ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

4

(139)

Подписывайтесь,
читайте,
пишите в наш журнал

Москва 2022

Все новейшие достижения и современные разработки предприятий оборонного комплекса — в научно-технических журналах ФГУП «НТЦ оборонного комплекса «Компас»

ФГУП «Научно-технический центр оборонного комплекса «Компас» является издателем следующих научных журналов:

Межотраслевой научно-технический журнал

Оборонный комплекс — научно-техническому прогрессу России
(4 выпуска)

Подписной индекс **79379**

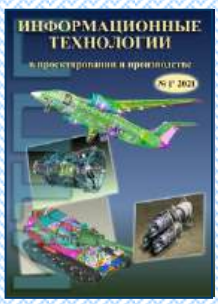
Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года



Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года

Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

Все издания ФГУП "Научно-технический центр оборонного комплекса «Компас»:

✓ *включены решением ВАК Министерства науки и высшего образования России в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата и доктора наук;*

✓ *метаданные выпусков включены в базу данных Российского индекса научного цитирования (РИНЦ).*

Более подробную информацию об изданиях, подписке, дополнительных услугах можно получить
по тел.: 8 (495) 491-43-17, 8 (495) 491-77-67, 8 (495) 491-77-20 (*подписка*);
факс: 8 (495) 491-44-80.
E-mail: izdanie@ntckompas.ru

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР ОБОРОННОГО КОМПЛЕКСА «КОМПАС»
(ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС»)

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

4 (139)

Москва 2022

Основан в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2022.
Вып. 4 (139). С. 1—52.

Компьютерная верстка: *Н. В. Ильина, К. В. Трыкина*

Подписано в печать 12.12.2022. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 6,0. Уч.-изд. л. 6,2.
Тираж 400 экз. Заказ 2007. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, офис 105.
ИП Кириченко Алексей Викторович.
Индекс 79187.

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.056.52
DOI: 10.52190/2073-2600_2022_4_3
EDN: IZGLKW

Разработка функциональной схемы и алгоритма биометрической идентификации для обеспечения информационной безопасности

А. М. Трошков, канд. техн. наук; *С. В. Богданова*, канд. пед. наук;
А. Н. Ермакова, канд. эконом. наук; *Е. А. Косинова*, канд. эконом. наук
ФГБОУ ВО «Ставропольский государственный аграрный университет»,
г. Ставрополь, Россия

Проанализирован функционал современных систем доступа к информационным ресурсам. Выявлены недостатки систем в части аутентификации по проверке знания логина и пароля пользователем. Для повышения стойкости системы защиты информации рассмотрены преимущества использования биометрической идентификации. Предложено использование синтезированной биометрической характеристики — управление компьютерной мышью по динамике набора заранее определенных фигурных конструкций и выявление таким образом права доступа в систему методом сравнения почерка управления. Разработаны функциональная схема и алгоритм функционирования динамической системы идентификации пользователей по выделению биометрической характеристики и управлению графическим манипулятором на основе индивидуального поведенческого параметра биологической характеристики человека. Результаты данного исследования рекомендуется включать в состав эшелонированной системы информационной безопасности.

Ключевые слова: идентификация, аутентификация, информационная безопасность, биологическая характеристика человека, несанкционированный доступ.

На сегодняшний день биометрия занимает значительную часть во всех сферах деятельности и используется в качестве практичного и надежного механизма обеспечения безопасности информационных систем.

Актуальность заявленной темы исследования обусловлена растущим интересом к автоматизированному процессу распознавания и идентификации пользователей в информационных системах.

Трошков Александр Михайлович, доцент, доцент кафедры "Информационные системы".
E-mail: troshkov1954@mail.ru
Богданова Светлана Викторовна, доцент кафедры "Информационные системы".
E-mail: svetvika@mail.ru
Ермакова Анна Николаевна, доцент, доцент кафедры "Информационные системы".
E-mail: dannar@list.ru
Косинова Елена Александровна, доцент, доцент кафедры "Экономическая теория".
E-mail: kosinova5@rambler.ru

Статья поступила в редакцию 11 октября 2022 г.

В рамках разработки биометрических систем появляется возможность определить основные пути и способы решения этих задач через использование биологических характеристик человека, обеспечивая безопасность информации на очень высоком уровне.

Истинными идеологами идеи биометрической идентификациями являются писатели-фантасты Роберт Хайн-лайн, Айзек Азимов и др. Ученые Фрэнсис Гальтон, Карл Пирсон, Ролнальд Фишер, Брюс Вейр, Л. С. Каминский, П. В. Савостин и др. создали специальную науку под названием Биометрика, воплотив эти мечты в реальность [1]. Дальнейшее развитие информационных биометрических систем было катализировано научными изысканиями известных исследователей в области биометрии: Вуди Бледсо, Хармоном, Голдштейном, Леск, Майклом Кирби, Лоуренсом Сирович, Алексом Пентланд, Мэтью Терком [2].

Согласно Федеральному закону Российской Федерации от 27 июля 2006 г. № 152-ФЗ "О персональных данных" информация о состоянии здоровья гражданина — одна из самых уязвимых к разглашению видов конфиденциальной информации. Решение задач идентификации и аутентифи-

кации, по мнению авторов [3], невозможно без субтильного управления доступом пользователей. Развитие новых сервисов и систем позволяет озвучивать необходимость создания и практического применения надёжной системы идентификации сторон удалённого электронного взаимодействия. Идентификация по биометрическим характеристикам — один из самых интенсивно развиваемых методов идентификации и аутентификации личности. Биометрия привлекает разработчиков тем, что пользователю не надо запоминать или записывать идентификационную и аутентификационную информацию. За последние два десятилетия разработано несколько десятков методов идентификации [4].

Несмотря на то, что на мировом рынке информационных технологий имеется положительный опыт внедрения систем доступа к информационным ресурсам, согласно экспертным оценкам, они имеют недостатки, основным из которых является аутентификация по проверке знания логина и пароля, что существенно снижает стойкость защиты информации.

Методология

В процессе исследования проблемы доступа к информационным ресурсам использовался эмпирический метод исследования синтеза динамической биометрической характеристики. В процессе исследования были изучены доступные в открытой печати публикации, проведен всесторонний анализ перспектив биометрических систем аутентификации и идентификации.

Результаты

В представленной работе авторы предлагают использование синтезированной биометрической характеристики — управление мышью по динамике набора заранее определенных фигурных конструкций и выявление права доступа методом сравнения почерка управления. Как правило, для аутентификации и идентификации личности почерковедениических характеристик применяют искусственные нейронные сети, однако многие учёные-специалисты [5—9] считают, что нейронные сети не дают желаемых возможностей из-за временных показателей обучения, расширения памяти, увеличения времени оперативности принятия решений в области управления доступом к информации. Предложен эмпирический метод исследования синтеза динамической биометрической характеристики — управления мышью, основанный на модели статистических данных распределения времени повторения графических знаков, устойчивости их копирования с помощью мыши. Использование биометрической характеристики человека (БХЧ) — управление мышью требует настройки профиля пользователя:

- время действия пользователя, T;
- объем знаковых и архитектурных структур, V;
- количество повторов, N;
- оценочный вектор дисперсии, $\vec{\delta}$;
- формирование и предоставление знаковых и архитектурных структур, $\vec{Z}$;
- допустимый вектор ошибок, $\vec{R}$.

Созданный профиль пользователя позволит формировать модель, а на её основе проектировать функциональную схему биометрической идентификации по БХЧ — управление мышью (рис. 1).

Предложенная функциональная схема имеет ряд достоинств, которые реализуют новую методику удалённого доступа. На основе схемы рис. 1, разработан алгоритм работы, представленный на рис. 2.

Рис. 1. Функциональная схема биометрической идентификации

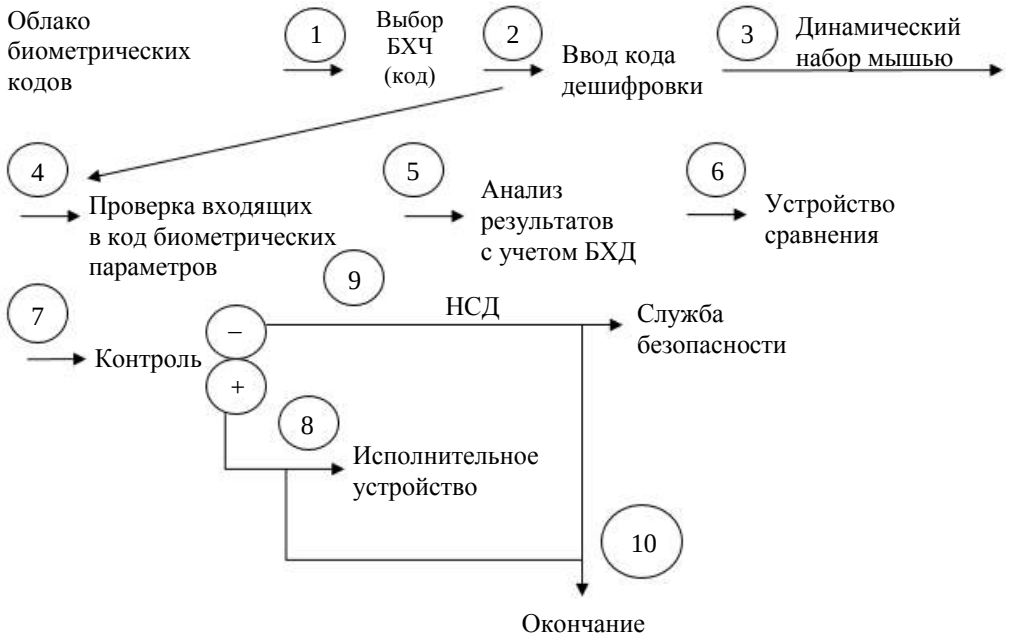


Рис. 2. Алгоритм функционирования функциональной схемы биометрической идентификации управления мышью

Предложенный алгоритм и схема функционирования демонстрируют возможность использования идентификации по управлению персональным компьютером с помощью мыши, которая реализует научную задачу повышения информационной безопасности, обеспечивающей управление доступом удалённого абонента [10]. Предложенное решение снижает риск несанкционированного доступа (НСД) к информации.

Заключение

Предложенные алгоритм и схема функционирования динамической системы идентификации по выделению биометрической характеристики и управлению мышью на основе индивидуального поведенческого параметра биологической характеристики человека существенно позволяют повысить информационную безопасность доступа к хранилищу информационных ресурсов по сравнению с другими системами, данный алгоритм и схема также могут быть включены в состав эшелонированной системы информационной безопасности.

Авторы благодарят экспертов ФГБОУ ВО "Ставропольский государственный аграрный университет", ФГАОУ ВО "Северо-Кавказский федеральный университет" и ООО "Компьютер-Союз" за советы и ценный вклад как в проведение исследований, так и в коррекцию содержания статьи.

Литература

1. *Леонов В. П.* История биометрики и ее применения в России // Применение статистики в статьях и диссертациях по медицине и биологии. 1999. Вып. 4. С. 7—19.

2. *Прудников И. В.* Исследование возможностей повышения точности идентификации информационных биометрических систем: дис. … канд. техн. наук. — М., 2012. — 190 с.

3. *Грушо А. А., Применко Э. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности. — М.: Академия, 2009. — 272 с.

4. *Крылова И. Ю., Рудакова О. С.* Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Молодой ученый. 2018. № 45(231). С. 74—79.

5. *Винокуров А. В.* Биометрические системы идентификации в кредитных организациях как инструмент противодействия мошенничеству // Финансы и кредит. 2016. № 21. С. 15—21.

6. *Выскуб В. Г., Прудников И. В.* Анализ направлений совершенствования биометрических распознающих систем (актуальные вопросы обеспечения оперативно-розыскной деятельности) // Оперативник (сыщик). 2012. Вып. 1(30). С. 57—60.

7. *Джейн А., Нандакумар К.* Биометрическая аутентификация: защита систем и конфиденциальность пользователей // Открытые системы. 2012. № 10. С. 38—41.

8. *Достов В. Л., Шуст П. М., Козырева А. Д.* Новые концепции применения риск-ориентированного подхода при осуществлении процедур идентификации // Юридическая наука. 2017. № 5. С.104—112.

9. *Селиверстова А. В.* Сравнительный анализ, выбор и реализация метода биометрической идентификации // Современные научные исследования и инновации. 2016. № 4. С. 135—142.

10. *Иванов А. И.* Биометрическая идентификация по динамике подсознательных движений. — Пенза: Изд-во ПГУ, 2000. — 188 с.

Development of functional scheme and algorithm for biometric identification of mouse control

A. M. Troshkov, S. V. Bogdanova, A. N. Ermakova, E. A. Kosinova
Stavropol State Agrarian University, Stavropol, Russia

The functionality of modern systems of access to information resources is analyzed. Shortcomings of modern systems of access to information resources in terms of authentication to check the knowledge of the username and password by the user are identified. To increase the stability of the information security system, the advantages of using biometric identification are considered. It is proposed to use a synthesized biometric characteristic — control of a computer mouse according to the dynamics of a set of predetermined curly structures. It is proposed to identify access rights to the system by comparing the control handwriting. A functional diagram and an algorithm for the functioning of a dynamic user identification system based on an individual behavioral parameter of a person's biological characteristics have been developed. The results of this study are recommended to be included in the structure of the layered information security system.

Keywords: identification, authentication, information security, human biological characteristics, unauthorized access.

Bibliography — 10 references. *Received October 11, 2022*

ДОВЕРЕННАЯ СРЕДА

УДК 004.056.52
DOI: 10.52190/2073-2600_2022_4_7
EDN: JCFPPO

Разработка системы безопасной аутентификации и поддержания сеанса пользователя на веб-ресурсе

С. Ю. Сидорин
Компания «Информзащита», Москва, Россия

А. А. Жердев
Group-IB, Москва, Россия

В. И. Шармаев
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

С помощью инструмента Burp Suite авторами продемонстрирована возможность перехвата логина и пароля в том случае, если он передается в открытом виде. Для решения данной проблемы предложен метод безопасной аутентификации пользователя и поддержания сеанса на веб-ресурсе. Приведено подробное описание использованных элементов безопасности и технологий. Для верификации разработанного метода были использованы сканеры уязвимостей Nessus и Netsparker. Результаты данного исследования можно использовать в разработке тактических и технических рекомендаций организациям по формированию более надежных алгоритмов аутентификации пользователей, выявлению уязвимостей и снижению рисков.

Ключевые слова: информационная безопасность, уязвимости, кибератаки, аутентификация, авторизация, cookie, JWT-токены.

При современных темпах развития информационных технологий и сети Интернет приоритетное внимание разработчиков уделяется вопросам безопасности, качественным методам разработки и надежному управлению процессом. От этого зависит уровень доверия клиентов, что, в свою очередь, является жизненной силой любого бизнеса, задачей которого является непрерывной рост [1].

При попытке пользователя войти в свой личный кабинет на веб-ресурсе, осуществляется три действия: идентификация, аутентификация и авторизация [2].

В первую очередь, при запросе системой логина и указании его пользователем, когда система распознает данный логин как существующий, происходит процесс идентификации, то есть пользователь определяется среди прочих по определенному идентификатору — логину.

Аутентификация — это процесс проверки личности пользователя. Другими словами, это способ убедиться в том, что то или иное лицо является тем, за кого себя выдает [3]. С концептуальной точки зрения уязвимости аутентификации являются одними из самых простых проблем для понимания. Однако они могут быть одними из самых важных из-за очевидной связи между аутентификацией и безопасностью. Помимо потенциального предоставления злоумышленникам прямого доступа к конфиденциальным данным и функциональным возможностям, они также открывают дополнительную поверхность атаки для дальнейшей эксплуатации уязвимостей. По этой причине изучение способов выявления и использования уязвимостей аутентификации, в том числе способов обхода общих мер защиты, является фундаментальной задачей.

Система аутентификации — одна из областей программной системы, безопасность которой необходимо обеспечить на максимально высоком уровне. Плохо реализованная система аутентифи-

Сидорин Сергей Юрьевич, специалист.
E-mail: sarmatsid@yandex.ru
Жердев Александр Александрович, вирусный аналитик.
E-mail: misterrio535@gmail.com
Шармаев Вадим Игоревич, аспирант, инженер НИО-402.
E-mail: vadidq@ya.ru

Статья поступила в редакцию 6 ноября 2022 г.

кации может привести не только к потере доверия клиентов, но и иметь серьезные последствия для финансов компании, а также общей репутации и соответствия нормативным требованиям.

Существует множество векторов, используемых злоумышленниками для реализации проблем небезопасной аутентификации. Деятельность злоумышленника может быть направлена на поиск и эксплуатацию уязвимостей в инфраструктурной части, куда можно отнести программное обеспечение, стек используемых сетевых технологий и средств защиты, а также аппаратные средства. Однако наиболее популярным и простым в реализации для злоумышленника является такой метод социальной инженерии, как фишинг, где воздействие оказывается не на систему, а на пользователя, в обход предпринятым мерам по обеспечению безопасности.

Воздействие уязвимостей аутентификации может быть очень серьезным. Если злоумышленнику удастся скомпрометировать учетную запись с высоким уровнем привилегий, например, системного администратора, он сможет получить полный контроль над всем приложением и потенциально получить доступ к внутренней инфраструктуре [4].

При формировании архитектуры системы аутентификации пользователя разработчику необходимо, помимо факторов, отвечающих за автоматизацию, доступность, универсальность и масштабируемость, обращать внимание на уровень защищенности проектируемой среды.

Цель работы — выявление и исследование проблем небезопасной аутентификации, а также разработка собственной системы безопасной аутентификации и поддержания сеанса пользователя на веб-ресурсе.

Теоретическая часть

Самой простой и распространенной формой аутентификации является аутентификация по паролю. Данный метод называется однофакторным, или первичным. Он крайне небезопасен, так как единственный фактор может быть угадан или получен с помощью фишинга [5].

Двухфакторная аутентификация (*2FA*) представляет собой однофакторную аутентификацию на основе определенного кода с использованием дополнительного фактора. Самая популярная форма двухфакторной аутентификации использует генерируемый программным обеспечением одноразовый пароль на основе времени (также называемый TOTP или "мягкий токен") [6]. В этом случае пользователь должен загрузить и установить бесплатное приложение *2FA* на свой смартфон или компьютер (*MobilePass+, Google Authenticator, Microsoft Authenticator*) и при появлении запроса на сайте ввести код, отображаемый в приложении [7].

Главной задачей злоумышленника в вопросах аутентификации пользователя является получение учетных данных пользователя или его сессионных данных, выданных ему сервером при успешном входе в систему. Следовательно, что аутентификация и формирование сессии пользователя являются двумя взаимосвязанными процессами. Это означает, что при определении безопасных компонентов системы аутентификации важно также принимать необходимые меры по созданию и обеспечению безопасной сессии пользователя.

Данные сессии могут храниться в файлах *cookie*, главной проблемой которой является возможность перехвата, например, посредством сниффера *Wireshark* [8]. Большинство веб-сайтов используют файлы *cookie* в качестве единственных идентификаторов пользовательских сеансов, поэтому в случае захвата файла *cookie* злоумышленник может выдать себя за пользователя и получить несанкционированный доступ к веб-ресурсу.

JSON Web Token (*JWT*) был разработан в качестве альтернативы файлам *cookie*, как формат обмена аутентификационными и авторизационными данными в клиент-серверной архитектуре. *JWT* представляет собой закодированный набор информационных полей (объектов) в формате *JSON*, которые, в свою очередь, позволяют серверу произвести процессы аутентификации и авторизации пользователя [9]. Подпись осуществляют посредством закрытого ключа, в то время как проверку выполняют открытым ключом, выданным провайдером идентификации (с использованием алгоритмов *RSA* или *ECDSA*) [10].

JWT-токены состоят из заголовка, полезной нагрузки и подписи [11]. Заголовок обычно состоит из двух частей: типа токена (*JWT*) и используемого алгоритма подписи, например, *SHA256* или *RSA*. В полезной нагрузке (payload) должна передаваться информация, позволяющая серверу идентифицировать и в дальнейшем авторизовать пользователя. Подпись *JWT*-токена зависит от выбранного алгоритма шифрования. На рис. 1 представлена подпись при использовании алгоритма шифрования *SHA256*.

```
HMACSHA256 (
    base64UrlEncode(header) + " . " +
    base64UrlEncode(payload),
    secret)
```

Рис. 1. Подпись JWT-токена

При использовании атаки типа "человек посередине" (*Man-in-the-Middle*) злоумышленники располагаются между двумя машинами или сетевыми устройствами таким образом, чтобы они могли перехватывать и управлять трафиком между обеими сторонами. Злоумышленник ошибочно идентифицирует себя как существующий сетевой хост или службу, заставляя клиентов получить доступ к своей машине, а не к фактической службе. Затем все запросы от клиента к злоумышленнику будут ретранслироваться в фактическую службу, а все ответы от службы будут ретранслироваться обратно клиенту [12]. Теперь злоумышленник может свободно перехватывать поток данных и манипулировать ими в своих интересах. Большинство популярных почтовых сервисов и приложений онлайн-банкинга полагаются на *HTTPS*, чтобы гарантировать, что связь между веб-браузером и серверами осуществляется в зашифрованном виде [13].

Для демонстрации уязвимости с помощью инструмента *Burp Suite* был выполнен перехват пакетов, передающихся при авторизации на странице социальной сети m*.ru. В пакетах, передающихся методом *POST*, были обнаружены авторизованные данные пользователя (рис. 2).

Пароль был отправлен веб-ресурсом в открытом виде, будучи только лишь закодированным в urlencoded, что необходимо для отправки данных по сети. Данная проблема может привести к утечке учетных данных в случае успешного выполнения атак класса *Man-in-the-Middle*.

Методология

В качестве решения описанной проблемы открытой передачи авторизованных данных была предложена система с реализацией двухступенчатого процесса аутентификации и регистрации пользователя.

При авторизации логин пользователя в первую очередь отправляется на сторону сервера, где осуществляется проверка на наличие логина в базе данных. В том случае, если логин был обнаружен в базе данных, сервер отправляет обратно публичный ключ для шифрования пароля.

После получения от сервера ключа на стороне пользователя производится шифрование пароля. Далее зашифрованный пароль отправляется на сервер, где он расшифровывается, хэшируется и проверяется на соответствие сохраненному в базе данных хэшу.

