питания, и, в зависимости от характеристик, выбранного ПО и настройки, способны на одновременное поддержание работы датчиков, WEB-сервера, взаимодействия с пользователем и с СУБД, обрабатывать информацию, полученную с камеры.

Процесс работы системы начинается с начальной настройки. При первом включении устройство должно иметь «белый» IP-адрес по умолчанию.

Затем оператор заполняет базу данных эталонных образов, используя средства СУБД MySQL. Каждого пользователя определяет профиль, состоящий из номера (id), имени (name), трех эталонных изображений (photo #1, #2, #3), должности (post). Таким образом создается эталонный образ пользователя, к которому в последствии будет обращаться обработчик лиц. Во второй таблице Histogram содержатся номер сотрудника (id), на который ссылается id из таблицы Person и три гистограммы, полученные после обработки фотографий алгоритмом LBP.

В БД данные должны храниться в зашифрованном виде, таким образом, даже злоумышленник не получит конфиденциальные данные. Стандартные средства шифрования MySQL позволяют воспользоваться алгоритмом AES-256. Данный алгоритм считается одним из самых надежных алгоритмов шифрования (для сравнения, его 256-битный ключ для атак типа Bruteforce аналогичен 15360-битному ключу RSA, хотя на сегодняшний день 2048-битный ключ RSA считается надежным и используется во многих системах [22]).