Для реализации проекта были определены следующие компоненты и инструменты: *Redis-server*, *JavaScript*, *Rust*, *BCrypt*, *RSA*, *JSON*, *Node.js*. В качестве хранилища данных (база данных) был выбран *Redis* — это быстрое хранилище данных типа ключ—значение в памяти с открытым исходным кодом. *JavaScript* используется для написания клиентской части (*Frontend*). *Rust* был выбран для описания серверной части (*Backend*) и находящегося в нем *Crypto*-модуля.

```
18 Connection: close
19
20 username=SARMATSID%40mail.ru&Login=SARMATSID%40mail.ru&password=%2C2%3AKHxKY%3F%5C%24gC4%3C5&
   Password=%2C2%3AKHxKY%3F%5C%24gC4%3C5&saveauth=1&new_auth_form=1&FromAccount=
   opener%3Daccount%26allow_external%3D1%26twoSteps%3D1&act_token=
   7b1079891df1421abbfb0fe51554bdc4&page=
   https%3A%2F%2Fe.mail.ru%2Fmessages%2Finbox%3Fapp_id_mytracker%3D58519%26authid%3Dlacdeova.8nc
   %26back%3D1%26dwhsplit%3Ds10273.b1ss12743s%26from%3Dlogin%26x-login-auth%3D1&back=1&lang=
   en_US
```

Рис. 2. Перехваченные аутентификационные данные

Представленный метод позволяет помимо решения проблемы передачи пароля в открытом виде устранить уязвимости протокола *HTTPS*, так как в случае перехвата трафика, злоумышленник не получит пароль пользователя, потому что он передается в зашифрованном виде.

UML-диаграмма предложенного метода представлена на рис. 3.

Обсуждение

Для верификации разработанного метода путем исследования уровня безопасности было проведено тестирование с помощью сканеров уязвимостей.

Сканирование инструментом *Nessus* [14] обнаружило 4 уязвимости с категорией *Medium*, каждая из которых связана с *SSL* (рис. 4).

Обнаруженные уязвимости связаны с тем, что веб-ресурсом используется неподтвержденный SSL-сертификат для формирования безопасного зашифрованного *HTTPS*-соединения. В работе был сгенерирован самоподписанный сертификат *SSL*, поэтому уязвимость определена как допустимая в рамках демонстрационного варианта.

Результат показал надежность технической стороны разработанного проекта, а также высокий уровень защищенности от веб-атак.

Результаты сканирования инструментом *Netsparker* [15] показали, что была найдена одна угроза уровня *Medium* (рис. 5).

Рис. 3. UML-диаграмма разрабатываемого метода

Vulnerabilities 59

8 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	6.5	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	6.4 *	SSL Self-Signed Certificate	General	1
MEDIUM	5.3	SSL Certificate with Wrong Hostname	General	1
INFO		SSL Certificate Information	General	2
INFO		SSL Cipher Suites Supported	General	2
INFO		SSL Perfect Forward Secrecy Cipher Suites Supported	General	2
INFO		SSL Certificate 'commonName' Mismatch	General	1
INFO		SSL Cipher Block Chaining Cipher Suites Supported	General	1

Рис. 4. Результаты сканирования инструментом Nessus

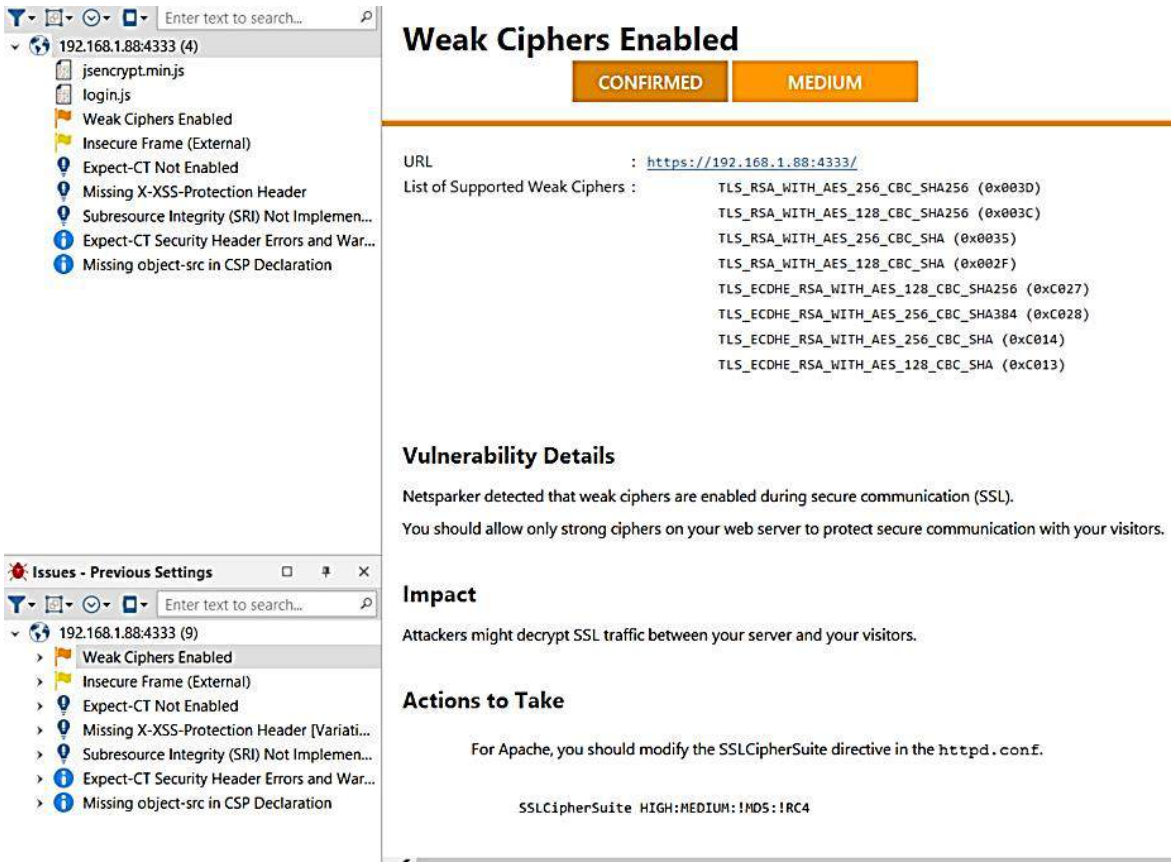


Рис. 5. Результаты сканирования инструментом Netsparker

Netsparker, как и *Nessus*, также обнаружил уязвимость использования самоподписанного сертификата *SSL*. В условиях реальной эксплуатации метода будет использоваться подписанный доверенным центром сертификации *SSL*-сертификат, привязанный к домену компании.

Заключение

Работа посвящена исследованию проблем процесса аутентификации на веб-ресурсе, а также разработке метода безопасной аутентификации с поддержанием сеанса пользователя с последующей реализацией в виде рабочего стенда, решающего выявленную проблему.

Авторами произведен анализ процесса аутентификации и защищенных способов аутентификации пользователя на веб-ресурсе, были определены факторы и типы аутентификации. Наиболее безопасным и надежным является многофакторная аутентификация, где от пользователя требуется два и более фактора проверки, что значительно снижает вероятность успешной кибератаки.

Исследованы два способа формирования сессии: файлы *cookie* и *JWT*-токены. Главной проблемой является возможность захвата файлов *cookie*, например посредством сниффера.

Поскольку большинство веб-сайтов используют файлы *cookie* в качестве единственных идентификаторов пользовательских сеансов, то в случае захвата файла *cookie* злоумышленник может выдать себя за пользователя и получить несанкционированный доступ.

Главным итогом исследования является наличие возможности перехвата пароля пользователя при его передаче в открытом виде. Для решения обнаруженной проблемы предложен метод, принцип которого заключается в использовании ассиметричного алгоритма шифрования *RSA*. В предложенном варианте аутентификации пароль на всех этапах сетевого взаимодействия передается в зашифрованном виде.

Литература

1. *Бушуев А. Л., Деревцова И. В., Мальцева Ю. А., Терентьева В. Д.* Роль информационной безопасности в условиях цифровой экономики // Baikal Research Journal. 2020. Т. 11. № 1. С. 6.

2. *Сухаревская Е. В.* Исследование систем аутентификации // Международный студенческий научный вестник. 2018. № 1. С. 71—71.

3. Шибанов С. В., Карпушин Д. А. Сравнительный анализ современных методов аутентификации пользователя // Математическое и программное обеспечение систем в промышленной и социальной сферах. 2015. № 1. С. 33—37.

4. *Ивличев П. С.* О проблеме небезопасных методов аутентификации пользователей и управления пользовательскими сессиями // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2021. № 7. С. 37—44.

5. *Метельков А. Н.* О проблеме аутентификации с использованием паролей при информационном взаимодействии // Национальная безопасность и стратегическое планирование. 2020. № 3. С. 59—68.

6. *Голубь И. С., Глаголев В. А.* Обзор методов двухфакторной аутентификации // Постулат. 2018. № 12-1(38). С. 95.

7. *Rezanov B., Kuchuk H.* Modeling the process of two-factor authentication // Advanced Information Systems. 2022. V. 6. № 2. P. 10—15.

8. *Choi Y. B., Loo Y. L., LaCroix K.* Cookies and Sessions: A Study of what they are, how they can be Stolen and a Discussion on Security // International J. Advanced Computer Science and Applications. 2019. V. 10. № 1.

9. *Колесников А. О.* Идентификация пользователей клиент-серверных приложений с помощью JWT-токена // ББК 1 Е91. 2021. С. 42.

10. *Лукашкин Е. В.* Разработка аутентификации, базирующейся на JWT-токенах: мат. XXIII республиканской науч. конф. студентов и аспирантов "Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях". 2020. С. 268—269.

11. *Бетелин А. Б., Егорычев И. Б., Прилипко А. А. и др.* О некоторых особенностях JWT аутентификации в веб-приложениях // Труды научно-исследовательского института системных исследований Российской академии наук. 2021. Т. 11. № 1. С. 4—10.

12. *Mallik A.* Man-in-the-middle-attack: Understanding in simple words // Cyberspace: J. Pendidikan Teknologi Informasi. 2019. V. 2. № 2. P. 109—134.

13. *Степанов П. П., Свалов А. А., Кобенко В. Ю., Гиль А. С.* Методы перехвата трафика // Прикладная математика и фундаментальная информатика. 2018. Т. 5. № 1. С. 60—65.

14. Nessus Vulnerability Assessment | Tenable [Электронный ресурс]. 2022. URL: https://www.tenable.com/products/nessus (дата обращения: 03.10.2022).

15. Netsparker professional — Web application security Scanner [Электронный ресурс]. 2022. URL: https://www.esecforte.com/products/netsparker-web-application-security-scanner/ (дата обращения: 03.10.2022).

Development of a system for secure authentication and maintaining a user session on a web resource

S. Yu. Sidorin
Company "Informzaschita", Moscow, Russia

A. A. Zherdev
Group-IB, Moscow, Russia

V. I. Sharmaev
Moscow Aviation Institute (National Research University), Moscow, Russia

Using the Burp Suite tool, authors demonstrated the possibility of intercepting a login and a request if it occurs in action. To solve this problem, a method for detecting user authentication and using a session on a web resource is proposed. A detailed description of the safety elements and technologies is given. Nessus and Netsparker vulnerability scanners were used to verify the developed method. The results of this study can be used in the development of tactical and technical means of the organization to create more effective user authentication algorithms, identify vulnerabilities and identify risks.

Keywords: information security, vulnerabilities, cyber-attacks, authentication, authorization, cookies, JWT tokens.

Bibliography — 15 references. *Received November 6, 2022*

УДК 004.056.53
DOI: 10.52190/2073-2600_2022_4_13
EDN: JCTYVV

Об особенностях формирования требований безопасности информации для масштабируемой доверенной платформы

[1]*А. В. Шарамок*, канд. техн. наук; [2]*Д. С. Брагин*; [1]*О. П. Симонова*
[1] Национальный исследовательский университет «МИЭТ», г. Зеленоград, Москва, Россия
[2] Центр компетенций национальной технологической инициативы «Технологии доверенного взаимодействия» Томского государственного университета систем управления и радиоэлектроники (ТУСУР), г. Томск, Россия

Изложены результаты работы по формированию требований безопасности информации для автоматизированной информационно-контролирующей системы сбора и обработки сенсорной информации, разрабатываемой Лидирующим исследовательским центром "Доверенные сенсорные системы". Описан подход к формированию требований безопасности информации в условиях противоречий участников разработки в рамках действующих ограничений проекта. Представленный подход может быть полезен при разработке других информационных систем в защищенном исполнении. Подход заключался в формировании логической связи между понятиями доверие и безопасность (защищенность) информационной системы, выделении доменов требований, анализа взаимосвязи и влияния доменов требований между собой с последующим формированием логической последовательности рассуждений для обоснования сформированных требований безопасности информации. Приведены оценки объема требований для различных уровней доверия.

Ключевые слова: информационная безопасность, защита информации, доверие, требования безопасности информации, требования доверия, доверенные сенсорные системы.

В Национальном исследовательском университете МИЭТ Лидирующим исследовательским центром "Доверенные сенсорные системы" завершается разработка автоматизированной информационно-контролирующей системы сбора и обработки сенсорной информации (далее масштабируемая доверенная Платформа). Важной особенностью этого проекта явился процесс формирования требований по информационной безопасности к разрабатываемой доверенной Платформе. Специфика формирования этих требований представлена в данной работе и может быть интересна при дальнейшем проведении аналогичных разработок.

Масштабируемая доверенная Платформа [1] представляет собой набор аппаратно-программных средств, упрощенная архитектура которого представлена на рис. 1.

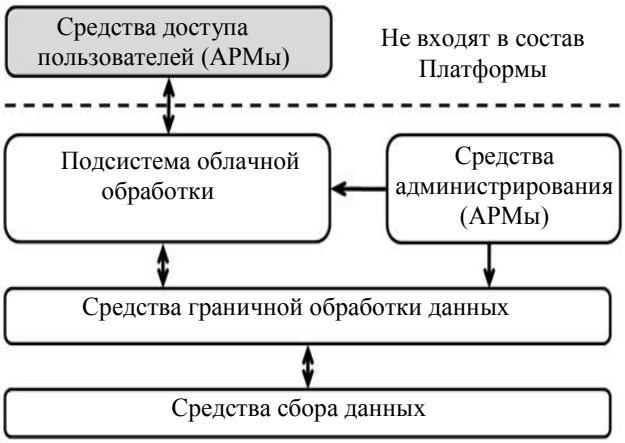


Рис. 1. Масштабируемая доверенная Платформа

Средства масштабируемой доверенной Платформы разделены на три уровня.

На нижнем уровне Платформы находятся средства сбора данных, реализованные в виде специализированного устройства под управлением микроконтроллера, которое осуществляет сбор показаний от разнородного набора датчиков.

Шарамок Александр Владимирович, доцент.
E-mail: sharamok@mail.ru
Брагин Дмитрий Сергеевич, руководитель проектного офиса.
E-mail: braginds@mail.ru
Симонова Ольга Петровна, инженер.
E-mail: otcs@miee.ru

Статья поступила в редакцию 10 ноября 2022 г.

Средства сбора данных могут осуществлять сбор, например, показаний от датчиков экологического мониторинга [2] или показаний различных параметров контролируемой среды [3].

Средства сбора данных передают данные на вышележащий уровень граничной обработки данных. Средства граничной обработки данных реализуются специализированным микропроцессорным устройством со встроенной операционной системой. Это средство осуществляет прием данных от нескольких средств сбора данных, агрегацию данных и промежуточную обработку данных в соответствии с концепцией граничных [4] и туманных вычислений [5].

С уровня граничной обработки данные передаются в подсистему облачной обработки, в которой осуществляется целевая прикладная обработка. Подсистема облачной обработки реализована в виде серверов, функционирующих на виртуальной инфраструктуре. Виртуальная инфраструктура не входит в рамки проекта и находится за границами безопасности рассматриваемой Платформы. Подсистема облачной обработки предоставляет доступ конечным пользователям к результатам обработки и хранимым данным. Доступ осуществляется с автоматизированных рабочих мест пользователей через веб-интерфейс, при этом средства доступа пользователей не входят в состав разрабатываемой Платформы и находятся за границами безопасности.

Администрирование Платформы осуществляется с автоматизированных рабочих мест администраторов, которые имеют доступ, как к подсистеме облачной обработки, так и к средствам граничной обработки данных.

Цель исследования

Требования по безопасности к разрабатываемой доверенной Платформе изначально формулировались в техническом задании в виде двух пунктов, содержание которых не позволяло однозначно понять предъявляемые требования. Формулировалось, что доверенная платформа — это набор аппаратно-программных средств, построенный с применением доверенной вычислительной базы (совокупности защитных механизмов информационной системы, реализующих определенную политику безопасности), и указывалось, что требования к защите информации от несанкционированного доступа должны быть сформированы на стадии разработки концепции.

Понимая, что выполнение требований защиты информации от несанкционированного доступа ведет к необходимости реализации ряда специфических решений, разработчики целевого функционала старались исключить требования по информационной безопасности (защите информации) из разрабатываемой концепции Платформы. Мотивируя это тем, что главенствующим является требование обеспечения доверия и реализации на доверенной вычислительной базе. Учитывая сложившуюся ситуацию, для корректного введения в проект требований по безопасности и обеспечению доверия необходимо было понять, что под доверием понимают участники проекта.

Первым тезисом по понятию доверия со стороны участников проекта было применение отечественной электронной компонентной базы (ЭКБ) или отдельных элементов на отечественной ЭКБ. В понимании разработчиков применение отечественного процессора в средствах граничной обработки данных подразумевало обеспечение доверия к Платформе.

Вторым тезисом была разработка платформы отечественными разработчиками. Предполагалось, что разработка доверенным (отечественным) коллективом должна обеспечить доверие к Платформе.

Третий тезис со стороны разработчиков заключался в том, что Платформа или её отдельные компоненты после разработки будут внесены в Единый реестр российских программ [6] или Единый реестр российской радиоэлектронной продукции [7]. Внесение Платформы в указанные реестры должно было обеспечить выполнение требований доверия.

Дополнительным четвертым тезисом, предложенным одним из участников проекта, было использование модного понятия "*Secure by Design*", т. е. реализация подхода по созданию безопасного в своей основе проекта Платформы, что должно обеспечить выполнение требований доверия.

Несмотря на то, что изложенные выше тезисы содержат компоненты обеспечения доверия, каждый из них по отдельности и вся их совокупность не соответствовали существующей международной и отечественной парадигме обеспечения доверия к продуктам информационной технологий (ИТ) [8, 9].

На основании предложенного можно констатировать, что участники проекта, используя модное понятие доверия, не понимали вытекающий из этого объем требований по обеспечению доверия и соответственно необходимый к выполнению объем работ.

Цель исследования авторов данной работы — формирование требований по обеспечению безопасности информации и доверия к Платформе с учетом формулировок в техническом задании на разрабатываемую Платформу, существующего

понимания требований доверия со стороны участников проекта и требований существующей нормативной базы в области обеспечения безопасности информации и доверия для продуктов ИТ.

Методология формирования требований обеспечения безопасности информации

Современная методология разработки защищённых информационных систем [8], средств защиты информации и продуктов ИТ предполагает разделение требований безопасности на две составляющие — это функциональные требования безопасности и требования доверия (табл. 1).

Функциональные требования безопасности — это требования к тем функциям безопасности, которые должны быть реализованы в системе. Примерами функциональных требований являются требования к идентификации, аутентификации (парольная защита, аутентификация с использованием сертификатов и др.), аудиту безопасности, неотказуемости источника (невозможности отказа от факта отправления сообщения), управления доступом, защиты трафика и т. д.

Требования доверия определяют насколько можно полагаться на реализованные механизмы функциональной безопасности, насколько они корректно реализованы и насколько они соответствуют среде безопасности, в которой предполагается применять защищенный продукт ИТ. Примерами требований доверия являются требования к строгости процесса разработки по поиску потенциальных уязвимостей и анализу их влияния на безопасность.

Методология формирования требований безопасности информации в РФ изложена в нормативных документах, соответствующих парадигме общих критериев оценки безопасности информационных технологий [8]. Формирование функциональных требований описано во второй части этого стандарта [11], а требования доверия — в третьей части стандарта [12].

Обеспечению доверия к продуктам ИТ дополнительно посвящены специализированные ГОСТы по основам доверия к безопасности информационных технологий [13—15]. Основным руководящим документом по обеспечению доверия в РФ является выписка из требований по безопасности информации, устанавливающая уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий [9].

Основываясь на приведенных документах и изложенной в них методологии, было осуществлено формирование требований безопасности информации для доверенной Платформы.

Связь между доверием и безопасностью

Для формирования требований безопасности информации необходимо обратиться к определению термина доверие (*assurance*) из приведённых выше документов:

- *первое определение* — выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности [13];
- *второе определение* — основание для уверенности в том, что сущность отвечает своим целям безопасности [8].

Необходимо отметить, что приведённые определения эквивалентны друг другу, и важным выводом из них является то, что доверие — это следствие из безопасности (защищенности) продукта или системы, т. е. продукт ИТ не может быть доверенным, если он не защищен, не соответствует некоторым целям безопасности. Доверие определяет уверенность насколько продукт ИТ соответствует своим целям безопасности.

Таблица 1

Разделение требований безопасности продуктов ИТ

Требования безопасности ИТ	
Функциональные требования безопасности	Требования доверия
Функциональные требования — это требования, предъявляемые к тем функциям продукта ИТ, которые предназначены для поддержания безопасности ИТ и определяют желательный безопасный режим функционирования продукта ИТ.	Требования доверия налагаются на действия разработчика, представленные свидетельства и действия оценщика.

Исходя из этого утверждения современной методологии обеспечения доверия до участников проекта была доведена необходимость формирования требований безопасности для разрабатываемой доверенной Платформы. Более того, в рамках проекта был принят подход, что доверие — это свойство Платформы, которое задает заказчик (владелец) Платформы для обеспечения уверенности в том, что принятые в Платформе контрмеры по противодействию угрозам минимизируют риски для защищаемых активов заказчика (владельца) Платформы и обеспечивается уверенностью[16]:

- в корректности реализации функций безопасности, т. е. оценки того, правильно ли они реализованы;
- в эффективности функций безопасности, т. е. оценки того, действительно ли они отвечают изложенным целям безопасности.

Недостатки отечественных подходов к обеспечению доверия

По мнению авторов, в приведенной совокупности документов по обеспечению доверия существует серьёзный пробел — отсутствие требования к разработке доверенного продукта ИТ доверенным разработчиком, т. е. обеспечения некоторого доверенного технологического маршрута разработки продукта ИТ. Например, еще более 20 лет назад в [17] указывалось — "для программного обеспечения, которое явно много проще человека, нет научно обоснованных проверок и рекомендаций по поиску закладок".

Приведенное утверждение остается верным и сегодня. Используемые методики по контролю отсутствия недекларированных возможностей [18, 19] как для программного, так и аппаратного обеспечения способны только снизить вероятность отсутствия недекларированных возможностей, но не могут гарантировать их отсутствия.

Остается верным предложенный в [17] подход — "идеальным вариантом была бы разработка его (программного обеспечения) коллективом, которому государство может доверять, т. е. коллективу, который сам прошел соответствующую кадровую проверку. Тогда данное программное обеспечение можно было бы назвать доверенным". Отметим, что приведенный тезис соответствует одному из тезисов, высказанному участниками проекта по разработке доверенной Платформы, в [20] этот тезис был назван базисом доверия.

Несмотря на отсутствие базиса доверия в отечественных нормативных документах в явном виде, сложившаяся в последнее время конъюнктура компенсирует этот недостаток.

В настоящее время созданы Единый реестр российских программ для электронных вычислительных машин и баз данных [6] и Единый реестр российской радиоэлектронной продукции [7], критерии попадания в которые ставят серьезный барьер для продуктов ИТ от разработчиков, которым не доверяют. При этом применение продуктов ИТ в ответственных системах во многих случаях невозможно без присутствия в приведенных реестрах.

Взаимосвязи доменов требований масштабируемой доверенной Платформы

В [20] было сформулировано понятие доменов требований. Домен требований — это совокупность взаимосвязанных между собой технических требований к продукту ИТ. Для одного продукта ИТ может быть несколько доменов требований, при этом требования могут быть сгруппированы в домены таким образом, что различные домены требований могут существовать относительно независимо друг от друга. Примерами доменов требований могут быть функциональные требования безопасности и требования доверия.

При разработке требований для доверенной Платформы были сформулированы три домена требований:

- функциональные требования к доверенной Платформе, требования к целевому функционалу доверенной Платформы;
- функциональные требования безопасности, сформулированные с точки зрения необходимых функций безопасности;
- требования доверия к Платформе.

Дополнительно были определены два субъекта, влияющие на требования к доверенной Платформе, — это "Заказчик" и "Среда безопасности". Под "Заказчиком" подразумевалась вся совокупность субъективных факторов, влияющих на требования к разрабатываемой доверенной Платформе. Под "Средой безопасности" понималась вся совокупность факторов (технические, организационные, экономические, правовые и прочие), влияющих на требования безопасности информации [16].

Домены требований и взаимосвязи между ними представлены на рис. 2.

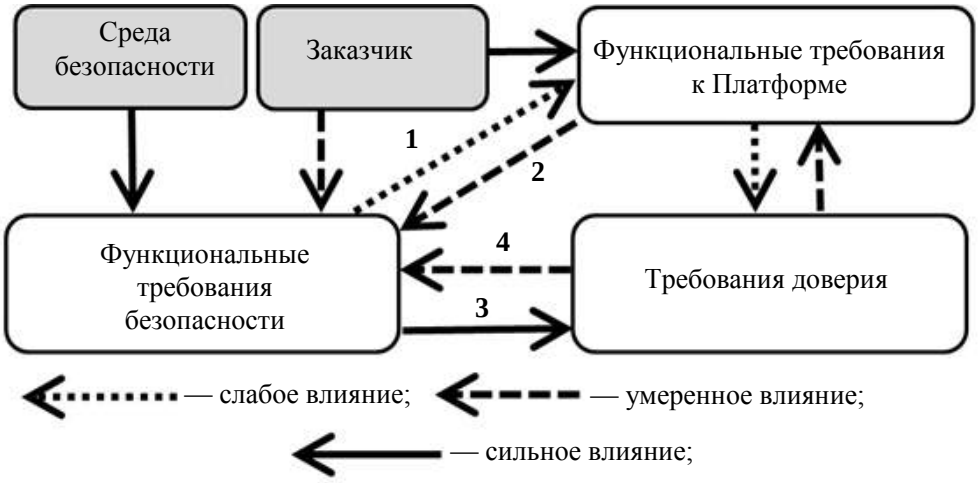


Рис. 2. Взаимосвязь доменов требований доверенной Платформы

Для описания влияния доменов требований друг на друга были классифицированы три уровня возможного влияния доменов друг на друга: слабое влияние, умеренное влияние и сильное влияние.

Заказчик сильно влияет на функциональные требования к доверенной Платформе и умеренно влияет на функциональные требования безопасности. Умеренное влияние на функциональные требования безопасности обусловлено отсутствием у заказчика компетенции в вопросах безопасности, но присутствием влияния через бюджет и ограничения проекта. Среда безопасности является определяющим фактором (сильное влияние) для функциональных требований безопасности. На рис. 2 представлено влияние других доменов требований друг на друга:

1. Слабое влияние функциональных требований безопасности на функциональные требования Платформы обусловлено влиянием только через общие ограничения проекта.

2. Умеренное влияние функциональных требований к Платформе на функциональные требования безопасности обусловлено необходимостью реализации защиты для целевого функционала Платформы.

3. Сильное влияние функциональных требований безопасности на требования доверия при императивном формулировании требований безопасности. При императивном подходе к формированию требований безопасности установленному классу защиты однозначно соответствует уровень доверия [9].

4. Умеренное влияние требований доверия на функциональные требования безопасности через требования к стойкости функций безопасности и качеству их реализации.

5. При императивном формулировании требований безопасности существует слабое влияние функциональных требований к Платформе на требования доверия, заключающееся во влиянии через ограничения проекта, таких как конкуренция за общий ресурс проекта (требования бюджетов, сроков и др.).

6. Умеренное влияние требований доверия на функциональные требования к Платформе через необходимость разработки дополнительных доказательств удовлетворения требований доверия, таких как требования к качеству документирования и тестирования, требования к процессу разработки и др.

Логическая последовательность формирования требований безопасности информации

Проведенный выше анализ позволил сформировать логическую последовательность формирования требования безопасности информации к доверенной Платформе (рис. 3). В логическую цепочку были введены псевдооперации, позволяющие формализовать условия перехода от одного этапа формирования требований к другому этапу. Операции выполняют некоторые внешние по отношению к доверенной Платформе субъекты, введенные ранее: "Заказчик" и "Среда безопасности".

1. Платформа должна быть доверенной (**императивное требование**, ***Заказчик***),
2. Доверие есть безопасность (**логическая связь**);
3. Для формирования требований безопасности необходимо классифицировать Платформу (ИСПДн, КИИ, АСУТП или др.) (**выбор,** ***Заказчик***),
4. Формирование требований безопасности (функциональных и доверия) (**итерация**)

Влияние ограничений (бюджет, сроки, подготовленность разработчиков и т. д.)

4.1. В соответствии с РД ФСТЭК РФ необходимо определить класс (уровень) защищенности (**выбор,** ***среда безопасности***);
4.2. Класс защищенности определяет уровень доверия (**логическая связь**);

Рис. 3. Последовательность формирования требований

В псевдооперации введены:

- **императивное требование** — формирование внешним субъектом требований;
- **логическая связь** — переход от одного утверждения к другому в соответствии с логической связью, определяемой внешними факторами;
- **выбор** — выбор внешним субъектом из нескольких возможных вариантов, определяемых внешними факторами;
- **итерация** — повторение набора операций до достижения желаемого результата (условия).

В результате применения приведённой логической цепочки рассуждений было определено, что доверенную Платформу предлагается применять на объектах критической информационной инфраструктуры и к ней предъявляются требования по обеспечению безопасности информации третьей категории для значимых объектов критической информационной инфраструктуры [21, 22] и предъявляются требования по обеспечению доверия в соответствии с шестым уровнем доверия [9]. На основании отнесения к указанному классу объектов КИИ и соответствующему уровню доверия были сформированы требования по безопасности информации для доверенной Платформы.

Обсуждение результатов работы

Несмотря на то, что было принято решение формировать требования безопасности информации к доверенной Платформе на основании требований к объектам КИИ выбор вида требований (к АСУ, АСУ ТП или объект КИИ) не носит принципиального характера, так как разделение по классам безопасности внутри этих требований дает приблизительно одинаковые требования по безопасности к системам и техническим средствам из их состава (табл. 2). Возможным преимуществом использования требований к АСУ и АСУ ТП [23] перед требованиями к объектам КИИ может являться отсутствие требования подключения к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) [24].

Таблица 2

Соотнесение требований безопасности информации для КИИ и АСУ ТП

Тип системы	Средства защиты информации	Средства вычислительной техники	Интерфейс для передачи данных в систему ГосСОПКА	Критерии оценки	Основание
КИИ 3-й категории	6-го класс защиты	Не ниже 5-го класса защиты	Да	Объективные, опираясь на конкретные количественные показатели, но с учетом экспертного мнения.	Приказ ФСТЭК № 239 [21], ФЗ 187 [24]
АСУ ТП 3-го класс защищенности	6-го класс защиты	Не ниже 5-го класса защиты	Нет	Субъективные, опираясь только на мнение экспертов.	Приказ ФСТЭК № 31 [23]

При проведении итерационного формирования требования безопасности информации (рис. 3) был проведен анализ требований уровней доверия [9], и выявлено, что в документе можно выделить 89 пунктов требований, из них 43 требования можно соотнести со стандартными требованиями по разработке, производству и эксплуатации изделий и программных продуктов, обеспечивающих качество разработки, и только 46 требований являются дополнительными требованиями по обеспечению доверия. При этом из этих дополнительных требований 21 требование доверия приводит к дополнительным работам на этапе разработки, 14 требований предъявляется к этапу проведения сертификации и 11 требований необходимо выполнять на этапе эксплуатации.

Примем за 100 % объем требований обеспечения доверия требования по 4-му уровню выписки (89 пунктов требований), то для 5-го уровня доверия объем требований сокращается до 76 % (68 пунктов требований), для 6-го уровня доверия объем требований сокращается до 58 % (52 пунктов требований). Сравнение объема требований представлено в табл. 3.

Таблица 3

Оценка объема требований доверия для Платформы

	Уровни доверия		
Оценка соотношения объема дополнительных работ	6-й	5-й	4-й
	58 %	76 %	100 %

В рамках представленного исследования предпринималась попытка ввести меру объема работ для доверенной Платформы в зависимости от установленного уровня доверия. К сожалению, авторам это сделать не удалось, и они видят введение такой меры предметом дальнейшего исследования. Представленные результаты в виде логики формирования требований безопасности информации, оценки объема требований при выборе того или иного уровня доверия могу быть использованы при формировании требований для других продуктов ИТ и информационных систем.

Заключение

Авторы постарались изложить результаты работы по формированию требований безопасности информации для масштабируемой доверенной Платформы. При этом авторы полагают, что трудности и обстоятельства, с которыми они столкнулись, являются весьма типичными при разработке информационных систем в защищенном исполнении. Эти трудности в основном связаны с противоречиями участников разработки в рамках действующих ограничений проекта. Изложенный опыт авторов и примененный ими подход к формированию требований безопасности информации может быть полезен при разработке других информационных систем в защищенном исполнении.

Работа подготовлена в рамках реализации программы ЛИЦ "Доверенные сенсорные системы" (Договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО "РВК". Идентификатор соглашения о предоставлении субсидии — 0000000007119P190002.

Литература

1. *Bulatov E., Konev A., Bragin D., Bakhtin A., Sharamok A.* Information security subsystem model for a trusted platform for collecting and processing sensory information // Lecture Notes in Networks and Systems. 2021. V. 228. P. 325—340.

2. *Шарамок А.* В. Автоматизированная система мониторинга окружающей среды как объект защиты информации // Вопросы защиты информации. 2020. № 1(128). С. 61—67.

3. *Djuzhev N. A., Demin G. D., Makhiboroda M. A., Evsikov I. D., Pozdnyakov M. M., Bespalov V. A., Ryabov V. T.* Measurement system for wide-range flow evaluation and thermal characterization of MEMS-based thermoresistive flow-rate sensors // Sensors and actuators A: Physical. 2021. V. 330. P. 112832. DOI: 10.1016/j.sna.2021.112832

4. *Кашкаров Д. В., Кучерявый А. Е.* Анализ приложений и перспектив развития технологий граничных вычислений с множественным доступом в сетях связи // Информационные технологии и телекоммуникации. 2020. Т. 8. № 1. С. 28—33.

5. *Лоднева О. Н.* Аналитический обзор методов построения туманных вычислений // Современные информационные технологии и ИТ-образование. 2020. Т. 16. № 2. С. 358—370. DOI 10.25559/SITITO.16.202002.358-370

6. Единый реестр российских программ для электронных вычислительных машин и баз данных (Постановление Правительства РФ от 16 ноября 2015 г. № 1236).

7. Единый реестр российской радиоэлектронной продукции (Постановление Правительства РФ от 10.07.2019 г. № 878).

8. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель.

9. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка). Утверждена приказом ФСТЭК России от 30 июля 2018 г. № 131.

10. ГОСТ Р ИСО 7498-2-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 2. Архитектура защиты информации.

11. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности.

12. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Компоненты доверия к безопасности.

13. ГОСТ Р 54581-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Ч. 1. Обзор и основы.

14. ГОСТ Р 54582-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Ч. 2. Методы доверия.

15. ГОСТ Р 54583-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Ч. 3. Анализ методов доверия.

16. ГОСТ Р 57628-2017 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

17. *Расторгуев С. П.* Информационная война. — М.: Радио и связь, 1999. — 416 с.

18. Руководящий документ. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации 4 июня 1999 г. № 114.

19. Информационное сообщение. Об утверждении методики выявления уязвимостей и недекларированных возможностей в программном обеспечении. ФСТЭК России 10 февраля 2021 г. № 240/24/647.

20. *Бахтин А. А., Брагин Д. С., Конев А. А., Шарамок А. В.* Оценка соответствия модели угроз и требований доверия систем Интернета вещей массового применения // Наноиндустрия. 2020. Т. 13. № S4(99). С. 137—138.

21. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены приказом ФСТЭК России 25 декабря 2017 г. № 239.

22. *Петухов А. Н. и др.* Управление безопасностью критических информационных инфраструктур: учеб. пособие / под ред. А. В. Душкина. — М.: МИЭТ. 2021. — 240 с.

23. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждена приказом ФСТЭК России 14 марта 2014 г. № 31.

24. Федеральный закон -ФЗ О безопасности критической информационной инфраструктуры Российской Федерации. Утвержден 26.07.2017 г. № 187.

About the specifics of information security requirements development for a scalable trusted platform

[1] A. V. Sharamok, [2] D. S. Bragin, [1] O. P. Simonova

[1] National Research University MIET, Zelenograd, Moscow, Russia

[2] Competence Center of the National Technology Initiative "Trusted Interaction Technologies" of Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, Russia

The results of the work on the development of information security requirements for an automated information control system for collecting and processing sensory information developed by the Leading Research Center "Trusted Sensor Systems" are presented. The approach to the formation of information security requirements in the conditions of contradictions of the development participants within the existing project constraints is described. The presented approach can be useful in the development of other secured information systems. The approach consisted in developing a logical connection between the concepts of assurance and an information security, identifying the domains of requirements, analyzing the relationship and influence of the domains each other, followed by the formation of a logical sequence of reasoning to justify the formed information security requirements. Estimates of the volume of requirements for different assurance levels.

Keywords: information security, information protection, assurance, information security requirements, assurance requirements, trusted sensor systems.

Bibliography — 24 references. *Received November 10, 2022*

УДК 004.056.5
DOI: 10.52190/2073-2600_2022_4_21
EDN: JGVTOS

Направления обеспечения информационной безопасности объектов военного назначения от утечки речевой информации по техническим каналам, образованными лазерными акустическими системами разведки

И. С. Рекунков, канд. техн. наук; *В. А. Щербаков*, д-р техн. наук
Военная академия РВСН им. Петра Великого, г. Балашиха, Московская обл., Россия

Рассмотрены перспективные направления обеспечения информационной безопасности объектов военного назначения от утечки речевой информации по техническим каналам, образованным лазерными акустическими системами разведки.

Ключевые слова: информационная безопасность, акустооптический технический канал утечки информации, лазерная акустическая системы разведки.

Акустооптический (лазерный) технический канал утечки информации образуется при облучении лазерным лучом вибрирующих в акустическом поле, возникающем при ведении разговоров, тонких отражающих поверхностей (стекол окон, картин, зеркал и т. д.). Отраженное лазерное излучение модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация. Причем лазер и приемник оптического излучения могут быть установлены в одном или различных местах (помещениях).

Для перехвата речевой информации по данному каналу используют сложные лазерные акустические системы разведки (ЛАСР).

ЛАСР состоит из источника когерентного излучения (лазера) и приемника оптического излучения, оснащенного фокусирующей оптикой.

Принцип действия системы заключается в следующем: передатчик осуществляет облучение наружного оконного стекла узким лазерным лучом; приемник принимает рассеянное отраженное излучение, модулированное по амплитуде и фазе по закону изменения акустического (речевого) сигнала, возникающего при ведении разговоров в контролируемом помещении; принятый сигнал детектируется, усиливается и прослушивается на головных телефонах или записывается на носитель информации. Для улучшения разборчивости речи в приемнике используется специальное шумоподавляющее устройство.

Для наведения лазерного луча на цель совместно с передатчиком и приемником используются специальные устройства — визиры.

Современные ЛАСР позволяют снимать информацию не только с наружных, но и с внутренних оконных стекол, зеркал, стеклянных дверей и других предметов.

К типовой лазерной акустической системе разведки относится система HKG GD-7800, которая состоит из передатчика на основе полупроводникового лазера мощностью 5 мВт и работающего в диапазоне 0,75—0,84 мкм и приемника лазерного излучения на основе малошумящего PIN-диода, закамуфлированного под стандартную зеркальную камеру. При переноске вся система размещается в обычном кейсе.

В данной статье будут рассмотрены направления обеспечения информационной безопасности объектов военного назначения от утечки речевой информации по техническим каналам, образованным лазерными акустическими системами разведки.

Защита выделенного помещения является важной частью комплекса мер, направленных на повышение информационной безопасности объектов военного назначения. В реальных условиях задача сводится к нахождению баланса между степенью защищенности выделенного помещения, денежными затратами на его реализацию, а также комфортом использования помещения.

Рекунков Иван Сергеевич, докторант кафедры.
E-mail: ivan.grek.1982@mail.ru
Щербаков Виталий Алексеевич, заместитель начальника кафедры.
E-mail: svasvarog@yandex.ru

Статья поступила в редакцию 28 ноября 2022 г.

Защищенность выделенного помещения оценивается исходя из модели угроз, которая в обязательном порядке включает [1, 2]:

- ведение визуально-оптической разведки;
- применение закладных устройств;
- применение лазерных систем акустической разведки;
- применение направленных микрофонов, в т. ч. электронных стетоскопов и игольчатых микрофонов.

Комфорт использования выделенного помещения сильно зависит от:

- наличия в нем оборудования для проведения демонстраций;
- удобной и красивой мебели;
- элементов роскоши, сопутствующих ведению переговоров;
- акустических свойств помещения;
- средств кондиционирования;
- освещения, особенно естественного;
- общего стиля выделенного помещения.

Денежные затраты всегда рассчитываются в контексте комфорта и защищенности. Таким образом, трилемма: защищенность—комфорт—стоимость для выделенного помещения схожа с аналогичным состоянием: целостность—доступность—конфиденциальность для информации. Улучшение любого показателя ведет к ухудшению других.

Наличие окна в выделенном помещении существенно улучшает его освещенность, кондиционирование, создается приятная атмосфера для ведения переговоров. Однако окно является каналом визуально-оптической и акустической утечки информации. На практике окна оснащают двойным пластиковым стеклопакетом для звукоизоляции, задергивают плотными шторами или жалюзи. Для нивелирования возможности перехвата речевой информации посредством систем лазерно-акустической разведки используют генераторы шума, рольставни.

С учетом требований, предъявляемых к оборудованию выделенного помещения, окно теряет все свои положительное свойства с точки зрения сохранения эргономических свойств помещения и рассматривается лишь в качестве потенциального источника угрозы утечки информации. Более того, шторы и жалюзи подвержены запылению, загрязнению, требуют стирки. В ряде случаев регулярная стирка вообще невозможна. В качестве альтернативы шторам и жалюзи авторы предлагают вариант, предусматривающий использование в стеклопакете smart-стекла вместо обычного.

Smart-стекло (умное стекло) — композит из слоев стекла и различных химических материалов, изменяющий свои оптические свойства при изменении внешних условий, например, освещённости, температуры или при подаче электрического напряжения. Smart-стекла могут изготавливаться на основе:

- жидкокристаллического слоя (LCD, liquid crystal devices);
- взвешенных частиц (SPD, suspended particle devices);
- электрохромного слоя.

Для использования внутри офисов наибольшее распространение получили смарт-стекла на основе LCD-слоя, структурная схема и принцип работы такого стекла изображены на рис. 1.

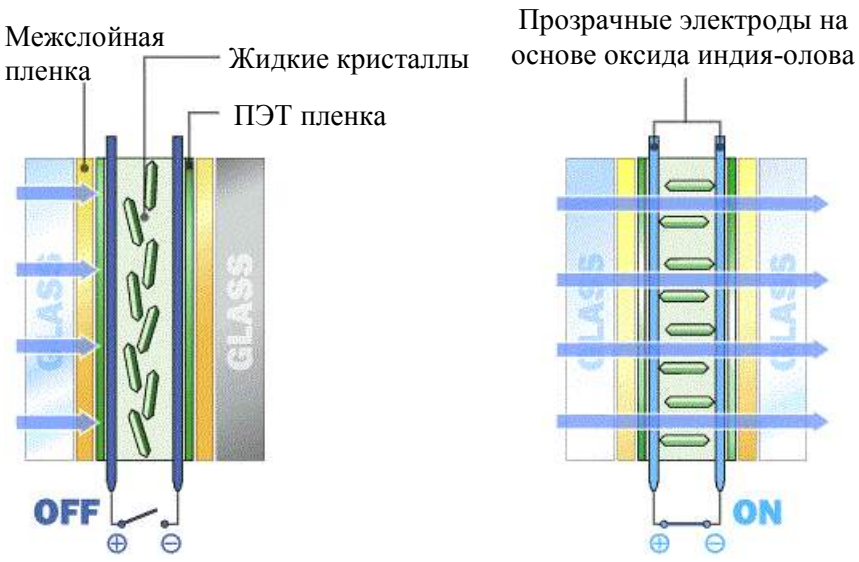


Рис. 1. Структурная схема и принцип работы LCD смарт-стекла

При отсутствии электрического напряжения полимерно-дисперсные жидкие кристаллы находятся в неполяризованном состоянии, из-за чего стекло является непрозрачным. При подаче постоянного напряжения 12—100 В кристаллы поляризуются, стекло становится прозрачным. Пример использования основных свойств smart-стекла показан на рис. 2.