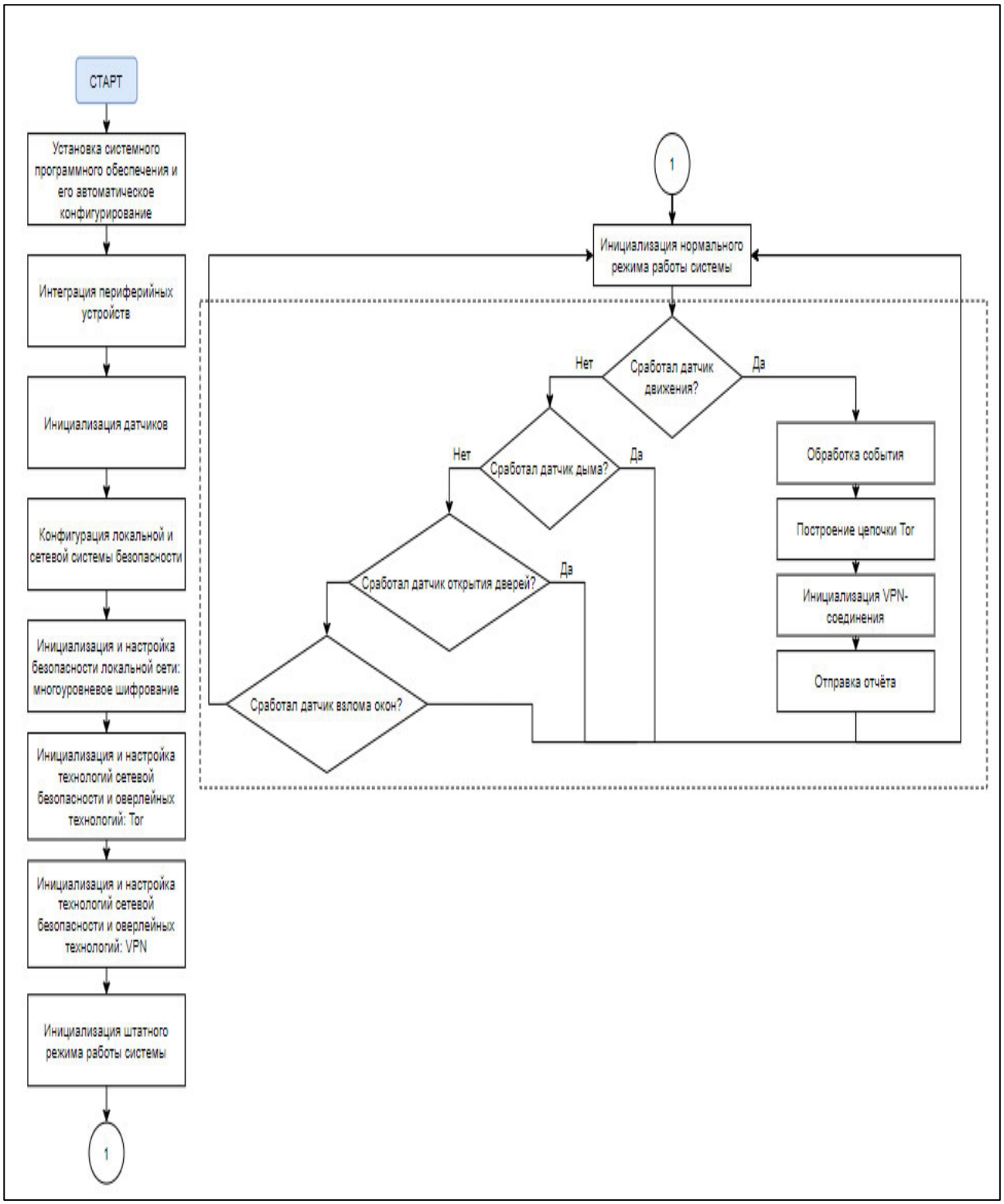

Рис. 3. Блок-схема функционирования разрабатываемого интерфейса

Три данных технологии реализованы на сервере разработчика и обеспечивают контроль процесса проектирования. Оператор или пользователь системы никак не связаны с данным технологиями. Применение данных технологий обеспечивает легкое сопровождение системы.

При программных изменениях или программном дополнении системы, от разработчика потребуется сформировать Docker-контейнер и передать его на сервер, при помощи технологии Ansible. Главный сервер получает контейнер и все программные изменения применяются автоматически.

Обсуждение результатов и описание планируемых улучшений решения

После реализации системы были проведены тесты, проверяющие ее устойчивость.

Тестирование системы проводилось методами активного и пассивного анализа трафика при помощи сканеров, снифферов, зондеров, пентеста и др. Т.к. крайне важно было убедиться в том, что трафик, передаваемый системой, шифруется на каждом этапе передачи.

В частности, проводилось тестирование при помощи SharkTap Gigabit Network Sniffer в открытой и частной сети. Для анализа трафика, проходящего через SharkTap, использовалась программа WireShark 2.6.0.

В результате тестирования было выявлено, что трафик действительно шифруется системой и корректно инкапсулируется при помощи технологий OpenVPN-сервер и Tor, а затем зашифрованный трафик приходит оператору, где расшифровывается как показано на (рис. 4).

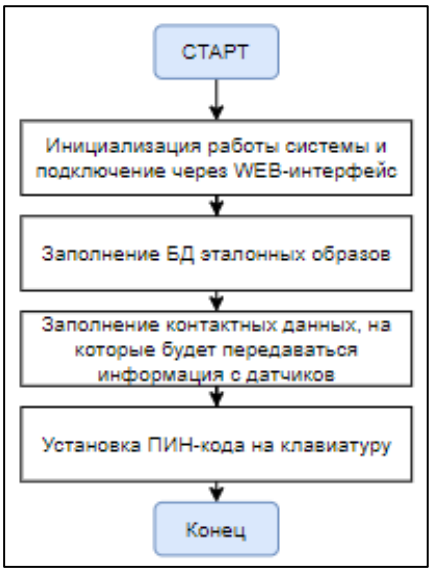

Рис. 4. Блок-схема первичного взаимодействия оператора с системой

Заключение

В ходе работы была разработана и реализована комплексная охранная система на базе одноплатного компьютера Jetson Nano с использованием оверлейных технологий Tor и OpenVPN для обеспечения конфиденциальности трафика. Предлагаемое решение предназначено для разграничения доступа на различные объекты как в частном, так и в государственном секторе.

В ходе тестирования было подтверждено, что система отвечает всем поставленным требованиям и успешно справляется со своими задачами: трафик передается в зашифрованном виде, пользователь успешно взаимодействует с системой через WEB-интерфейс, показания датчиков передаются по протоколу Z-Wave Plus, лицо пользователя считывается и идентифицируется методом Виолы-Джонса и алгоритмом LBP.