Рис. 2. Смарт-стекло в качестве окна офиса

Как показано на рис. 2, при переводе стекла в "защищенный" режим свет продолжает поступать в помещение, тем самым сохраняя естественное освещение помещения, при этом оптическая непрозрачность стекла не позволяет эффективно использовать лазерные акустические системы перехвата речевой информации, что в свою очередь, обеспечивает сохранение комфортности помещения, с одной стороны, и его защищенность, с другой.

Типовые оптические характеристики LCD smart-стекол представлены в табл. 1.

Таблица 1

Типовые оптические характеристики LCD смарт-стекол

Характеристики	Стекло включено	Стекло выключено
Пропускание света в видимом диапазоне	70—80 %	50—70 %
Оптическая чистота	76—80 %	4—10 %
Отражение света в видимом диапазоне	14—18 %	18—24 %
Пропускание света в УФ-диапазоне	0,5—14 %	0,5—14%
Пропускание света в ИК-диапазоне	40—60 %	10—40 %
Угол обзора	120—160°	120—160°

Приведенные в таблице данные получены путем анализа отчетов о тестировании смарт-стекол по международному стандарту EN 410, а также из научных статей и технических характеристик, заявляемых производителями [3—5].

С точки зрения защиты информации от утечки по акустооптическому каналу важно, чтобы оптическая чистота была минимальной при выключенном состоянии стекла. Под чистотой здесь подразумевается количество света, которое подвержено рассеиванию под углом менее 2,5° от нормального. Определение порогового значения этого параметра для использования смарт-стекол в выделенном помещении является перспективной темой для дальнейших научных исследований.

Пропускание света для смарт-стекла в ИК- и УФ-спектре также должно быть минимальным.

В ближнем ИК-диапазоне для смарт-стекла были получены следующие фотографии в зависимости от напряжения на стекле: слева направо 80 В, 45 В, 0 В [6]. При отсутствии напряжения человека за стеклом не видно.

Рис. 3. Смарт-стекло в ближнем ИК-диапазоне

Звукоизолирующие свойства конструкций на основе smart-стекол практически не отличаются от свойств конструкций на основе обычных стекол и сильно зависят от ширины стекла, а также от рамы в которую их устанавливают. Типовые характеристики коэффициента ослабления звука для LCD smart-стекла в зависимости от его толщины представлены в табл. 2. Также некоторые производители предлагают smart-стекла с повышенной звукоизоляцией, но технические характеристики не публикуют.

Таблица 2

Типовые значения коэффициента ослабления звука для LCD smart-стекол

Толщина композита, мм	Толщина слоев: первое стекло / LCD слой / второе стекло, мм	Среднее ослабление звука в октавных полосах, дБ
9,2	4 / 1,2 / 4	35
11,2	5 / 1,2 / 5	37
13,2	6 / 1,2 / 6	39
25,2	12 / 1,2 / 12	44

Экономически выгодно устанавливать смарт-стекло в паре с обычным стеклом в двойной стеклопакет, это повысит звукоизолирующие свойства окна, но по стоимости получится дешевле стеклопакета с двумя smart-стеклами. Помимо использования композитного smart-стекла, возможно использовать лишь LCD-слой, наклеив его поверх обычного стекла (smart-пленка). Этот вариант то-

же дешевле, но, что более важно, он способствует сохранению акустических свойств исходного стекла, то есть такую пленку возможно наклеить поверх стекла звукоизолирующего окна, тем самым будет обеспечена надлежащая защита информации от утечки по акустическому и визуально-оптическому каналу.

Аналогично окну с обычным стеклом окна со smart-стеклом требуют использования генератора шума для защиты речевой информации от утечки посредством использования систем лазерно-акустической разведки, однако, в данном случае эффективность использования ЛАСР будет обусловлена лишь возможностью.

Помимо окон, smart-стекло также может использоваться в качестве материала для дверей и стен. Такой подход вписывается в концепцию помещения открытого типа. Более того, в таких конструкциях отсутствуют потенциально опасные с точки зрения защиты информации коммуникационные каналы (арматура, трубы и т. д.).

На рис. 4 представлена переговорная комната, полностью выполненная из смарт-стекла, для повышения звукоизоляции выложен второй ряд стен из обычного стекла.

При поданном напряжении видно происходящее в комнате, при отсутствии напряжения — не видно. Сведений об ослаблении звука производитель не предоставил.

На основе изложенных в статье данных, был проведен анализ возможности использования композитных смарт-стекол и смарт-пленки для защиты информации в выделенных помещениях, результаты представлены в табл. 3.

Как показывают результаты анализа, на данном этапе развития технологии рациональнее использовать smart-стекла и smart-пленку исключительно для окон выделенного помещения. Отделка дверей и стен возможна, но нецелесообразна ввиду необходимости использования генератора шума, а также генератора акустической помехи для компенсации относительно небольших звукоизоляционных качеств. Для выявления пороговых значений коэффициента оптической чистоты, а также пороговых значений пропускания в УФ- и ИК-диапазонах требуются дополнительные исследования.

Рис. 4. Переговорная комната, выполненная из смарт-стекла

Таблица 3

Результаты анализа возможностей использования композитного smart-стекла и smart-пленки для защиты информации в выделенных помещениях

№ п/п	Направление применения	Особенности	Требуется генератор шума	Требуется генератор речевой помехи
1	В качестве стен выделенного помещения	Требует двойного остекления с зазором порядка 200 мм. Стекла должны быть достаточно толстыми, каркас должен обладать высокими звукоизолирующими свойствами, оснащен поперечными профилями для стыкования стекол	Да	Да
2	В качестве дверей выделенного помещения	Требуется дверная рама с возможностью подвести провода и с повышенной звукоизоляцией, стык двери и дверного проема должен быть оформлен в виде специального паза. На рынке существуют готовые решения со звукоизоляцией до 45 дБ	Да	Да
3	В качестве окон выделенного помещения	В случае использования пленки потребуется подводить провода, что возможно не для любого стеклопакета	Да	Нет

Явными преимуществами использования смарт-стекол вместо обычных являются: возможность обеспечить естественное освещение в выделенном помещении без угрозы утечки информации через акустооптический канал; отказ от штор и жалюзи, требующих стирки; повышение общего комфорта в выделенном помещении, сопутствующего ведению переговоров.

Вторым направлением обеспечения информационной безопасности объектов военного назначения от утечки речевой информации по техническим каналам, образованным лазерными акустическими системами разведки является — использование устройства перекрытия, представляющего собой пленку-штору с флуоресцентными пигментными пятнами, светящимися под воздействием искусственного ультрафиолетового излучения, при использовании которой обеспечивается возможность обнаружения факта попытки получения несанкционированного доступа к речевой информации с использованием лазерных акустических систем разведки, а за счет того, что четко определены требования к размещению пятен, их размерам и взаимному расположению друг относительно друга, обеспечиваются необходимые и достаточные эргономические условия, характеризующиеся тем, что светопропускающе-рассеивающая поверхность пленки, свободная от флуоресцентных пигментных пятен, достаточна для прохождения солнечного света или уличного освещения, но недостаточна для свободного прохождения лазерного луча системы разведки.

Сущность устройства поясняется чертежом, представленным на рис. 5.

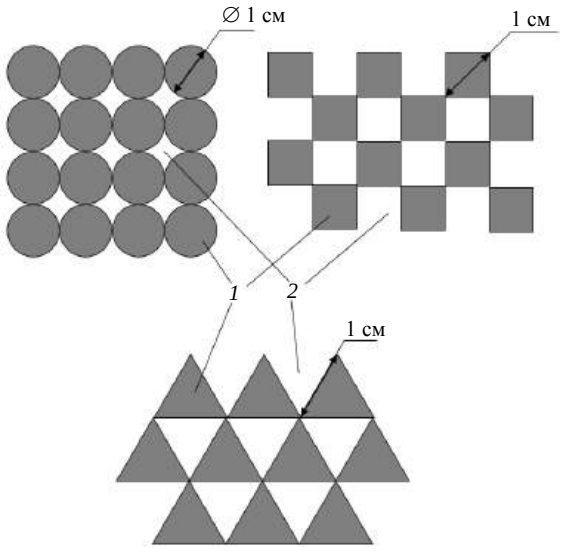


Рис. 5. Варианты исполнения флуоресцентных пигментных пятен на светопропускающе-рассеивающей поверхности пленки

На рис. 5 приведены варианты исполнения флуоресцентных пигментных пятен на светопропускающе-рассеивающей поверхности пленки, в составе:

1 — пятно с флуоресцентным пигментом;

2 — светопропускающе-рассеивающая поверхность пленки.

Устройство работает следующим образом: в случае реализации перехвата акустической информации из интересуемого помещения с использованием лазерной акустической системы разведки, функционирующей в ультрафиолдетовом диапазоне длин волн злоумышленники направляют луч лазера через оконный проем на светопропускающе-рассеивающую поверхность пленки, которая имеет в своем составе набор пятен с флуоресцентным пигментом, размещенных так, что их размер по площади был бы не менее одного квадратного сантиметра, а расстояние между пятнами было бы равно не более одного сантиметра. С учетом возможностей современных образцов подобных систем площадь пятна сфокусированного луча лазера на мишени — светопропускающе-рассеивающей поверхности пленки на расстоянии от 50 м составляет приблизительно 2 см.

Характер размещения пятен, вариант которого приведен на рис. 5, а также то, что максимально возможный линейный размер светопропускающе-рассеивающей поверхности пленки, свободный от пятен с флуоресцентным пигментом, не превышает одного сантиметра, приведет к тому, что площадь пятна контакта потока излучения лазера через светопропускающе-рассеивающую поверхность пленки превысит площадь, свободную от пятен с флуоресцентным пигментом, и тем самым вызовет свечение той области пятен с флуоресцентным пигментом, площадь которых пересекается с площадью пятна контакта потока излучения лазера. При этом участники переговоров будут осведомлены о факте попытки перехватить содержание речевой информации и смогут предпринять необходимые действия организационного или технического характера.

В случае отсутствия деятельности злоумышленников солнечный свет, а также свет от внешних источников освещения, будет попадать в защищаемое помещение через светопропускающе-рассеивающую поверхность пленки, свободной от пятен с флуоресцентным пигментом, тем самым сохраняя эргономические свойства помещения.

С учетом того, что достаточно широко известны материалы и вещества, выполненные как целиком, так и в виде красителей, которые нашли широкое применение, например, в криминалистике

для пометки документов или купюр, и которые под воздействием искусственного ультрафиолетового излучения начинают светиться в видимом диапазоне длин волн, реализовать производство пленки-шторы будет достаточно легко. Пигментные пятна можно наносить непосредственно на светопропускающе-рассеивающую поверхность пленки или можно наклеить на неё, а также они могут быть включены в её состав на стадии производства самой светопропускающе-рассеивающей пленки.

Для сохранения эргономических свойств пленки-перекрытия-шторы пигментацию целесообразно проводить не по всей поверхности перекрытия, а только с учетом возможностей системы фокусировки лазерной акустической системы разведки. Для придания пленке-перекрытию-шторе сходства с типичными элементами оборудования окна, например, бытовыми шторами, пигментация пленки-перекрытия-шторы может быть осуществлена в виде принта с изображением совокупности геометрических примитивов, например, чередования окружностей, диаметр которых не превышает 1 см, или чередования квадратов с диагональю, не превышающей 1 см, или чередования равнобедренных треугольников с длинной стороны, не превышающей 1 см, как показано на рис. 5.

В случае появления более совершенных систем фокусировки луча лазера требования к размещению пигментных пятен на поверхности пленки-перекрытия-шторы могут быть пересмотрены. Кроме того, в целях экономии времени и средств на изготовление нового защитного перекрытия, пленка—перекрытие—штора, в данном случае может быть установлена в два слоя со смещением одного рисунка защитного перекрытия относительно другого, что приведет к уменьшению площади светопропускающе-рассеивающей поверхности пленки, свободной от пятен с флуоресцентным пигментом.

Учитывая типовой размер стандартных оконных проемов, заблаговременно подготовленная защитная пленка-перекрытие-штора легко может быть использована на других объектах в случае передислокации организации.

Таким образом, применение предложенных перспективных направлений позволит обеспечить информационную безопасность объектов военного назначения от утечки речевой информации по техническим каналам, образованным лазерными акустическими системами разведки.

Литература

1. *Хорев А. А.* Техническая защита информации: учеб. пособие: в 3-х т. Т. 1. Технические каналы утечки информации. — М.: НПЦ "Аналитика", 2008. — 436 с.
2. *Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. и др.* Технические средства и методы защиты информации: учеб. пособие для студентов вузов / под ред. А. П. Зайцева, А. А. Шелупанова. — М.: Лань, 2012. — 616 с.
3. URL:http://smartglassinternational.com/downloads/LC_SmartGlass_Handbook.pdf (дата обращения: 04.05.2021).
4. URL:https://www.huichipdlc.com/uploads/201812035/Smart-glass-technical-data.pdf (дата обращения: 04.05.2021).
5. *Hemaida A., Ghosh A., Sundaram S., Mallick T. K.* Evaluation of thermal performance for a smart switchable adaptive polymer dispersed liquid crystal (PDLC) glazing // Solar Energy. 2020. V. 195. P. 185—193.
6. *Pozhidaev E. P., Kaznacheev A. V., Torgova S. I., Kesaev V. V., Barbashov V. A.* Polymer dispersed liquid crystals with electrically controlled light scattering in the visible and near-infrared ranges // Optical Materials Express. 2020. V. 10. № 12. P. 3030—3040.

Directions of ensuring the information security of military facilities from the leakage of speech information through technical channels formed by laser acoustic reconnaissance systems

I. S. Rekunkov, V. A. Shcherbakov
Military Academy of strategic Missile forces named after Peter Great, Balashikha, Moscow region, Russia

This article considers promising directions for ensuring the information security of military facilities from the leakage of speech information through technical channels formed by laser acoustic reconnaissance.

Keywords: information security, acousto-optic technical channel of information leakage, laser acoustic reconnaissance system.

Bibliography — 6 references. *Received November 28, 2022*

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26
DOI: 10.52190/2073-2600_2022_4_27
EDN: JYLMGW

Алгоритм ЭЦП со скрытой группой, основанный на вычислительной трудности двух независимых задач

А. Б. Левина, канд. физ.-мат. наук; *А. А. Молдовян*, д-р техн. наук;
Н. А. Молдовян, д-р техн. наук
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Санкт-Петербург, Россия

Рассмотрен вопрос повышения уровня безопасности алгебраических алгоритмов ЭЦП со скрытой группой за счет такого построения, при котором взлом алгоритма требует одновременного решения двух независимых вычислительно-трудных задач. Последними являются нахождение дискретного логарифма и решение системы из многих квадратных уравнений с многими неизвестными. Описан алгоритм, реализованный в рамках данного подхода.

Ключевые слова: информационная безопасность, постквантовая криптография, цифровая подпись, конечная ассоциативная алгебра, некоммутативная алгебра, циклическая группа, двухмерная цикличность.

Алгебраические алгоритмы со скрытой группой представляют значительный интерес как постквантовые двухключевые криптосхемы. Известны две разновидности алгоритмов данного типа: основанные на вычислительной трудности скрытой задачи дискретного логарифмирования (ЗДЛ) [1—3] и основанные на вычислительной трудности нахождения решения системы из многих квадратных уравнений с многими неизвестными [4—6]. Практическое применение алгоритмов электронной цифровой подписи (ЭЦП) предполагает их безопасность, под которой понимается выполнение следующих двух условий: обладание достаточно высокой стойкостью, под которой понимается высокое значение трудоемкости лучшего известного алгоритма подделки подписи и пренебрежимо малая вероятность появления в обозримом будущем прорывного алгоритма взлома. Количественно уровень безопасности в такой трактовке можно охарактеризовать векторным значением, включающем значение стойкости и указанную вероятность.

В частности, появление прорывного решения базовой вычислительно трудной задачи означает появление прорывного алгоритма взлома криптосхемы. Одним из подходов к повышению уровня безопасности криптосхем с открытым ключом является уменьшение вероятности появления прорывного алгоритма взлома за счет того, что криптсхема строится на базе двух независимых вычислительно-трудных задач. При этом построение конкретной криптосхемы выполняется таким образом, что ее взлом требует одновременного решения указанных двух задач. Этот подход к повышению безопасности криптосхем с открытым ключом реализован при построении алгоритмов открытого шифрования [7], коммутативного шифрования [8], ЭЦП [7], слепой ЭЦП [9—11], коллективной ЭЦП [7]. В перечисленных случаях парой базовых вычислительно-трудных задач являются ЗДЛ и задача факторизации.

В литературе неизвестны случаи использования пары базовых вычислительно-трудных задач, включающих задачу нахождения решения системы из многих квадратных с многими неизвестными. В настоящей статье впервые предлагается построение алгебраического алгоритма со скрытой группой, взлом которого требует одновременного решения последней задачи и ЗДЛ.

Некоммутативные алгебры как носители алгоритмов ЭЦП со скрытой группой

Реализация алгоритмов ЭЦП со скрытой группой предполагает использование конечных алгебраических структур, в которых может быть задано достаточно большое число коммутативных групп, как подмножеств таких структур. Этому требова-

Левина Алла Борисовна, доцент.
E-mail: alla_levina@mail.ru
Молдовян Александр Андреевич, профессор.
E-mail: maa1305@yandex.ru
Молдовян Николай Андреевич, профессор.
E-mail: nmold@mail.ru

Статья поступила в редакцию 14 октября 2022 г.

нию удовлетворяют конечные некоммутативные ассоциативные алгебры (КНАА) размерности $m \geq 4$, заданные над конечными простыми полями $GF(p)$, где характеристика p является достаточно большим простым числом [3], или над расширениями двоичного поля $GF(2)$ [12]. Элементами КНАА являются m-мерные векторы, координаты которых являются элементами конечного поля. Операция сложения в КНАА представляет собой стандартную операцию сложения векторов, а операция умножения, обладающая свойствами дистрибутивности, слева и справа задается с помощью таблиц умножения базисных векторов (ТУБВ) и операций сложения и умножения в конечном поле. Детальное описание операции умножения в КНАА представлено, например, в [13].

Примером КНАА, пригодной для использования в качестве алгебраического носителя алгоритмов ЭЦП со скрытой группой, является алгебра, заданная над простым конечным полем (например, с характеристикой вида $p = 2q + 1$ при простом значении q, имеющем большой размер [3]) по ТУБВ, представленной как табл. 1 [13].

Таблица 1

Частный вариант алгебры k-кватернионов [13]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_3$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_1$	$-\mathbf{e}_2$	$\mathbf{e}_3$	$-\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$-\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$-\lambda\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$

Исследование декомпозиции данной КНАА на коммутативные подалгебры, выполненное в работе [13], показало, что она содержит три типа коммутативных подалгебр, отличающихся значением порядка и строением их мультипликативной группы:

- алгебра с циклической мультипликативной группой порядка $\Omega_1 = p^2 - 1$;
- алгебра с мультипликативной группой порядка $\Omega_2 = (p-1)^2$, обладающей двухмерной цикличностью (группа с двумя образующими одинакового порядка, равного значению $p - 1$);
- алгебра с циклической мультипликативной группой порядка $\Omega_3 = p(p-1)$.

Число подалгебр первого η_1, второго η_2 и третьего η_3 типов равно

$$\eta_1 = \frac{p(p-1)}{2}; \quad \eta_2 = \frac{p(p+1)}{2}; \quad \eta_3 = p+1.$$

Эти формулы показывают, что КНАА, заданная по табл. 1, содержит не менее p коммутативных конечных групп каждого их трех возможных типов, т. е. она удовлетворяет базовому требованию, предъявляемому к алгебраическим носителям алгоритмов ЭЦП со скрытой группой. При этом наибольший интерес представляет задание скрытой группы, относящейся к мультипликативным группам первого и второго типов, поскольку число групп таких типов примерно равно квадрату значения p. В следующих разделах предполагается использование данной четырехмерной КНАА.

Генерация открытого ключа

Для генерации открытого ключа задается скрытая коммутативная группа, обладающая двухмерной цикличностью и задаваемая парой перестановочных секретных векторов **G** и **H** порядка q как базисом <**G**, **H**> этой группы. Для генерации базиса <**G**, **H**> можно использовать следующую процедуру.

1. Сгенерировать случайный обратимый вектор **R** и вычислить вектор $\mathbf{L} = \mathbf{R}^2$.

2. Если $\mathbf{L}^q = \mathbf{E}$, где **E** — вектор, являющийся глобальной двухсторонней единицей КНАА, используемой в качестве алгебраического носителя, и $\mathbf{L} \neq \lambda\mathbf{E}$ для всех значений $\lambda \in GF(p)$ (т. е. если **L** не является скалярным вектором), то перейти к шагу 3, иначе перейти к шагу 1.

3. Сгенерировать случайное значение $\alpha \in GF(p)$, отличное от нуля и единицы поля $GF(p)$, такое, что α^2 также не равно единице поля $GF(p)$.

4. Сгенерировать случайное целое число k $(0 < k < q)$.

5. Вычислить вектор $\mathbf{H} = \alpha^2\mathbf{L}^k$.

6. Выдать в качестве базиса <**G**, **H**> случайной группы с двухмерной цикличностью два вектора $\mathbf{G} = \mathbf{L}$ и **H**, порядок каждого из которых равен q.

Секретный ключ генерируется в виде набора четырехмерных векторов **A**, **B**, **D**, **G**, **H** и натуральных чисел x и w $(1 < x, w < q)$. В качестве векторов **A**, **B** и **D** генерируются случайные обратимые векторы, удовлетворяющие следующим условиям $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BD} \neq \mathbf{DB}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{DG} \neq \mathbf{GD}$.

Открытый ключ вычисляется в виде набора четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$ по следующим формулам

$$\mathbf{Y}_1 = \mathbf{AGB}, \ \mathbf{Z}_1 = \mathbf{DHA}^{-1}, \ \mathbf{Y}_2 = \mathbf{AG}^x\mathbf{B}, \ \mathbf{Z}_2 = \mathbf{DH}^w\mathbf{A}^{-1}. \quad (1)$$

Размер открытого ключа зависит от значения разрядности простого числа q. Для случая 160-битного значения q открытый ключ имеет размер ≈320 байт.

Генерация ЭЦП

Процедура генерации подписи в виде вектора **S** и чисел e и σ включает следующие шаги.

1. Сгенерировать случайные целые числа u и t, удовлетворяющие условиям $1 < u < q$ и $1 < t < q$, и вычислить вектор $\mathbf{R}_1 = \mathbf{A}\mathbf{G}^{u}\mathbf{H}^{t}\mathbf{A}^{-1}$.

2. Используя некоторую коллизионно-стойкую 320-битную хэш-функцию f_H, вычислить значение $e = e_1 \| e_2 = f_H(M \| \mathbf{R}_1)$, где M — подписываемый электронный документ и хэш-значение e представлено как конкатенация двух 160-битных чисел e_1 и e_2.

3. Вычислить целочисленные значения n и d по следующим двум формулам:

$$n = \frac{u - e_1 - xe_2}{e_1 + e_2} \bmod q, \tag{2}$$

$$d = \frac{t - e_1 - we_2}{e_1 + e_2} \bmod q\,. \tag{3}$$

4. Вычислить четырехмерный вектор **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{D}^{-1}. \tag{4}$$

5. Сгенерировать случайные целые числа u' и t', удовлетворяющие условиям $1 < u' < q$ и $1 < t' < q$, и вычислить вектор $\mathbf{R}_2 = \mathbf{A}\mathbf{G}^{u'}\mathbf{H}^{t'}\mathbf{A}^{-1}$.

6. Вычислить 160-битное значение $\varepsilon = (f_H(M \| \mathbf{R}_2) \bmod q)$.

7. Решить следующую систему из двух линейных сравнений относительно неизвестных σ_1 и σ_2:

$$\begin{cases} (\varepsilon + \varepsilon n)\sigma_1 + (x + n)\sigma_2 = u' \bmod q; \\ (\varepsilon + \varepsilon d)\sigma_1 + (w + d)\sigma_2 = t' \bmod q. \end{cases}$$

Цифровой подписью является вектор **S** и пять 160-битных значений e_1, e_2, ε, σ_1 и σ_2. Общий размер ЭЦП равен ≈180 байт. Вычислительная трудоемкость процедуры генерации ЭЦП определяется шестью операциями экспоненцирования четырехмерных векторов и может быть оценена как ≈23000 операций умножения в поле $GF(p)$.

Верификация ЭЦП

Процедура проверки подлинности ЭЦП описывается следующим образом.

1. Вычислить четырехмерные векторы $\mathbf{R}'_1$ и $\mathbf{R}'_2$ по формулам

$$\mathbf{R}'_1 = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1}\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{e_2}, \tag{5}$$

$$\mathbf{R}'_2 = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{\varepsilon\sigma_1}\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{\sigma_2}. \tag{6}$$

2. Вычислить значения $e' = (e'_1 \| e'_2) = f_H(M \| \mathbf{R}'_1)$ и $\varepsilon' = (f_H(M \| \mathbf{R}'_2) \bmod q)$.

3. Сравнить значения e' и e и значения ε' и ε. Если $e' = e = (e_1 \| e_2)$ и $\varepsilon' = \varepsilon$, то ЭЦП признается подлинной, в противном случае ($e' \neq e$ или $\varepsilon' \neq \varepsilon$) ЭЦП отклоняется как ложная.

Вычислительная сложность процедуры верификации ЭЦП определяется четырьмя операциями экспоненцирования четырехмерных векторов и ее можно оценить как 15360 умножений в поле $GF(p)$.

Для доказательства корректности предложенной схемы ЭЦП предположим, что подпись ($\mathbf{S}$, e_1, e_2, ε, σ_1, σ_2) к документу M была сгенерирована в соответствии с процедурой, описанной в разделе выше. Покажем, что эта подпись проходит процедуру верификации как подлинная подпись.

Доказательство корректности схемы ЭЦП.

С учетом формул (1)—(6) и системы из двух линейных уравнений, решаемой на шаге 7 процедуры генерации ЭЦП, получаем:

$$\begin{aligned}
&\mathbf{R}'_1 = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1}\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{e_2} = \\
&= \left(\mathbf{A}\mathbf{G}\mathbf{B}\mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{D}^{-1}\mathbf{D}\mathbf{H}\mathbf{A}^{-1}\right)^{e_1} \times \\
&\times \left(\mathbf{A}\mathbf{G}^{x}\mathbf{B}\mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{D}^{-1}\mathbf{D}\mathbf{H}^{w}\mathbf{A}^{-1}\right)^{e_2} = \\
&= \left(\mathbf{A}\mathbf{G}^{n+1}\mathbf{H}^{d+1}\mathbf{A}^{-1}\right)^{e_1}\left(\mathbf{A}\mathbf{G}^{n+x}\mathbf{H}^{w+d}\mathbf{A}^{-1}\right)^{e_2} = \\
&= \mathbf{A}\mathbf{G}^{ne_1+e_1}\mathbf{H}^{de_1+e_1}\mathbf{A}^{-1}\left(\mathbf{A}\mathbf{G}^{e_2n+e_2x}\mathbf{H}^{e_2w+e_2d}\mathbf{A}^{-1}\right) = \\
&= \mathbf{A}\mathbf{G}^{n(e_1+e_2)+e_2x+e_1}\mathbf{H}^{d(e_1+e_2)+e_2w+e_1}\mathbf{A}^{-1} = \\
&= \mathbf{A}\mathbf{G}^{u}\mathbf{H}^{t}\mathbf{A}^{-1} = \mathbf{R}_1;
\end{aligned}$$

$$\begin{aligned}
&\mathbf{R}'_2 = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{\varepsilon\sigma_1}\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{\sigma_2} = \\
&= \left(\mathbf{A}\mathbf{G}\mathbf{B}\mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{D}^{-1}\mathbf{D}\mathbf{H}\mathbf{A}^{-1}\right)^{\varepsilon\sigma_1} \times \\
&\times \left(\mathbf{A}\mathbf{G}^{x}\mathbf{B}\mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{D}^{-1}\mathbf{D}\mathbf{H}^{w}\mathbf{A}^{-1}\right)^{\sigma_2} = \\
&= \left(\mathbf{A}\mathbf{G}^{n+1}\mathbf{H}^{d+1}\mathbf{A}^{-1}\right)^{\varepsilon\sigma_1}\left(\mathbf{A}\mathbf{G}^{n+x}\mathbf{H}^{d+w}\mathbf{A}^{-1}\right)^{\sigma_2} = \\
&= \mathbf{A}\mathbf{G}^{(\varepsilon+\varepsilon n)\sigma_1}\mathbf{H}^{(d+1)\varepsilon\sigma_1}\mathbf{A}^{-1}\left(\mathbf{A}\mathbf{G}^{(n+x)\sigma_2}\mathbf{H}^{(d+w)\sigma_2}\mathbf{A}^{-1}\right) = \\
&= \mathbf{A}\mathbf{G}^{(\varepsilon+\varepsilon n)\sigma_1+(n+x)\sigma_2}\mathbf{H}^{(\varepsilon+\varepsilon d)\sigma_1+(w+d)\sigma_2}\mathbf{A}^{-1} = \\
&= \mathbf{A}\mathbf{G}^{u'}\mathbf{H}^{t'}\mathbf{A}^{-1} = \mathbf{R}_2.
\end{aligned}$$

$$\left\{\mathbf{R}'_1 = \mathbf{R}_1, \mathbf{R}'_2 = \mathbf{R}_2\right\} \Rightarrow \left\{e'_1 = e_1, e'_2 = e_2, \varepsilon' = \varepsilon\right\}.$$

Последние три равенства соответствуют выполнимости условий шага 3 процедуры верификации подписи, т. е. описанная схема ЭЦП работает корректно.

Обсуждение

Описанная выше схема подписи является кандидатом на практичную постквантовую криптосхему, поскольку она основана на вычислительной трудности решения систем многих квадратных уравнений с многими неизвестными — на задаче, для решения которой квантовый компьютер является неэффективным [14], и которая лежит в основе ряда известных постквантовых криптоалгоритмов [15, 16].

Система квадратных векторных уравнений, трудность решения которой лежит в основе описанного алгоритма ЭЦП, определяется формулами (1), связывающими секретные векторы **A**, **B**, **D**, **G**, **H**, $\mathbf{H}_w = \mathbf{H}^w$ и $\mathbf{G}_x = \mathbf{G}^x$ (являющимися неизвестными в рассматриваемой системе) с элементами открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$). Заметим, что вместо неизвестных векторов $\mathbf{H}_w$ и $\mathbf{G}_x$ можно было бы рассматривать неизвестные числовые значения x и w, однако в этом случае возникает система, включающая экспоненциальные уравнения с неизвестными основаниями при операции экспоненцирования, что предположительно приводит к более высокой вычислительной сложности процедуры нахождения решения.

Формулы (1) задают четыре квадратных векторных уравнения. С учетом того, что векторы **G**, **H**, $\mathbf{H}_w$ и $\mathbf{G}_x$ являются попарно перестановочными имеем еще три квадратных уравнения, задающих условие перестановочности вектора **G** с каждым из векторов **H**, $\mathbf{H}_w$ и $\mathbf{G}_x$. Последнее условие определяет также попарную перестановочность векторов **H**, $\mathbf{H}_w$ и $\mathbf{G}_x$ (см. утверждение 1 в [13]). Таким образом, имеем систему из 7 квадратных векторных уравнений с 7 неизвестными. Записывая каждое из этих векторных уравнений в скалярной форме, получаем систему из 28 квадратных уравнений в поле $GF(p)$ с 28 неизвестными, которыми являются координаты неизвестных векторов.

При появлении прорывных способов решения систем из многих квадратных уравнений с многими неизвестными станет возможным вычисление секретных векторов и формирование элементов подписи **S**, e_1, e_2 и ε (см. шаги 1–6 процедуры генерации ЭЦП). Однако вычисление элементов подписи σ_1 и σ_2, выполняемое как решение системы из двух линейных сравнений с двумя неизвестными x и w, входящими в качестве коэффициентов в указанные уравнения, требует знания значений x и w (см. шаг 7 процедуры генерации ЭЦП). Нахождение числовых значений x и w, удовлетворяющих уравнениям $\mathbf{H}_w = \mathbf{H}^w$ и $\mathbf{G}_x = \mathbf{G}^x$ при известных **H**, **G**, $\mathbf{H}_w$ и $\mathbf{G}_x$, представляет собой ЗДЛ.

Таким образом, взлом предложенного алгоритма ЭЦП со скрытой группой требует одновременного решения двух независимых вычислительно-трудных задач: нахождение решения системы из многих квадратных уравнений; нахождение решения ЗДЛ. При появлении прорывного алгоритма решения ЗДЛ предложенный алгоритм подписи остается постквантовым. При появлении прорывного алгоритма решения первой задачи он перестает быть постквантовым. Пока не появятся практически доступные многокубитные квантовые компьютеры, предложенный алгоритм ЭЦП представляет собой криптосхему, основанную на вычислительной трудности двух независимых задач.

Криптосхемы [7—11], основанные на трудности одновременного решения задачи факторизации и ЗДЛ, перестают быть безопасными с момента появления квантового компьютера на практике. Это показывает, что в постквантовом аспекте схемы подписи на основе ЗДЛ и задачи нахождения решения системы из многих квадратных уравнений являются более привлекательными для практического использования.

Заключение

Впервые предложен алгоритм ЭЦП, основанный на решении двух вычислительно-трудных задач, одной из которых является задача нахождения решения системы из многих квадратных уравнений с многими неизвестными. Использованный для этого способ построения схемы ЭЦП представляет интерес для поиска новых алгоритмов такого типа. При этом интересно найти способ реализации алгоритмов ЭЦП, в которых в качестве второй вычислительно-трудной задачи будет задана скрытая ЗДЛ (например, в виде, рассмотренном в работе [3]), что потенциально будет сохранять постквантовость алгоритма при появлении прорывного способа решения систем многих квадратных уравнений с многими неизвестными. Такой поиск представляет собой задачу самостоятельного исследования.

Работа выполнена частично в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0015).

Литература

1. *Молдовян Д. Н., Молдовян А. А., Костина А. А.* Постквантовая схема цифровой подписи с двойным маскированием операции экспоненциирования // Вопросы защиты информации. 2020. № 2. С. 41—48.
2. *Moldovyan D. N.* New Form of the Hidden Logarithm Problem and Its Algebraic Support // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2020. № 2(93). P. 3—10.
3. *Moldovyan D. N.* A practical digital signature scheme based on the hidden logarithm problem // Computer Science J. Moldova. 2021. V. 29. № 2(86). P. 206—226.
4. *Молдовян Д. Н.* Типовые проверочные уравнения в алгебраических алгоритмах ЭЦП со скрытой группой // Вопросы защиты информации. 2022. № 1. С. 31—37. DOI: 10.52190/2073-2600_2022_1_31
5. *Молдовян Д. Н., Молдовян А. А.* Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7—17. DOI: 10.21681/2311-3456-2022-2-7-17
6. *Курышева А. А., Костина А. А., Молдовян Н. А.* Алгебраические алгоритмы со скрытой группой над конечными полями характеристики два // Вопросы защиты информации. 2022. № 2. С. 13—20. DOI: 10.52190/2073-2600_2022_2_13
7. *Березин А. Н., Молдовян Н. А., Щербаков В. А.* Общий метод построения криптосхем, основанных на трудности одновременного решения задач факторизации и дискретного логарифмирования // Вопросы защиты информации. 2014. № 2. С. 3—11.
8. *Молдовян А. А., Березин А. Н., Рыжков А. В.* Коммутативные шифры на основе трудности одновременного решения задач факторизации и дискретного логарифмирования // Информационно-управляющие системы. 2014. № 4. С. 106—110.
9. *Minh N. H., Binh D. V., Giang N. T., Moldovyan N. A.* Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems // Applied Mathematical Sciences. 2012. V. 6. № 139. P. 6903—6910.
10. *Tahat N. M. F., Shatnawi S. M. A., Ismail E. S.* A New Partially Blind Signature Based on Factoring and Discrete Logarithms // J. Mathematics and Statistics. 2008. № 4(2). P. 124—129.
11. *Tahat N. M. F., Ismail E. S., Ahmad R. R.* A New Blind Signature Scheme Based On Factoring and Discrete Logarithms // International J. Cryptology Research. 2009. № 1(1). P. 1—9.
12. *Молдовян А. А., Молдовян Н. А.* Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58—68. DOI: 10.21681/2311-3456-2022-3-58-68
13. *Молдовян А. А., Молдовян Д. Н., Молдовян Н. А., Костина А. А.* Конечные кватернионоподобные алгебры как носители постквантовых алгоритмов ЭЦП // Вопросы защиты информации. 2022. № 2. С. 21—29. DOI: 10.52190/2073-2600_2022_2_21.
14. *Ding J., Petzoldt A.* Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. V. 15. № 4. P. 28—36.
15. *Shuaiting Q., Wenbao H., Yifa Li, Luyao J.* Construction of Extended Multivariate Public Key Cryptosystems // International J. Network Security. 2016. V. 18. № 1. P. 60—67.
16. *Ding J., Schmidt D.* Rainbow, a new multivariable polynomial signature scheme // In Conference on Applied Cryptography and Network Security — ACNS 2005. Springer Lecture Notes in Computer Science. 2005. V. 3531. P. 164—175.

Signature algorithm with a hidden group, based on computational complexity of two independent problems

A. B. Levina, A. A. Moldovyan, N. A. Moldovyan
St. Petersburg Electrotechnical Univeristy "LETI", St. Petersburg, Russia

The issue of increasing the security level of algebraic digital signature algorithms with a hidden group is considered. The applied method is connected with the design due to which breaking the signature algorithm requires the simultaneous solving two independent computationally difficult problems. The latter are finding the discrete logarithm and solving a system of many quadratic equations with many unknowns. An algorithm implemented within the framework of this approach is described.

Keywords: information security, post-quantum cryptography, digital signature, finite associative algebra, non-commutative algebra, cyclic group, two-dimensional cyclicity.

Bibliography — 16 references. *Received October 14, 2022*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004
DOI: 10.52190/2073-2600_2022_4_32
EDN: KBGWDS

Обеспечение информационной безопасности в интеллектуальных системах среды умного города

В. В. Кабаков
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

В современном мире актуализируется создание умных городов, функционирующих на интеллектуальных технологиях Интернета вещей. Рассмотрен вопрос обеспечения информационной безопасности интеллектуальных технологий. Основной целью представленной статьи является исследование средств и методов защиты информации в интеллектуальных системах среды умного города. В результате работы используются научные материалы зарубежного и отечественного авторства, а также применяются теоретические методы исследования.

Ключевые слова: информационная безопасность, умный город, защита информации, интеллектуальная система, Интернет вещей.

В рамках технологического прогресса особую актуальность получает развитие различного рода цифровых и информационных технологий (ИТ). Именно посредством данных технологий на сегодняшний день достигается и обеспечивается высокая эффективность и рациональность использования ресурсов предприятия, а также разрабатываются инновационные решения, не только используемые в профессиональной сфере жизнедеятельности человека, но и в бытовой. Таким образом, в современном мире прослеживается достаточно интенсивная динамика интеграции цифровых технологий в повседневной жизни людей, которые, в свою очередь, позволяют автоматизировать те или иные процессы, а также упростить жизнь человека в целом. Современные разработки из сферы ИТ позволяют экономить время, трудовые ресурсы и выполнять рутинные задачи без использования человеческих рук.

Таким образом, одной из наиболее актуальных и инновационных сфер из области разработки информационных технологий является Интернет вещей (IoT). Концепция Интернета вещей строится на основе сети передачи данных, посредством которой люди получают возможность общаться с техническими устройствами, а технические устройства с людьми. Данная технология получает интенсивное развитие, а также имеет колоссальные результаты и богатый опыт практического использования. Практически в каждой квартире можно встретить умные вещи, активно используемые в повседневной жизни.

Основной проблемой при создании среды умного города является обеспечение информационной безопасности. Это обуславливается тем, что в рамках среды такого города практически все процессы выполняются на основе использования информационных систем и технологий. Передача данных, сбор показателей в квартирах, общение, обмен конфиденциальной информацией и иное – все это обуславливает интеграцию эффективных решений информационной безопасности. Целью представленной работы — обоснование актуальности вопроса обеспечения информационной безопасности в рамках среды умного города, а также анализ и систематизация ключевых средств и методов защиты информации для использования при решении данных задач [1].

Объектом исследования является среда умного города. Предметом исследования является вопрос информационной безопасности среды умного города.

Кабаков Виталий Валериевич, старший преподаватель.
E-mail: ser-kvv73@mail.ru

Статья поступила в редакцию 11 июля 2022 г.

Методы

Автором использованы теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных изучены научные работы отечественных и зарубежных авторов [1—6]. В каждой из данных работ затрагиваются фундаментальные вопросы, необходимые для проведения общего анализа, касающегося информационной безопасности среды умного города.

Раскрываются такие вопросы, как: угрозы для информационной безопасности в высокоорганизованных системах типа умный город; влияние информатизации городского пространства на обеспечение общественной безопасности; проблемы кибербезопасности умных городов и другие.

Актуализация концепции развития умного города на базе интеллектуальных средств

Умный город является одной из ключевых частей цифровизации экономики. Концепция умного города состоит из множества подсистем, огромного множества интегрированных электронно-вычислительных машин, контроллеров и датчиков, посредством которых происходит управление городской средой, начиная с его имущества и заканчивая обеспечением энергетического снабжения в целях экономии энергоресурсов.

Инфраструктура умного города со стороны цифрового обеспечения является очень сложной системой, которая, как уже было отмечено, состоит из множества средств информационных технологий. Каждое из данных устройств в результате своей работы порождает огромное количество данных, которые требуется собирать, анализировать и обменивать между информационными системами. Для корректной работы умного города требуется, в первую очередь, дорогая инфраструктура, а также понимание того, какие именно задачи и в какой очередности их решать [2].

Необходимо отметить, что первоначальным шагом создания умного города является сбор новых и более эффективных данных. Благодаря этим данным предоставляется возможность использования аналитических методов, включая методы предиктивной аналитики, позволяющей решать проблемы до их возникновения. Данная задача имеет достаточно сложный характер, исходя из чего помощь городам в сборе и обработке данных является одним из основных направлений, выполняемых посредством интеллектуальных систем. Источниками данных в системе умного города являются всевозможные датчики, данные о продаже в магазинах и компаниях, статистика покупок билетов на транспорт, данные о потреблении услуг жилищно-коммунального хозяйства, отчеты муниципальных служб и многое другое.

Основная особенность концепции умного дома заключается во вбирании в себя возникшую ранее концепцию умного дома. В концепции умного дома реализовывается функция включения и выключения света, домашней сигнализации или же кондиционера с помощью смартфона или по заранее установленному режиму. Посредством умных вещей человек получает возможность настройки работы холодильника, климатических систем, кофеварки и иной бытовой техники. Так, например, человек с помощью Интернета вещей имеет возможность заранее установить время варки кофе и увеличить этим самым количество утреннего сна. Также посредством IoT пользователь может настроить через телефонное приложение отопление в своем автотранспортном средстве для того, чтобы автомобиль успел прогреться, а человек сел в теплый салон, не испытывая дискомфорта от холода. Это только единичные примеры использования Интернета вещей в бытовых вопросах, которые доказывают высокую актуальность и перспективность его использования.

Проблемы информационной безопасности в среде умного города

Актуальным становится вопрос использования технологии искусственного интеллекта и машинного обучения при своем использовании в умном городе. Интернет вещей предоставляет множество методов воздействия со стороны злоумышленника, который может использовать слабые стороны цифровых устройств и перехватывать конфиденциальную информацию, применяя её для собственной выгоды. При разработке новых интеллектуальных устройств остается проблема обеспечения конфиденциальности, целостности и доступности данных. Именно это и является основным замедлителем широкого распространения Интернета вещей и повсеместного создания пространств умного города [3].