Тестирование системы производилось с использованием механизмов активного и пассивного анализа трафика, автоматизированных Unit-тестов и тестов на энергопотребление.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Juels Strengthening, EPC Tags Against Cloning. 4th ACM Workshop on Wireless Security, pp. 67–76, 2005.
2. R. Jain, D.K. Chaudhary, K. Sanjiv, "Analysis of Vulnerabilities in Radio Frequency Identification (RFID) Systems", 8th International Conference on Cloud Computing Data Science & Engineering (Confluence), pp. 453–457, 2018
3. Михайлов Д.М., Шептунов А.А., Зуйков А.В., Толстая А.М. "Возможности осуществления атаки на системы автоматизации с использованием уязвимостей технологии RFID" Спецтехника и связь. 2012. № 5–6. С. 54–56.
4. C. Naveed, "NFC – Vulnerabilities and defense", 2014 Conference on Information Assurance and Cyber Security (CIACS), pp. 35–38, 2014.
5. Мезенов В.А., Стадниченко Н.С. "Уязвимости "NFC" на примере транспортных карт". В сборнике: Информационные системы и технологии Сборник материалов IV Международной научно-технической конференции. 2018. С. 69–71.
6. Иванов А.О. "Опасность NFC-технологий для личной информации". В сборнике: Научное сообщество студентов XXI столетия. Технические науки сборник статей по материалам LXXIII студенческой международной научно-практической конференции. 2019. С. 84–88.
7. K. Scarfone, J. Padgette, "Guide to Bluetooth Security", Special Publication 800–121. Recommendations of the National Institute of Standards and Technology, pp. 1–50, 2008.
8. Минин П.Е., Самойлов А.С., Кузин А.А. "Уязвимости канала данных bluetooth для прослушивания злоумышленниками" Безопасность информационных технологий. 2012. Т. 19. № 2S. С. 50–53.
9. Валагов Д.А., Толоконцева А.С., Овчинникова А.А. "Bluebourne-вирус, передающийся по воздуху". Теория и практика современной науки. 2017. № 9 (27). С. 300–302.
10. Калашникова В.А., Львова А.П. "Уязвимости протокола передачи данных bluetooth". В сборнике: Российская наука в современном мире Сборник статей XII международной научно-практической конференции. 2017. С. 107–108.
11. M. Beck, E. Tews, "Practical attacks against WEP and WPA [C]", Proceedings of the 2nd ACM Conference on Wireless Network Security WiSec'09, pp. 79–85, 2009.
12. Савин И.В. "Krack как одна из наиболее опасных уязвимостей wi-fi". В сборнике: Развитие науки и образования в современном мире Сборник научных трудов по материалам Международной научно-практической конференции: в 2 частях. 2017. С. 57–58.
13. D. J. Fehér, S. Barnabás, "Effects of the WPA2 KRACK Attack in Real Environment", 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), pp. 239–242, 2018.
14. M. VcbjØrn, H. Raddum, K. J. Hole, "Weaknesses in the temporal key hash of WPA", ACM SIGMOBILE Mobile Computing and Communications Review, pp. 76–83, 2004.
15. SecurOS Face datasheet, [электронный источник] режим доступа: https://iss.ru/pub/uploads/cb6b3821-2952-4d07-b82f-49388a8e1318/securos-face-datasheet-ru.pdf

16. SecureOS Face purchase options, [электронный источник] режим доступа: https://www.syssoft.ru/Intelligent-Security-Systems/SecurOS-Face/

17. E. Barker, "Recommendation for Key Management Part 1: General", Natl. Inst. Stand. Technol. Spec. Publ. 800–57 Part 1 Revision 4 160 pages, January 2016.

18. Киянов И.Р. “Tor и луковая маршрутизация” Электронный сетевой политематический журнал". Научные труды КубГТУ". 2016. № 13. С. 129–135.

19. Basinya E. A. Countermeasure method against unauthorized and anonymous information system data collection [Electronic resource] / E. A. Basinya, V. E. Khitsenko, A. A. Rudkovskiy // Dynamics of systems, mechanisms and machines (DYNAMICS) : proc., 13 intern. sci. and techn. conf., Omsk, 5–7 Nov. 2019. – IEEE, 2019. – 6 p.

20. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия = Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure / Е. А. Басыня // Безопасность информационных технологий = IT Security. – 2018. – Т. 25, № 4. – С. 43–52.

21. Басыня Е.А., Хиценко В.Е., Рудковский А.А. “ Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации”. Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22. № 2. С. 45–51.