Есть необходимость пересмотреть принципы обеспечения защиты информации и разрабатывать новые с учетом появления новейших цифровых устройств, используемых в рамках городской среды.

На рис. 1 представлены основные требования, предъявляемые к информационной безопасности Интернета вещей.

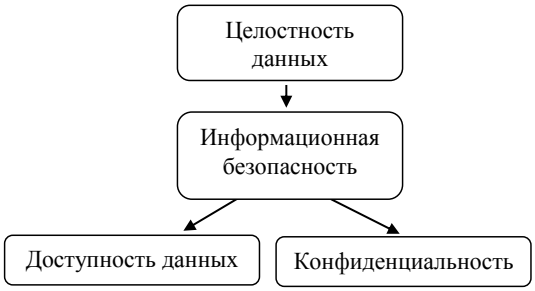


Рис. 1. Требования к информационной безопасности устройств Интернета вещей

При этом актуализация вопроса доступности данных происходит ввиду смены перечня угроз. В рамках умного города для датчиков, сенсоров и иных устройств необходима доступность. Это является следствием того, что доступность данных обеспечивает возможность их своевременного использования при решении различных задач. Обеспечение должного уровня информационной безопасности должно рассматриваться в каждом из создаваемых проектов Интернета вещей в целях защиты экосистемы. Для этого необходимо четко понимать методы и средства обеспечения защиты данных, наряду с механизмами безопасности на различных уровнях разработки и интеграции умных устройств [4].

Способы и средства обеспечения информационной безопасности в рамках умной городской среды

С помощью информации, непрерывно обрабатываемой и передающейся в различных информационных системах и сетях умного города, происходит обмен конфиденциальными данными, производятся транзакции на различных предприятиях, а также выполняется работа с засекреченной информацией и данными ограниченного доступа. Ввиду этого, формируется и актуализируется проблема, связанная с обеспечением безопасности работы с информационными ресурсами. Таким образом, вопрос информационной безопасности – это одно из ключевых и приоритетных направлений становления современного технологического прогресса. Для решения данной задачи существует ряд способов и средств защиты информации в различных информационно-коммуникационных системах и сетях. На рис. 2 представлены основные способы защиты информации.

Именно способы защиты информации формируют кластер развития средств защиты информации, используемых в современных системах умного города. Современные средства защиты информации можно разделить на ряд основных направлений развития. Основные средства защиты информации указаны на рис. 3.

Рис. 2. Способы обеспечения безопасности информационных систем умного города

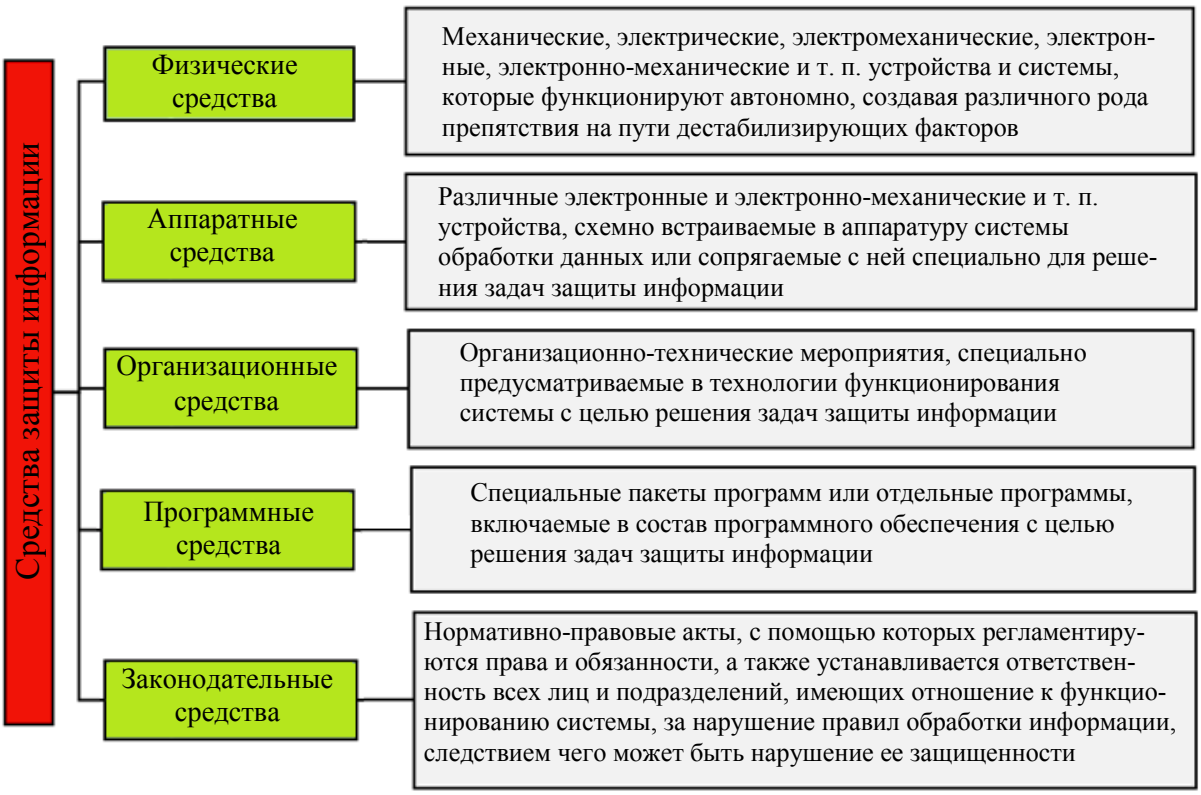


Рис. 3. Средства защиты информации систем Интернета вещей

Помимо этого, умные города должны постоянно иметь актуальную информацию, касающуюся о передовых методах и инструментах, которые используются хакерами по всему миру. Именно на основе данной информации может своевременно обновляться программное обеспечение на более подходящие варианты прошивки, обеспечивающие должный уровень защиты информации. Также для обеспечения максимальной эффективности цифровой безопасности умного города требуется акцентировать внимание на использование технологии интеллектуального обнаружения потенциальных угроз. Другим направлением интеллектуальной защиты информации является прогностическая аналитика. Аналитические системы, используемые сейчас для предотвращения утечки данных, могут быть изменены и использованы в дальнейшем с целью поиска слабых мест в инфраструктуре системы безопасности. Другим направлением развития данного вопроса является необходимость правового регулирования вопросов, связанных с обеспечением информационной безопасности системы умного города [5].

Заключение

Таким образом, основной целью представленной статьи являлось исследование средств и методов защиты информации в интеллектуальных системах среды умного города. В рамках представленной работы были проанализированы и систематизирована информация по таким вопросам, как: актуализация развития среды умного города и использования цифровых инструментов; используемые на сегодняшний день программные и аппаратные решения для защиты информации в системе умного города; необходимость разработки инновационных средств и методов обеспечения информационной безопасности в рамках среды умного города.

Автор отмечает, что в результате развития Интернета вещей вопросы обеспечения информационной безопасности представляют наиболее высокую значимость для сети умного города. Количество вредоносного программного обеспечения, используемого для нарушения работы умных городов, растет ежегодно. Исходя из этого, актуализируется вопрос разработки единых стандартов для обеспечения безопасности и улучшения механизмов защиты [6].

Литература

1. *Курчеева Г. И., Денисов В. В.* Угрозы для информационной безопасности в высокоорганизованных системах типа «Умный город» // Интернет-журнал науковедение. 2016. Т 8. № 3 (34). С. 45.

2. *Тарасенко А. А., Болтенкова Ю. В.* Влияние информатизации городского пространства на обеспечение общественной безопасности // Вестник белгородского юридического института МВД России им. И. Д. Путилина. 2020. № 4. С. 48—53.

3. *Промыслов В. Г., Семенков К. В., Жарко Е. Ф.* Методы оценки информационной угрозы для беспилотных транспортных средств в среде «Умного города» // Проблемы управления. 2020. № 3. С. 49—58.

4. *Аблязов Т. Х., Асаул В. В., Вишнивецкая А. И.* Формирование комфортной среды жизни человека на основе концепции "Программируемого" города // Московский экономический журнал. 2020. № 8. С. 15.

5. *Головенчик Г. А., Краско Г. В., Головенчик М. Г.* Проблемы кибербезопасности умных городов // Наука и инновации. 2020. № 1(214). С. 51—57.

6. *Наралиев Н. А., Самаль Д. И.* Обзор и анализ стандартов и протоколов в области Интернет вещей. Современные методы тестирования и проблемы информационной безопасности IOT // International Journal of Open Information Technologies. 2019. Т. 7. № 8. С. 94—104.

Ensuring information security in intelligent systems of the smart city environment

V. V. Kabakov
Moscow Aviation Institute (National Research University), Moscow, Russia

In the modern world, the creation of smart cities functioning on the intelligent technologies of the Internet of Things is becoming relevant. The main issues of the research area is the provision of information security. The main purpose of the presented article is to study tools and methods of information protection in intelligent systems of the smart city environment. Because of the work, scientific materials of foreign and domestic authorship are used, as well as theoretical research methods are applied.

Keywords: information security, smart city, information protection, intelligent system, Internet of things.

Bibliography — 6 references. *Received October 5, 2022*

УДК 004
DOI: 10.52190/2073-2600_2022_4_37
EDN: KIDAHU

Актуальность проведения исследований в области создания новых способов поиска уязвимостей с применением отечественных высокотехнологичных вычислительных платформ

П. В. Коренев
ПАО «Институт электронных управляющих машин имени И. С. Брука», Москва, Россия

В. А. Пиков, А. Г. Вилесов
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Статья посвящена актуальным вопросам поиска уязвимостей в информационных системах различного предназначения. Детально рассмотрены понятия аудит информационной безопасности, уязвимости, а также используемые способы их поиска. Выполнен анализ нормативных правовых актов по тематике проводимого исследования: аудит информационной безопасности, уязвимости, классификация уязвимостей информационных систем. Сформулированы недостатки известных способов поиска уязвимостей в информационных системах. Выполнен аналитический обзор известных методов оценивания эффективности систем защиты информации. На основании полученных результатов исследования сделаны выводы о том, что существует потребность в дальнейшей работе по созданию новых способов поиска уязвимостей с применением отечественных высокотехнологичных вычислительных платформ, что позволит учесть особенности проводимого в Российской Федерации импортозамещения и влияния санкций иностранных государств.

Ключевые слова: информация, защита информации, информационная безопасность, уязвимость, способы поиска уязвимостей, безопасное программное обеспечение, доверенные платформы, отечественная вычислительная платформа «Эльбрус».

Одной из основных задач бизнеса является защита особого вида информации, позволяющей сохранить предприятию занимаемое положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, называемой коммерческой тайной. Для нашего государства задача защиты особого вида информации — государственной тайны является одной из самых высокоприоритетных. Защита конфиденциальной информации всегда будет являться актуальной задачей, решаемой за счёт построения эффективной системы защиты информации, представляющей собой комплекс организационно-технических мер. Перечень актуальных угроз безопасности конфиденциальной информации, представленный, например, в базе данных угроз Федеральной службы по техническому и экспортному контролю (далее — ФСТЭК России), практически ежемесячно пополняется. Ежедневно поступают отчёты о выявленных уязвимостях программных продуктов и программно-аппаратных платформ. Благодаря этому система защиты информации организации является «живым» организмом, требующим постоянной модернизации для соответствия реалиям. Можно сделать вывод о том, что в стадию эксплуатации жизненного цикла системы защиты информации должен быть заложен механизм её актуализации, включая изменение состава и параметров функционирования используемых средств защиты информации. Одним из действующих способов, позволяющим понять потребность в изменении системы защиты информации, является аудит информационной безопасности. Нельзя забывать и о начальном этапе функционирования системы и процедуре аттестации, предшествующей вводу её в строй. По определению, «аттестация информационных систем — это большой комплекс организационно-технических мероприятий, в результате которых подтверждается соответствие информационных систем предприятия (как единой системы) требованиям стандартов или иных нормативно-технических

Коренев Павел Валерьевич, научный сотрудник.
E-mail: ineum@ineum.ru
Пиков Виталий Александрович, старший преподаватель.
E-mail: pikov@ya.ru
Вилесов Анатолий Григорьевич, ассистент кафедры.
E-mail: dshavelkin@inbox.ru

Статья поступила в редакцию 30 ноября 2022 г.

документов по обеспечению безопасности информации».

Итак, аудит защищённости информационных систем предприятия — это серьёзный системный процесс получения объективных качественных и количественных оценок уровня текущего состояния безопасности информации в соответствии с определёнными критериями и показателями. Множество способов проведения аудита, реализованных в виде инструментов аудита – программных продуктов, реализующих технологии, методики и, конечно, способы аудита информационной безопасности, можно считать неотъемлемой частью деятельности специалиста по информационной безопасности в организации.

Безопасность защищаемых информационных ресурсов информационных систем предприятия определяют их отдельными свойствами, которые описываются показателями, значения которых имеют либо конкретную величину, либо находятся в определенных интервалах (критерии безопасности информации). Можно сделать вывод о том, что в зависимости от значения этих показателей можно устанавливать разные уровни безопасности информации, её защищённости для конкретных условий эксплуатации информационных систем организации.

На этом этапе подведём некоторые итоги и сделаем выводы, от которых зависит ход дальнейшего исследования: безопасность, как состояние защищаемых информационных ресурсов информационных систем организации определяется её свойствами для конкретных условий существования в определенный момент времени; уровень безопасности защищаемых информационных ресурсов информационных систем предприятия определяется значениями или интервалами значений показателей, характеризирующих соответствующие их свойства.

Материалы и методы

Обеспечение безопасности защищаемых информационных ресурсов информационных систем предприятия осуществляют путем проведения комплекса мероприятий. Одна группа мероприятий направлена на изменение свойств самой информации ограниченного распространения (доступа) в соответствии с изменившимися условиями его существования и определяется как уровень её защиты, а другая — против осуществляемых источником угроз воздействий или на изменение свойств источника угроз, и определяется как противодействие.

Соответственно, понятие защищенности защищаемых информационных ресурсов информационных систем предприятия, её безопасности — не только качественное, но и количественное, так как мы можем говорить о так называемых "уровнях защищенности", которые, в первую очередь, должны определяться ценностью содержащейся в информационных ресурсах информации.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности. Также это процесс, обеспечивающий состояние информационной безопасности.

Информационная безопасность — это состояние защищённости информационной среды. Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации ограниченного распространения, несанкционированных и непреднамеренных воздействий на неё, т. е. процесс, направленный на достижение этого состояния.

В настоящее время нет сложившегося и чёткого определения аудита, сформулированного в нормативных правовых актах, применяемого для анализа уровня информационной безопасности. В различных источниках у различных авторов можно встретить разные определения. Приведем некоторые из них.

Аудит — это форма независимого, нейтрального контроля какого-либо направления деятельности организации [1].

Аудит — это совокупность специальных приемов (методов), используемых при обработке исходной информации для достижения поставленных целей [1].

Многообразные приемы аудита проверок обычно объединяют в четыре группы: определение реального состояния объектов, анализ, оценка, формирование технических предложений [2].

Аудит — это систематический, независимый и документированный процесс получения записей, фиксирования фактов или другой соответствующей информации и их объективного оценивания в целях установления степени выполнения заданных требований [3].

Аудит информационных систем — это проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам с последующей оценкой рисков сбоев в их функционировании [4].

Аудит информационной безопасности — это мероприятия по оценке состояния информационной

безопасности информационной автоматизированной системы и разработки рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных ресурсов информационной системы от угроз информационной безопасности [1].

Аудит информационной безопасности — это системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности [4].

Аудит информационной безопасности — это комплекс организационно-технических мероприятий, проводимых независимыми экспертами, имеющих цель оценить состояние информационной безопасности объекта аудита и степень его соответствия критериям аудита [5].

Наиболее общим и в максимальной степени отражающим процесс проведения аудита, а также гармонизирующим ISO 19011-2011 «Руководящие указания по аудиту систем менеджмента», является следующее определение:

Аудит информационной безопасности — это систематический, независимый и документируемый процесс получения оценок состояния информационной безопасности объекта аудита и объективного их оценивания в целях установления степени соответствия критериям аудита [6].

Анализируя данные определения, можно сделать вывод об общей и о частных задачах аудита информационной безопасности.

Общей задачей аудита информационной безопасности является проверка и оценивание информационной системы на соответствие критериям, которые определяют требования, предъявляемые к уровню безопасности информации.

Частными задачами аудита информационной безопасности являются: анализ рисков, связанных с возможностью реализации угроз безопасности информации; оценка текущего уровня защищенности информационной системы; выявление уязвимостей в подсистеме защиты и «узких мест» информационной системы; оценка соответствия информационной системы и ее защиты существующим стандартам в области информационной безопасности, а также политике безопасности; формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты информации [1, 5].

Цели аудита можно подразделить на [5]: превентивные — цели, направленные на превентивное выявление угроз и уязвимостей и предотвращение инцидентов информационной безопасности; детектирующие — цели, направленные на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты информации во время или после инцидентов информационной безопасности; корректирующие — цели, направленные на формирование комплекса мер повышения эффективности существующей системы защиты информации после инцидентов информационной безопасности с учетом вновь выявленных угроз и уязвимостей [1, 5].

В настоящее время аудит информационной безопасности проводят по отношению к следующим объектам: организации; бизнес-процессы; системы управления (менеджмента); информационные системы; технические системы [3].

По форме аудит информационной безопасности может быть: организационно-нормативным — когда анализируют организационные мероприятия обеспечения информационной безопасности и нормативные акты в данной сфере; техническим — когда анализируют технические средства и способы обеспечения информационной безопасности [3].

Аудит информационной безопасности объекта аудита является наиболее общей формой оценки его состояния. Аудит информационной безопасности проводят на соответствие любым требованиям, сформулированным как заинтересованными лицами, так и нормативными документами. Аудит может включать в себя проведение различных способов тестирования подсистем и процессов объекта аудита, анализ документации и других информационных источников, интервьюирование специалистов и т. д.

При проведении аудита информационной безопасности обычно соблюдается следующая последовательность мероприятий.

Первый этап – подготовительный: выбор объекта аудита информационной безопасности; выбор критериев и методов аудита информационной безопасности; выбор средств и способов аудита информационной безопасности; формирование команды аудиторов (специалистов, экспертов); определение объема и масштаба аудита информационной безопасности, установление его сроков [1, 2].

Второй этап – основной: анализ состояния информационной безопасности объекта аудита; регистрация, сбор и проверка статистических данных и результатов инструментальных измерений уязвимостей и угроз; оценка результатов проверки аудита информационной безопасности; формирование отчета о результатах проверки по отдельным элементам объекта аудита и различным аспектам информационной безопасности [1, 2].

Третий этап — заключительный: составление итогового отчета; формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты; разработка плана мероприятий на предприятии по устранению уязвимостей и недостатков в обеспечении требуемого уровня информационной безопасности [1, 2].

Исследуем уязвимости, как источник реализации угроз безопасности информации. В открытых источниках не выделено единой классификации уязвимостей, при этом попыток навести порядок в данной области можно найти много. Как правило, подразумевают одну из двух известных классификаций уязвимостей.

Первая классификация:

- уязвимости, возникшие на этапе проектирования;
- уязвимости, возникшие при реализации;
- уязвимости, допущенные в конфигурации.

Вторая классификация:

- некорректная обработка (проверка) входных данных системы;
- слабые механизмы аутентификации;
- недостаточно качественная проверка подлинности данных;
- ошибки в конфигурации программного обеспечения;
- некорректное использование методов криптографии;
- ошибки, допущенные в процессе управления учетными записями.

В соответствии с требованиями ГОСТ Р 56545–2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» установлена классификация уязвимостей, правила описания уязвимостей, содержание и порядок выполнения работ по выявлению и оценке уязвимостей информационных систем. В стандарте приняты правила описания уязвимостей, которые могут быть использованы специалистами по информационной безопасности при создании и ведении базы данных уязвимостей информационных систем, разработке средств контроля (анализа) защищенности информации, разработке моделей угроз безопасности информации и проектировании систем защиты информации, проведении работ по идентификации, выявлению уязвимостей, их анализу и устранению. Важно отметить, что «стандарт не распространяется на уязвимости информационных систем, связанные с утечкой информации по техническим каналам, в том числе уязвимостями электронных компонентов технических (аппаратных и аппаратно-программных) средств информационных систем» [7].

В сети Интернет в открытом доступе находятся многочисленные базы данных, которые содержат информацию о сотне тысяч найденных уязвимостях в программном обеспечении. Наиболее авторитетными среди специалистов в области информационной безопасности признаны базы данных уязвимостей: NVD (National Vulnerability Database), CVE (Common Vulnerabilities and Exposures), Oval (Open Vulnerability and Assessment Language).

Реализацией способов проведения аудита информационной безопасности и поиска уязвимостей являются сканеры уязвимостей – программы, программные комплексы, системы комплексного анализа защищённости, которые в той или иной мере используют указанные публичные базы данных уязвимостей информационных систем.

Выполним исследование понятия уязвимость и терминов, связанных с этим явлением. Приведём определения из международных стандартов в области информационной безопасности, а также с официального сайта ФСТЭК России. В соответствии ISO/IEC 27000:2014 «Уязвимость — это слабость актива или управления, эксплуатация которой приведёт к реализации одной или нескольких угроз» [8].

Базовый вектор [уязвимости] (Base vector [of vulnerability]) – текстовая формализованная запись (строка), представляющая собой комбинированные данные о базовых метриках (критериях) уязвимости, на основании которой определяется численная базовая оценка уязвимости [9].

Уровень опасности уязвимости – оценка опасности уязвимостей, определяемая на основе численного значения базовой оценки уязвимости. В банке данных в зависимости от значения базовой оценки уязвимости V используются следующие уровни опасности:

- низкий уровень, если $0{,}0 \le V \le 3{,}9$;
- средний уровень, если $4{,}0 \le V \le 6{,}9$;
- высокий уровень, если $7{,}0 \le V \le 9{,}9$;
- критический уровень, если $V = 10{,}0$ [9].

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использован для реализации угроз безопасности информации [7].

Уязвимость нулевого дня (Zero-day vulnerability) — уязвимость, которая становится известной до момента выпуска разработчиком программного обеспечения информационной системы мер защиты информации по ее устранению, исправлению ошибок или соответствующих обновлений [10; 7].

Уязвимость программного обеспечения — ошибка в программном обеспечении, способная

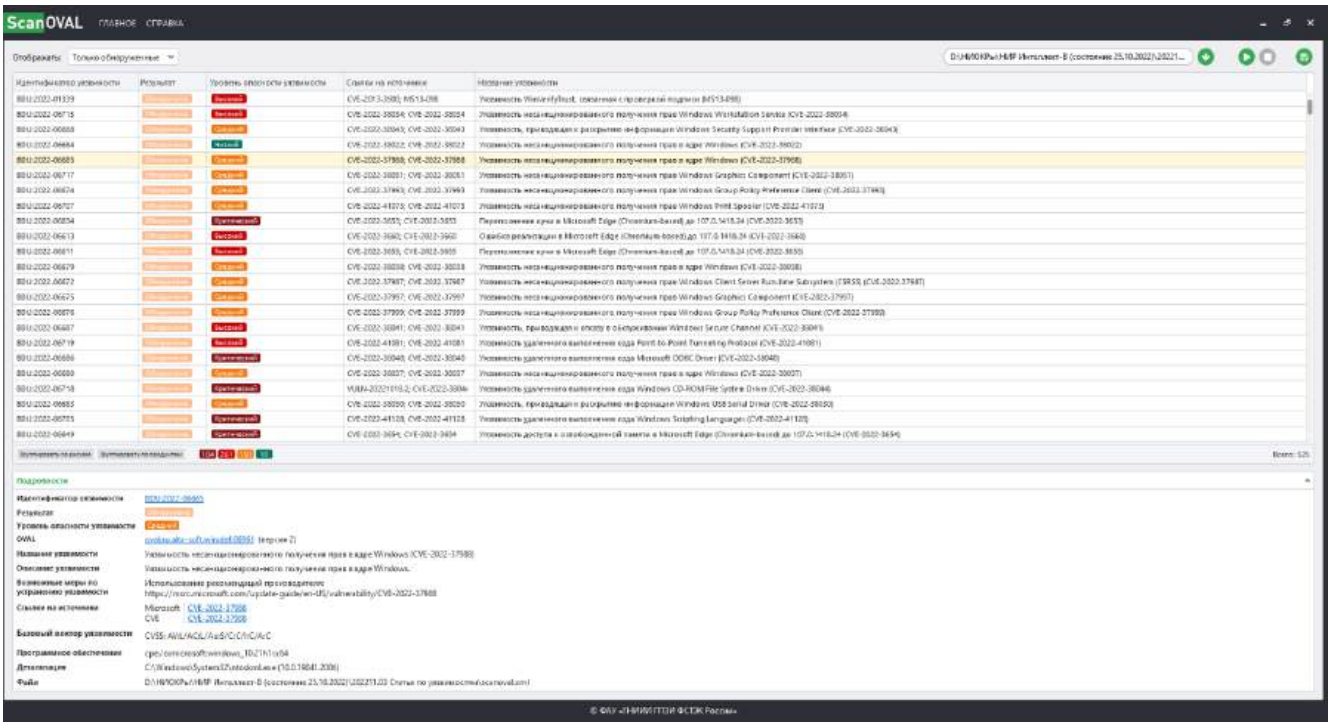
напрямую быть использована хакером для получения доступа к системе или сети [11].

Угроза — возможная причина нежелательного инцидента, которая может нанести ущерб [информационной] системе или всей организации [8].

Угроза безопасности информации (Information security threat) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [12].

Приведём мнение относительно программ-сканеров уязвимостей известного евангелиста в области обеспечения информационной безопасности, Алексея Лукацкого: «Сканирование уязвимостей — это, пожалуй, самый популярный метод оценки защищенности, который используется для повышения своей ситуационной осведомленности в отношении имеющихся уязвимостей приложений, системного программного обеспечения, сетевой инфраструктуры и т. п. Кроме того, подобная защитная мера является обязательной согласно требованиям ФСТЭК России и ЦБ России для государственных и муниципальных организаций, субъектов КИИ, финансовых организаций, владельцев АСУ ТП, операторов персональных данных и прочее. Важно отметить, что, будучи полностью автоматизированным, этот метод, к сожалению, имеет и существенные недостатки. Во-первых, он позволяет найти только известные уязвимости, заложенные производителем в свой сканер уязвимостей (а потому так важно регулярно обновлять его базу знаний). Во-вторых, работа сканера может повлечь за собой нарушение работоспособности отдельных компонентов инфраструктуры, не очень хорошо спроектированных или не способных выдержать массовую проверку уязвимостей и выходящих из строя (такое бывает с некоторыми элементами АСУ ТП). В-третьих, обычно сканеры безопасности выявляют атомарные, единичные уязвимости, не учитывая их взаимосвязи с другими, и цепочки уязвимостей, которые применяются хакерами в реальной жизни. Наконец, этот метод находит известные ему дыры в инфраструктуре, но не подтверждает возможность их использования, в отличие от пентестов или решений класса BAS. Запускаться такие решения могут как самой компанией, так и внешними подрядчиками. В ряде случаев последнее требуется законодательством, например, стандартом PCI DSS или положениями Банка России» [13].

В 2022 г. ФСТЭК России опубликовала на своём официальном сайте программу ScanOVAL, предназначенную для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующих под управлением операционных систем семейства Microsoft Windows и Linux (рисунок).



Главное окно программы «ScanOVAL», предназначенной для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах

В соответствии с ГОСТ Р 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» принята «классификация уязвимостей информационных систем исходя из области происхождения уязвимостей, типов недостатков информационных систем и мест возникновения (проявления) уязвимостей информационных систем [14].

В соответствии со стандартом в основе классификации уязвимостей информационных систем используются следующие классификационные признаки: область происхождения уязвимости; типы недостатков информационных систем; место возникновения (проявления) уязвимости информационных систем.

Важно отметить, что в качестве уязвимых компонентов информационной системы рассматриваются: общесистемное (общее), прикладное, специальное программное обеспечение, технические средства, сетевое (коммуникационное, телекоммуникационное) оборудование, средства защиты информации [14].

В соответствии с пунктом 5.1 стандарта уязвимости информационных систем по области происхождения подразделяются на следующие классы: уязвимости кода; уязвимости конфигурации; уязвимости архитектуры; организационные уязвимости; многофакторные уязвимости.

Согласно требованиям пункта 5.2 уязвимости информационных систем по типам недостатков информационных систем подразделяются на: недостатки, связанные с неправильной настройкой параметров программного обеспечения; недостатки, связанные с неполнотой проверки вводимых (входных) данных; недостатки, связанные с возможностью прослеживания пути доступа к каталогам; недостатки, связанные с возможностью перехода по ссылкам; недостатки, связанные с возможностью внедрения команд ОС; недостатки, связанные с межсайтовым скриптингом (выполнением сценариев); недостатки, связанные с внедрением интерпретируемых оператором языков программирования или разметки; недостатки, связанные с внедрением произвольного кода; недостатки, связанные с переполнением буфера памяти; недостатки, связанные с неконтролируемой форматной строкой; недостатки, связанные с вычислениями; недостатки, приводящие к утечке/раскрытию информации ограниченного доступа; недостатки, связанные с управлением полномочиями (учетными данными); недостатки, связанные с управлением разрешениями, привилегиями и доступом; недостатки, связанные с аутентификацией; недостатки, связанные с криптографическими преобразованиями (недостатки шифрования); недостатки, связанные с подменой межсайтовых запросов; недостатки, приводящие к "состоянию гонки"; недостатки, связанные с управлением ресурсами; иные типы недостатков [14].

В соответствии с пунктом 5.3 стандарта уязвимости информационных систем по месту возникновения (проявления) подразделяются на: уязвимости в общесистемном (общем) программном обеспечении; уязвимости в прикладном программном обеспечении; уязвимости в специальном программном обеспечении; уязвимости в технических средствах; уязвимости в портативных технических средствах; уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании; уязвимости в средствах защиты информации [14].

Результаты

Для достижения целей, связанных с предотвращением появления и/или устранением уязвимостей программ, принят государственный стандарт ГОСТ Р 56939–2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». Стандарт содержит перечень мер, которые рекомендуется реализовать на соответствующих этапах жизненного цикла программного обеспечения информационных систем различного назначения. Сертификации по требованиям стандарта в настоящий момент нет. Необходимость выполнения требований стандарта, например, может быть прописана в технических заданиях (тактико-технических заданиях) на создание (модернизацию) новых образцов вооружения и военной и специальной техники (для нужд Министерства обороны РФ), проверена на соответствие в ходе проведения испытаний.

Примером организации процедуры поиска уязвимостей в автоматизированных системах, созданных для силовых структур РФ, является тот факт, что в Вооруженных Силах РФ действует типовой регламент организации работ по устранению уязвимостей и выпуску обновлений безопасности программных средств (изделий) из состава комплексов средств автоматизации (автоматизированных систем военного назначения) (типовой регламент ВС РФ). Типовой регламент ВС РФ устанавливает порядок организации работ по устранению уязвимостей, внесению изменений в рабочую конструкторскую (эксплуатационную) документацию и информированию о выпуске обновлений безопасности программных средств (изделий) из состава комплексов средств автоматизации (автоматизированных систем военного назначения) [15].

Системы анализа и контроля защищенности предназначены для проверки информационной системы на наличие возможных уязвимостей и слабых мест сетевого периметра, инфраструктуры, на наличие ошибок в конфигурации, программных обеспечениях и программном коде приложений. Все это может стать потенциальным местом, через которое злоумышленник попытается получить несанкционированный доступ во внутреннюю сеть. Такие средства защиты информации, чаще называемые сканерами уязвимостей, обладают следующими функциями [16]: определение возможных путей проникновения злоумышленника; предоставление оценки эффективности применяемых мер защиты информационной сети; контроль за качеством внедрения программных и программно-аппаратных средств и систем защиты информации; предоставление оценки рисков и уязвимостей в созданной инфраструктуре созданной сети; проверка на наличие слабых мест в разрабатываемых приложениях; предоставление отчетов об общем уровне защищенности инфраструктуры информационной сети; проведение инвентаризаций и предоставление полного списка сервисов, протоколов, уязвимостей и возможных мест, через которые можно осуществить несанкционированный доступ [16].

В ходе проведения анализа сканеры уязвимостей проверяют на наличие уязвимостей сетевой периметр, внутренние сетевые устройства, беспроводную инфраструктуру, программное обеспечение, веб-приложения и т. д. При этом, как правило, существует два режима работы: статическое сканирование, при котором проводится пассивный анализ информационной сети, и динамическое сканирование, когда сканер уязвимостей имитирует действия злоумышленника и проводит атаки для проверки устойчивости системы и ее реакции.

Принцип работы систем анализа и контроля защищенности построен на последовательности следующих шагов:

- сбор данных об имеющейся инфраструктуре информационной системы;
- производится обнаружение потенциальных уязвимостей методом сканирования;
- подтверждается наличие найденных уязвимостей динамическими методами;
- создание отчётов о результатах проведенного анализа;
- автоматическое исправление найденных уязвимостей (при наличии такой функции).

С помощью средств защиты информации данного типа, так же называемых сканерами уязвимостей, возможно сканировать корпоративную сеть предприятия, проверяя узлы сети на устойчивость ко взлому. Такие сканеры сети могут помочь предотвратить DoS-атаки, атаку spoofing и некоторые другие. Ярким отечественным примером такого средства защиты информации является Сканер-ВС от компании «Эшелон» [16].

Для того чтобы провести оценивание эффективности систем защиты информации необходимо определиться с показателями, а также планируемыми к использованию методами или методиками.

Основными методами оценивания эффективности систем защиты информации можно назвать [6, 16]:

- статический метод характерен проведением обработки потенциальных угроз безопасности их последствий, показателем оценки будет возникновение угрозы определенного типа за период времени;
- вероятностный метод определяет вероятность отказа в работе системы от обработки информации при успешной реализации угрозы;
- частотный метод строится на основании анализа статистического материала, в котором рассчитывается значение показателя ожидаемого ущерба как функции показателей частоты возникновения угрозы и условного ущерба;
- экспертный метод помогает определить количество и перечень параметров, которые характеризуют СЗИ, показателем оценки важности в этом случае будет степень обеспечения безопасности системы;
- информационно-энтропийный метод подразумевает проведение аналитического вычисления информационной энтропии системы с использованием понятия свертки функции, а эффективной систему защиты информации считают при реализации линейной зависимости, показатель оценки – величина информационной энтропии Шеннона;
- нейросетевой (многокритериальный) метод оценки показывает принадлежность определенного уровня безопасности значению промежутка [0, 1], оценка эффективности проводится по четко выбранным показателям;
- метод минимизации рисков подразумевает последовательное проведение следующих действий: фиксации рисков, индексации риска, проведения классификации рисков, определения способа их обработки, расчёта показателей характеристик рисков и расчёта показателей экономического эффекта от управления этими рисками, а полученный на последнем шаге показатель экономического эффекта от управления рисками и будет служить показателем оценки эффективности;
- матричный (формальный) метод также подразумевает выполнение ряда шагов: определение параметров, составление трехмерной матрицы отношений, преобразование этой матрицы в двумерную

таблицу и определение качественных и количественных показателей значений показателей, показателями оценки эффективности могут служить параметры состояния системы защиты информации;

- многоуровневый метод описывает состояние системы защиты информации совокупностью уровней и набором категорий конфиденциальности;
- комбинаторный (оптимизационный) метод решает задачу оптимизации некой функции при заданных параметрах.

Можно выделить следующие достоинства и недостатки вышеперечисленных методов оценивания эффективности систем защиты информации (таблица) [16].

Достоинства и недостатки методов оценивания эффективности систем защиты информации

Метод оценки эффективности	Достоинства	Недостатки
Статистический	Возможность получения результатов в случаях отсутствия знаний о параметрах СЗИ; Оценка СЗИ любой сложности	Большие объемы статистических данных для обработки; Результаты считаются достоверными с определенной вероятностью
Вероятностный	Анализ полного спектра угроз; Рассмотрение взаимосвязей при реалистичном подходе	Сложные вычисления; Невозможность выявления плавности изменения вероятностных характеристик
Частотный	Удобное представление графических характеристик СЗИ	Большая статистическая выборка
Экспертный	Быстрое получение результатов; Отсутствует необходимость в статистических сведениях	Влияние человеческого фактора на результаты; Субъективность; Зависимость от квалификации специалиста ИБ
Информационно-энтропийный	Легкость оценки эффективности по присутствию линейной зависимости	Случайные события в процессе оценки не рассматриваются; Необходимость определения пороговых значений
Нейросетевой (многокритериальный)	Учет большого количества критериев оценки СЗИ, а также количественных и качественных показателей критериев оценки СЗИ; Неопределенности не мешают проведению оценки	Необходимость в больших вычислительных ресурсах; Выбор оптимальной структуры сложен
Минимизация рисков	Необходимость наличия полной и точной информации отсутствует; Простота использования	Зависимость от экспертной оценки рисков; Сложность самой оценки; Необходимость использования нескольких моделей оптимизации
Матричный (формальный) метод	Универсальность метода; Возможность проведения оценки оперативно; Требование в вычислительных мощностях минимально	Наличие неопределенности является препятствием для проведения оценки
Многоуровневый	Повышенная объективность и корректность; Возможна обработка нечеткой информации и качественных характеристик	Сложность вычисления и формирования уровней оценивания
Комбинаторный (оптимизационный)	Гибкость в применении к построениям; Наибольшая эффективность в оценке эффективности СЗИ	Сложность в вычислениях

Показатели оценки сформулированы в требованиях регулирующих документов, например, таких, как ГОСТ Р ИСО/МЭК 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», и будут определяться в ходе создания системы защиты информации информационной системы. Но при этом неправильный выбор показателей оценки может привести к ряду проблем, таким, как: недостаточное или излишнее количество показателей, часть показателей находится в сложных взаимосвязях, неверное определение весов количественных показателей. Это может привести к некачественной или неверной оценке эффективности систем защиты информации [17].

Обсуждение

Достижение необходимых масштабов и сроков обнаружения уязвимостей в средствах вычислительной техники автоматизированных систем различного назначения (в информационных системах предприятия) потребует создания инновационных программно-технических средств автоматизированного анализа средств вычислительной техники, например с использованием особенностей архитектуры отечественных высокотехнологичных вычислительных платформ.

Целью исследований в области создания новых способов поиска уязвимостей с применением отечественных высокотехнологичных вычислительных платформ является повышение степени автоматизации выявления уязвимостей в средствах вычислительной техники автоматизированных систем различного назначения (в информационных системах предприятия).

Для достижения цели должны быть решены следующие задачи:

- провести исследования российских и зарубежных средств поиска уязвимостей;
- провести исследования возможности применения для поиска уязвимостей новых способов, учитывающих особенности отечественных высокотехнологичных вычислительных платформ, например, с помощью двоичного транслятора системы «Lintel» на архитектуре «Эльбрус»;
- разработать макет программно-технического комплекса для демонстрации возможности поиска уязвимостей с применением отечественных высокотехнологичных вычислительных платформ.

Заключение

Используемый в автоматизированных системах различного назначения (в информационных системах предприятия) метод фаззинг-тестирования не позволяет проводить полный перебор параметров и настроек из-за высокой временной и вычислительной сложности, поэтому целесообразно проведение научных исследований перспективных методов для повышения эффективности и скорости поиска уязвимостей. Также следует учесть, что известные российские программные реализации известных способов поиска уязвимостей не всегда учитывают особенности импортозамещения и санкций иностранных государств при переходе на отечественные высокотехнологичные вычислительные платформы. Требуется проработка новых подходов к поиску уязвимостей.

Следовательно, следует провести исследование в области создания новых способов поиска уязвимостей с учётом импортозамещения и перехода на отечественные высокотехнологичные вычислительные платформы. На сайте компании АО «МЦСТ» представлено описание средства запуска операционных систем в машинных кодах x86 на компьютерах архитектуры «Эльбрус» — двоичный транслятор системы Lintel (ТВГИ.00509-01): «Компонент системы двоичной трансляции, известный как Lintel, позволяет запустить на компьютере архитектуры «Эльбрус» операционную систему в машинных кодах x86 или x86-64, например, Microsoft Windows или Red Hat Enterprise Linux, без перекомпиляции из исходных текстов. Трансляция проходит в режиме реального времени, «на лету», с адаптивной многопроходной оптимизацией, что в сочетании с аппаратными средствами поддержки трансляции, заложенными в архитектуру «Эльбрус» и обеспечивающими низкие накладные расходы, даёт высокую скорость работы гостевых сис-тем. В отличие от транслятора приложений транслятор уровня системы создаёт наиболее полное подобие имитируемого x86-компьютера» [18].

Можно сделать вывод об актуальности исследования по проверке гипотезы о том, что разработка нового способа поиска уязвимостей в программе, написанной для Microsoft Windows, реализуемого за счёт запуска её на платформе «Эльбрус» с применением двоичного транслятора системы Lintel, обеспечит выявление уязвимостей незамеченных ранее другими методами.

Литература

1. *Аверичников В. И., Рытов М. Ю., Кувылкин А. В., Рудановский М. В.* Аудит информационной безопасности органов исполнительной власти: учебн. пособие. — М.: Флинта, 2011. — 100 с.

2. *Кульба В. В., Шелков А. Б., Гладков Ю. М., Павельев С .В.* Мониторинг и аудит информационной безопасности автоматизированных систем. — М.: ИПУ им. В. А. Трапезникова РАН, 2009. — 94 с.

3. *Марков А. С., Цирлов В. Л., Барабанов А. В.* Методы оценки несоответствия средств защиты информации / под ред. А. С. Маркова. — М.: Радио и связь, 2012. — 192 с.

4. *Хомяков В. А.* Аудит как метод модернизации системы обеспечения информационной безопасности // Экономический вестник Ярославского университета. 2013. № 29. С. 48—52.

5. *Астахов А.* Курс по аудиту информационной безопасности [Доклад] // GlobalTrust Solutions [Электронный ресурс]. 2008. URL: https://www.studmed.ru/astahov-aleksandr-vvedenie-v-audit-informacionnoy-bezopasnosti_f7c82aa80af.html (дата обращения: 18.11.2022).

6. ISO 19011:2011 Руководящие указания по аудиту систем менеджмента : Междун. стандарт / подгот. Техн. комитетом ISO/TC 176 "Менеджмент качества и обеспечение качества", подкомитет ПК 3 "Поддерживающие технологии".

7. ГОСТ Р 56545–2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей : нац. стандарт Рос. Федерации : утв. и введ. Приказом Федер. агентства по техн. регулированию и метрологии от 19 августа 2015 г. № 1180-ст : введ. впервые: дата введ. 2016-04-01 / разраб. ООО «Центр безопасности информации». — М.: Стандартинформ, 2015.

8. SO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary : Междун. стандарт / подгот. Объединённым техн. комитетом ISO/IEC JTC 1, Информационные технологии, Подкомитетом SC 27, Методы обеспечения безопасности в ИТ.

9. Список терминов БДУ ФСТЭК России [Электронный ресурс] URL: https://bdu.fstec.ru/ubi/terms/terms/view/id/5 (дата обращения: 18.11.2022).

10. ФСТЭК России: методический документ от 11.02.2014 «Меры защиты информации в государственных информационных системах».

11. CWE (Common Weakness Enumeration) — общий перечень дефектов (недостатков) безопасности [Электронный ресурс] URL: http://cwe.mitre.org (дата обращения: 18.11.2022).

12. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения : нац. стандарт Рос. Федерации : утв. и введ. Приказом Федер. агентства по техн. регулированию и метрологии от 18 декабря 2008 г. N 532-ст : введ. впервые: дата введ. 2009-10-01/ разраб. ФГУ "ГНИИИ ПТЗИ ФСТЭК России", ООО "НПФ "Кристалл". — М.: Стандартинформ, 2013.

13. *Лукацкий А.* Журнал IT Manager. [Электронный ресурс] URL: https://www.it-world.ru/cionews/security/188623.html (дата обращения: 18.11.2022).

14. ГОСТ Р 56546–2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем : нац. стандарт Рос. Федерации : утв. и введ. Приказом Федер. агентства по техн. регулированию и метрологии от 19 августа 2015 г. № 1181-ст : введ. впервые: дата введ. 2016-04-01 / разраб. ООО «Центр безопасности информации». — М.: Стандартинформ, 2015.

15. Типовой регламент организации работ по устранению уязвимостей и выпуску обновлений безопасности программных средств (изделий) из состава комплексов средств автоматизации (автоматизированных систем военного назначения), 2018.

16. *Стулова Е. В.* Разработка комплекса мер для повышения результативности систем защиты информации с применением комплексного средства анализа защищенности «Сканер-ВС», 2022.

17. *Миняев А. А.* Методика оценки эффективности системы защиты территориально-распределенных информационных систем [Текст] // А. А. Миняев. – СПб.: СПбГУТ, 2021. 216 с.

18. Двоичный транслятор системы «Lintel» (ТВГИ.00509-01) [Электронный ресурс] URL: http://www.mcst.ru/lintel (дата обращения: 18.11.2022).

The relevance of research in the field of creating new ways to search for vulnerabilities using Russian high-tech computing platforms

P. V. Korenev
PJSC "Institute of Electronic Control Machines named after I. S. Bruk", Moscow, Russia

V. A. Pikov, A. G. Vilesov
Moscow Aviation Institute (National Research University), Moscow, Russia

The article is devoted to topical issues of searching for vulnerabilities in information systems for various purposes. The concepts of information security audit, vulnerability, as well as currently used methods for their search are considered in detail. The analysis of regulatory legal acts about the ongoing research was carried out: audit of information security, vulnerabilities, classification of vulnerabilities of information systems. The shortcomings of known methods for searching for vulnerabilities in information systems are formulated. An analytical review of known methods for evaluating the effectiveness of information security systems has been carried out. Based on the results of the study, it was concluded that there is a need for further work to create new ways to search for vulnerabilities using domestic high-tech computing platforms, which will consider the peculiarities of the import substitution carried out in the Russian Federation and the impact of foreign sanctions.

Keywords: information, information security, information protection, vulnerability, ways to search for vulnerabilities, secure software, trusted platforms, domestic computing platform «Elbrus».

Bibliography — 18 references. *Received November 30, 2022*

УДК 004
DOI: 10.52190/2073-2600_2022_4_47
EDN: KJHWAN

К вопросу об организации беспроводной связи посредством модуляции светового потока

С. Е. Кондаков, канд. техн. наук
ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», Москва, Россия

Д. А. Тимонов
ФГБОУ ВО «Кубанский государственный технологический университет», г. Краснодар, Россия

Проведен анализ возможности создания канала беспроводной связи с использованием средств модуляции видимого света создаваемого светодиодами.

Ключевые слова: информация, модуляция видимого света, беспроводная связь, светодиод.

Одним из аспектов оборудования выделенных помещений, предназначенных для ведения конфиденциальных переговоров, является изоляция их от внешних воздействий, в том числе и посредством использования жалюзи или плотных штор на окнах помещения. Поэтому для обеспечения освещенности выделенных помещений приобретение в качестве осветительных приборов светильников построенных на основе сверхъярких светодиодах (мощностью от 1 Вт и более), является оправданным. Необходимо отметить тот факт, что в состав большей части техники, используемой для обработки информации, также входят светодиоды разной мощности.

Особенность использования светодиодов связана, в первую очередь, с качественным питанием, одной из характеристик которого является мерцание (пульсация). Мерцание – это мигания высокой частоты, создаваемые осветительным прибором. Человеческий глаз практически не воспринимает эти колебания, но мозг реагирует на мерцание лампы при частоте до 300 Гц. Оперируя частотой мерцания выше 300 Гц, а в некоторых случаях можно и меньше, т. к. большая часть мониторов, построенных на светодиодах, работает на более низкой частоте, можно передавать информацию незаметно для глаза. При этом необходимо отметить, что многие светодиоды могут быть не только передатчиками, но и приемниками [1].

Передача информация посредством модуляции видимого света известна с 2011 г. и подробно описана профессором Хаар, который ввел понятие Li-Fi [2, 3]. Сеть передачи данных на этой основе модуляции видимого света получила название Visible Light Communication (VLC) и является альтернативным методом связи, обладающим высокой пропускной способностью и невосприимчивостью к помехам от электромагнитных источников [4—7].

Системы связи, построенные на технологии VLC, используют видимый свет для связи, который занимает спектр от 380 нм до 750 нм, соответствующий частотному спектру от 430 ТГц до 790 ТГц.

Приемник VLC принимает сигналы только в том случае, если он находится в прямой видимости в пределах комнаты. Приемников и передатчиков может быть несколько, в таких случаях применяется неортогональная схема множественного доступа (NOMA)[8]. Схема множественного доступа позволяет одновременно осуществлять прием через один фотодиод (приемник) от разных источников света, что увеличивает количество абонентов.

Рассматривая приемник в технологии VLC, необходимо уделить особое внимание существующей элементной базе. В качестве фотоприемников могут выступать как фотодиоды, фоторезисторы, так и обычные светодиоды. Однако надо учитывать, что фотоприемник должен уметь принимать сигнал с частотой передатчика, а также учитывать другие источники окружающего света, которые могут вносить дополнительный шум в канале.

Кондаков Сергей Евгеньевич, доцент кафедры «Защита информации».
E-mail: sergeikondakov@list.ru
Тимонов Дмитрий Александрович, ассистент кафедры «Компьютерные технологии и информационная безопасность».
E-mail: dmitrii-timonov@bk.ru

Статья поступила в редакцию 30 ноября 2022 г.

Наиболее часто встречающимися источниками окружающего света являются светодиодные, вольфрамовые и люминесцентные лампы. Их относительные спектральные плотности мощности показаны на рисунке.

Как правило, существует высокий уровень стационарного или медленнофлуктуирующего окружающего света, создающего дробовой шум в фотодиоде. Кроме того, источники искусственного света также излучают быстроизменяющиеся компоненты, связанные с высшими гармониками сетевой частоты. Они могут быть устранены с помощью электрической фильтрации. Часть падающего окружающего света можно блокировать оптическим фильтром. Можно использовать фильтр оптических помех с полосой пропускания, соответствующей полосе пропускания источника светодиода (с учетом ненормального падения). Из-за различий в спектрах источников фильтр может блокировать окружающий свет с разной степенью эффективности. Пропускание составляет примерно 2 % при 650 нм и 75 % при длине волны светодиода 470 нм.

Уровень освещенности приемника необходимой для надежной передачи, в значительной степени определяет мощность оптического сигнала.

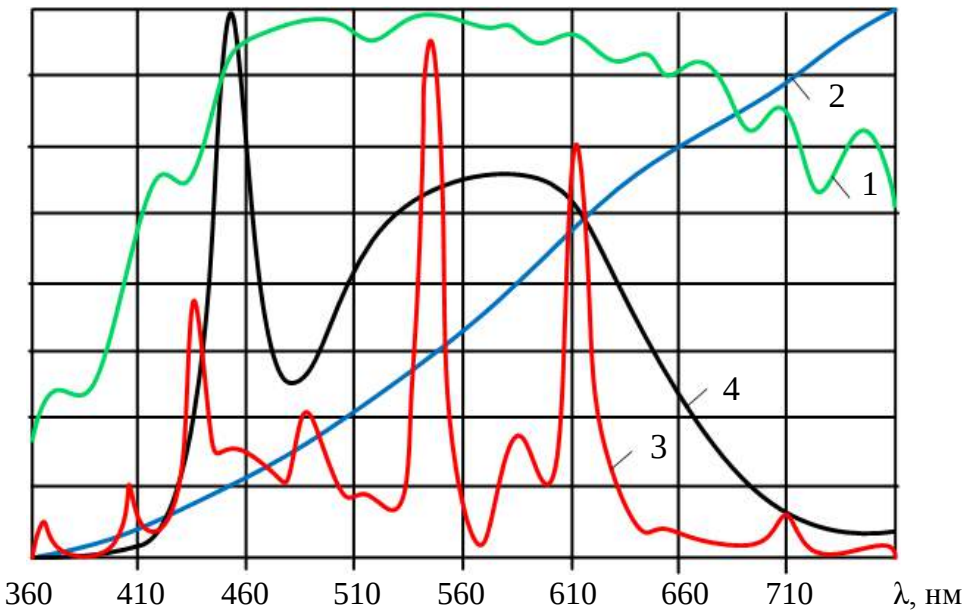
Распределение выходной мощности излучения (характеристики излучения) моделируется обобщенным законом Ламберта:

$$dP_n = \frac{n+1}{2\pi}(\cos\alpha)^n \, P_s \, d\Omega, \qquad (1)$$

где $P_s = \oint dP_n$.

Здесь P_s представляет собой полную мощность, излучаемую светодиодом, dP_n — мощность, излучаемую в телесный угол $d\Omega$, n — число, описывающее форму характеристик излучения, а α — полярный угол.

При этом надо отметить, что приемник, расположенный на приемном устройстве, должен быть компактным и недорогим, не требовать трудоемкой настройки и должен хорошо освещаться от источников передачи информации и обладать большим углом обзора и большой апертурой, чтобы обеспечить высокую пропускную способность нисходящего потока. Необходимо отметить, что увеличение активной области фотоприемника сопровождается уменьшением ширины его полосы пропускания и расфокусировкой светового луча в отношении угла и площади. Таким образом, произведение апертуры на телесный угол уменьшать нельзя. Для увеличения апертуры приемника можно использовать линзы или оптику, такую как концентрирующее составное параболическое зеркало, используемое для концентрации солнечной энергии.



Оптические спектры естественных и искусственных источников света:
1 – Солнце, 2 – лампа накаливания, 3 – флуоресцентная лампа, 4 – светодиод белого света.

Для сохранения широкой полосы пропускания можно использовать массив быстродействующих фотоприемников, совмещенных с отдельными электрическими предусилителями и каскадом суммирования [9]. Также имеет место вариант, когда функция сбора света отделяется от функции детектирования светового потока, что позволяет провести оптимизацию каждой функции отдельно. Широкий поверхностно-решетчатый соединитель (SGC), собирающий падающий свет, интегрированный с волноводом, ведущим к быстродействующему фотодиоду, способен поддерживать прием в формате бинарной модуляции (on/off keying или OOK) со скоростью в несколько гигабитов в секунду. Массив SGC позволяет еще больше увеличить апертуру без ущерба для пропускной способности. Такой вариант построения приемника может значительно увеличить дальность и скорость передачи информации. Одним из вариантов построения системы VLC является требование к производителям мобильных и бытовых устройств встраивать более чувствительные фотоприемники, которые были бы способны воспринимать информацию по средствам модуляции видимого света, создаваемого светодиодами.

Для хорошей передачи информации необходимо учитывать требования к помещениям, в которых будет предусмотрена передача информации по средствам модуляции видимого света, создаваемого светодиодами. Помещения не должны быть сложными, а должны быть хорошо освещены световыми приборами, а стены, пол и потолок обладать отражающими свойствами. В силу особенности расположения осветительных приборов обычно на потолке помещений при отсутствии специальных или художественных рассеивателей основной световой поток направлен на пол помещения. Однако при реальном проектировании системы передачи информации влияние средств модуляции видимого света, создаваемого светодиодами, необходимо учитывать.

Приемники и передатчики можно встраивать в настольные лампы, информационные настенные панели (телевизоры) стационарные персональные компьютеры, подсветки пола и рабочих зон. Для организации связи за пределами помещения можно использовать как встроенный фотоприемник (часть фотоприемника — апертуру) в потолок или стену, связанный с передатчиком, находящийся за пределами помещения. В случае размещения апертуры целесообразно ее совместить с вентиляцией. Однако более эффективно передавать информацию за пределы помещения, используя другие средства передачи, например, такие как, Wi-Fi.

Передача зависит от эффективного рассеяния падающего излучения светодиода от окружающих поверхностей, образующих структурную среду помещения. Здесь коэффициент отражения ρ_0 определяется как отношение полной мощности, отраженной в полусферу, к падающему излучению плоской волны.

В соответствии с ГОСТ Р 55710–2013 коэффициенты отражения окружающих поверхностей определены в диапазонах:

- от 0,7 до 0,9 — для потолков;
- от 0,5 до 0,8 — для стен;
- от 0,2 до 0,7 — для рабочих поверхностей;
- от 0,2 до 0,4 — для пола.

Характеристики отражения состоят из диффузной и зеркальной составляющих, причем последняя становится существенной для очень малых углов падающего излучения.

Таким образом, авторами показана принципиальная возможность построения в помещении беспроводной связи с использованием только модуляции светового потока. Выделены основные особенности при организации связи с использованием модуляции видимого света между устройствами, и определены требования к передатчику и приемнику, а также к помещению, в котором организуется передача информации.

Литература

1. *[Электронный ресурс] URL: https://usilitelstabo.ru/*ispolzovanie-svetodioda-v-kachestve-fotopriemnika.html?ysclid=law6zt772d791117591.

2.[Электронный ресурс] URL: http://purelifi.com/what_is_lifi/the-lifi-story/.

3. *Sarkar A., Agarwal S., Nath A.* Li-Fi technology: data transmission through visible light // Int. J. Adv. Res. Comput. Sci. Manag. Stud. 2015. Vol. 3. № 6. P. 1–10.

4. *Wang Y., Chi N., Wang Y., Tao L., Shi J.* Network architecture of a high-speed visible light communication local area network // IEEE Photonics Technol. Lett. 2015. Vol. 27. № 2. P. 197–200.

5. [Электронный ресурс] URL: https://mentor.ieee.org/802.15/dcn/08/15-08-0171-00-0vlc-10mbps-visible-light-transmission-system.pdf.

6. *Schmid S., Corbellini G., Mangold S., Gross T. R.* LED-to-LED visible light communication networks // Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing. 2013. P. 1–10. DOI: https://doi.org/10.1145/2491288.2491293.

7. *Ley-Bosch C., Alonso-González I., Sánchez-Rodríguez D., Ramírez-Casañas C.* Evaluation of the eff ects of hidden node problems in IEEE 802.15. 7 uplink performance, Sensors 16 (2). 2016.

8. *Marshoud H., Kapinas V. M., Karagiannidis G. K. , Muhaidat S.* Non-orthogonal multiple access for visible light communications // IEEE Photon Technol Lett. 2015. Vol. 28. № 1. P. 51–54. DOI: 10.1109/LPT.2015.2479600.

9. *Khalid A. M., Koonen A. M. J., Oh C. W. et al.* 10 Gbps indoor optical wireless communication employing 2D passive beam steering based on arrayed waveguide gratings IEEE Photonics Society Summer Topical Meeting Series (SUM), 2016. P. 134—135.

On the issue of organizing wireless communication using modulation of the light flux

S. E. Kondakov
Bauman Moscow State Technical University, Moscow, Russia

D. A. Timonov
Kuban State Technological University, Krasnodar, Russia

The article analyzes the possibility of creating a wireless communication channel using means of modulating visible light generated by LEDs.

Keywords: information, visible light modulation, wireless communication, LED.

Bibliography — 9 references. *Received November 30, 2022*

Правила для авторов по оформлению рукописей статей, предлагаемых к публикации в журналах

Направляя рукопись статьи в редакцию журнала, авторы передают редколлегии и издателю журнала безвозмездное неисключительное право опубликовать ее на русском языке в качестве статьи в печатной и электронной версиях журнала в сети Интернет. При этом за авторами сохраняются их интеллектуальные права на рукопись статьи (в том числе "авторское право"). В связи с этим и с учетом Четвертой части (Раздел VII) Гражданского кодекса РФ авторами должно быть представлено в редакцию письмо в следующей форме:

Лицензионный договор о передаче права на публикацию
(издательский лицензионный договор)

Мы, нижеподписавшиеся, авторы рукописи ……..……., предоставляем редколлегии журнала и журнала и издателю ФГУП «НТЦ оборонного комплекса «Компас» ……..……
(название журнала)
безвозмездную простую (неисключительную) лицензию на публикацию рукописи статьи как в печатной, так и в электронной версиях журнала.

Мы подтверждаем, что данная публикация не нарушает интеллектуальных прав других лиц или организаций.

Подписи авторов: …… (ф.и.о., ученая степень, дата)
……..…….
……...…….

Статья должна быть подписана всеми авторами. В случае нескольких авторов указывается фамилия автора, ответственного за переписку с редакцией. Рукопись статьи направляется на адрес редакции журнала: 125424, Москва, Волоколамское ш., д. 77, ФГУП «НТЦ оборонного комплекса «Компас», Редакция журнала. Дополнительная информация может быть получена в редакции при обращении по телефону: 8 (495) 491-43-17 или по E-mail: izdanie@ntckompas.ru.

Каждая статья рецензируется в соответствии с решением редколлегии журнала. Рецензенты выбираются из числа ученых и специалистов, компетентных в вопросах, рассматриваемых в статье, и имеющих собственные публикации в данном направлении. Решение о порядке публикации статьи принимается редколлегией с учетом мнения рецензентов. В случае разногласий среди членов редколлегии окончательное решение принимает главный редактор. При полном отклонении рукописи статьи от публикации редакция журнала направляет авторам мотивированный отказ. По этому факту редакция не вступает в полемику с авторами.

Комплектование статьи (обзора)

Статья должна быть представлена в редакцию в следующем комплекте:

- сопроводительное письмо, подписанное руководством организации;
- экспертное заключение о возможности опубликования в открытой печати и распространения в Российской Федерации и других государствах. При отсутствии в организации экспертной комиссии вместо экспертного заключения может быть представлено соответствующее заявление на имя главного редактора журнала от имени руководства организации, где работают авторы. В экспертном заключении или заявлении в обязательном порядке должна быть отражена возможность открытой публикации и передачи публикуемых материалов за границу.
- лицензионный договор по приведенному образцу;
- рукопись статьи — объем статьи (без рисунков) не должен превышать 10 страниц формата А4 при 1,5 межстрочных интервалах, а объем статьи обзорного характера — 20 страниц. Рекомендуемая гарнитура — New Times Roman. Размер шрифта — 12;
- Материал статьи представляется в редакцию в печатном виде (на бумажном носителе) и в электронном варианте с текстом в формате Word на электронную почту.

Оформление статьи:

- статья начинается с указания УДК;
- название статьи набирается строчными буквами (кроме начальной прописной) полужирным шрифтом, размер шрифта 14, для остального текста используется простой шрифт размером 12, причем рекомендуемая гарнитура шрифта — Times New Roman;
- после названия — список авторов, инициалы авторов предшествуют их фамилиям;

- далее представляется аннотация статьи (10—15 строк с раскрытием цели работы и её основных результатов);
- далее приводится список ключевых слов для данной статьи (не более десяти);
- страницы текста нумеруются без пропусков и добавлений литерных обозначений (типа 1*а*, 2*б* и т. п.), причем в сквозную нумерацию должны быть включены все элементы статьи;
- внизу первой страницы текста помещается отдельный абзац (с полужирным шрифтом), содержащий контактную информацию об авторе (или авторах) в следующем виде: фамилия, имя, отчество, должность, ученая степень, почтовый адрес предприятия, телефон, E-mail;
- основной текст статьи должен начинаться с четкой постановкой цели и задач работы, сопровождаемой аргументами в пользу ее выполнения на фоне существующего состояния затронутой в статье проблемы. Дальнейший текст статьи также должен иметь смысловые рубрикаторы (разделы и подразделы) без их нумерации. Заканчиваться статья должна отдельным разделом «Заключение» с перечислением основных результатов, следующих из них выводов и, по возможности, предложений по развитию исследований и использованию их результатов.
- после основного текста — список использованных источников "Литература" (не менее 5 источников); Список использованной литературы должен соответствовать всем ссылкам на внешние источники в тексте статьи. Ссылки оформляются в квадратных скобках, например, [1—6], [7, 8]. Внутренние ссылки, т. е. ссылки на формулы, рисунки и таблицы статьи оформляются с использованием круглых скобок, например, формула (1), уравнение (4), (рис. 3), (табл. 2). Любые ссылки в подписях к рисункам и в самих рисунках не рекомендуются;
- далее размещается подробная англоязычная информация о статье: название статьи, фамилия и инициалы авторов (английская транслитерация), предприятие, аннотация, ключевые слова (Keywords).

Оформление рисунков:

- рисунки и графики вставляются непосредственно в нужном месте в статье и в желаемом масштабе.
- рядом с осями графиков указываются отображаемые физические величины только в символьной (буквенной) форме, а через запятую — размерность величины по-русски (прямым шрифтом). Различные кривые на графиках рекомендуется нумеровать, даже если они характеризуются отдельным цветом или типом линии. Графики представляются только на белом фоне. Вспомогательные сетки на площади графика не допускаются;
- подписи под соответствующими рисунками (полужирный курсивный) представляются в нужных местах текста. Каждая подпись должна быть по возможности лаконичной, но емкой по содержанию.

Оформление формул:

- простые формулы вводить в текст в формате используемого текстового редактора, более сложные формулы — с использованием редактора формул MathType;
- стандартные математические обозначения (например, max, log, sin, exp и т. д.) должны быть набраны прямо. То же относится к цифрам и числам;
- для символьного обозначения невекторных физических (технических) величин использовать только латинский и греческий алфавиты, при этом в тексте для греческих букв использовать прямой шрифт, для латинских букв — наклонный шрифт (курсив);
- векторы и матрицы обозначать полужирным прямым шрифтом;
- для нижних и верхних индексов применять арабские цифры, латинские или греческие буквы. Если индекс представляет собой сокращенную форму русского слова — характеристики, то допустимо использовать в его обозначении русские буквы (прямой шрифт), например $U_{вх}$, $I_{вых}$, $\nu_{гр}$ и т. п.
- размерность физических величин обозначается всегда только по-русски прямым шрифтом.

Оформление таблицы:

- содержание таблицы не должно дублировать данные, приводимые на графиках или в тексте;
- графы должны иметь название без сокращения отдельных слов.

Рисунки, формулы и таблицы должны иметь свою отдельную сквозную нумерацию. Если на конкретную формулу нет дополнительных (возвратных) ссылок в тексте или она в единственном числе, то нумерация ее не нужна. Единственные таблица и/или рисунок также не нумеруются.

При публикации в журнале каждая статья (в контактной информации) сопровождается сноской со знаком охраны авторского права ©, поставленным перед фамилией автора (фамилиями авторов) и годом издания.

Авторы (или автор) каждой статьи после выхода журнала в свет имеют право на получение от редакции электронной версии статьи в PDF-формате (редактор Adobe Acrobat).