Даниил А. Похачевский
Московский физико-технический институт
(национальный исследовательский университет),
Институтский пер., 9, Долгопрудный, Московская область, 141701, Россия
e-mail: daniek9898@gmail.com, https://orcid.org/0000-0001-7403-0307

АНАЛИЗ УЯЗВИМОСТЕЙ, ВОЗНИКАЮЩИХ ПРИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ ACTIVE DIRECTORY

DOI: http://dx.doi.org/10.26583/bit.2020.4.02

Аннотация. В статье представлены результаты анализа и синтеза научно-технической литературы, нормативных актов, стандартов в области обеспечения информационной безопасности информационных систем (ИС), использующих сторонние сервисы аутентификации пользователей. Вводится контекст рассматриваемой ИС. Описываются уязвимости, возникающие при аутентификации пользователей с использованием службы каталогов Active Directory. На основе функциональных особенностей клиентского приложения, входящего в ИС, проводится построение концептуальной модели угроз информационной безопасности ИС, которая применяется для выявления и исследования возможных атак на процесс аутентификации пользователей. В результате выявления критических мест безопасности системы, формируются основные требования, соблюдение которых позволит повысить состояние защищенности систем, а именно: необходимость обеспечения подлинности и целостности ЭВМ, принимающих участие в процессе аутентификации пользователей в приложении, необходимость обеспечения конфиденциальности передаваемых и хранимых аутентифицирующих данных пользователей. Результаты данной работы позволяют обезопасить процесс аутентификации с использованием технологии Active Directory, а также проводить дальнейшие исследования в области аутентификации пользователей в распределенных системах. Проведенный анализ позволяет сделать вывод о безопасности применения предложенного способа аутентификации при соблюдении выявленных требований.
Ключевые слова: служба каталогов, Active Directory, аутентификация, модель угроз, объектно-ориентированный подход, требования безопасности.
Для цитирования: ПОХАЧЕВСКИЙ, Даниил А. АНАЛИЗ УЯЗВИМОСТЕЙ, ВОЗНИКАЮЩИХ ПРИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ ACTIVE DIRECTORY. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 17–24, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1302>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.02.

Daniil A. Pokhachevskiy
Moscow Institute of Physics and Technology (National Research University),
Institutskiy per., 9, Dolgoprudny, Moscow region, 141701, Russia
e-mail: daniek9898@gmail.com, https://orcid.org/0000-0001-7403-0307

Analysis vulnerabilities of user authentication process using Active Directory

DOI: http://dx.doi.org/10.26583/bit.2020.4.02

Abstract. The paper presents the results of the analysis and synthesis of scientific and technical literature, regulations, standards in the field of information security of information systems (IS), using third-party user authentication services. The context of the considered IS is introduced. Vulnerabilities in user authentication using the Active Directory service are described. Based on the functional features of the client application included in the IS, a conceptual model of threats to the information security of the IS is built. This model is used to identify and investigate possible attacks on the user authentication process. As a result of identifying critical points of system security, the main requirements are formed, the observance of which will improve the state of security of systems, namely: the need to ensure the authenticity and integrity of computers participating in the process of authenticating users in the application, the need to

ensure the confidentiality of transmitted and stored user authenticating data. The results of this work make it possible to secure the authentication process using Active Directory technology, as well as to carry out further research in the field of user authentication in distributed systems. The analysis performed allows us to conclude that the proposed authentication method is safe if the identified requirements are met.
Keywords: directory service, Active Directory, user authentication, threat model, object-oriented approach, safety requirements.
For citation: POKHACHEVSKIY, Daniil A. Analysis vulnerabilities of user authentication process using Active Directory. IT Security (Russia), [S.l.], v. 27, n. 4, p. 17–24, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1302>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.02.

Введение

Процесс аутентификации заключается в проверке принадлежности предъявленного идентификатора субъекту [1 с. 241].

В данный момент популярным явлением является аутентификация пользователей информационных систем выполняется с помощью сторонних сервисов, поэтому введение в научный оборот анализа уязвимостей, возникающих при аутентификации пользователей с использованием Active Directory, будет полезным.

Объектом анализа является процесс аутентификации пользователей с использованием службы каталогов технологии Active Directory.

Объект защиты рассматривается как часть следующей информационной системы (рис. 1). Клиентское приложение, в котором есть подсистема аутентификации, исполняется на некоторой ЭВМ, находящейся в одном сегменте вычислительной сети с контроллером домена. Рассматриваемая подсистема аутентификации входит в состав клиентского приложения. Возможности пользователей использовать определенную функциональность приложения зависят от результатов авторизации пользователей. Active Directory развернута на контроллере домена. Служба каталогов предоставляет интерфейс прикладного уровня сетевой модели OSI для взаимодействия с хранилищем Active Directory по протоколу LDAP. Клиентское приложение использует этот интерфейс для обращения к базе данных пользователей, хранящейся в LDAP-хранилище.

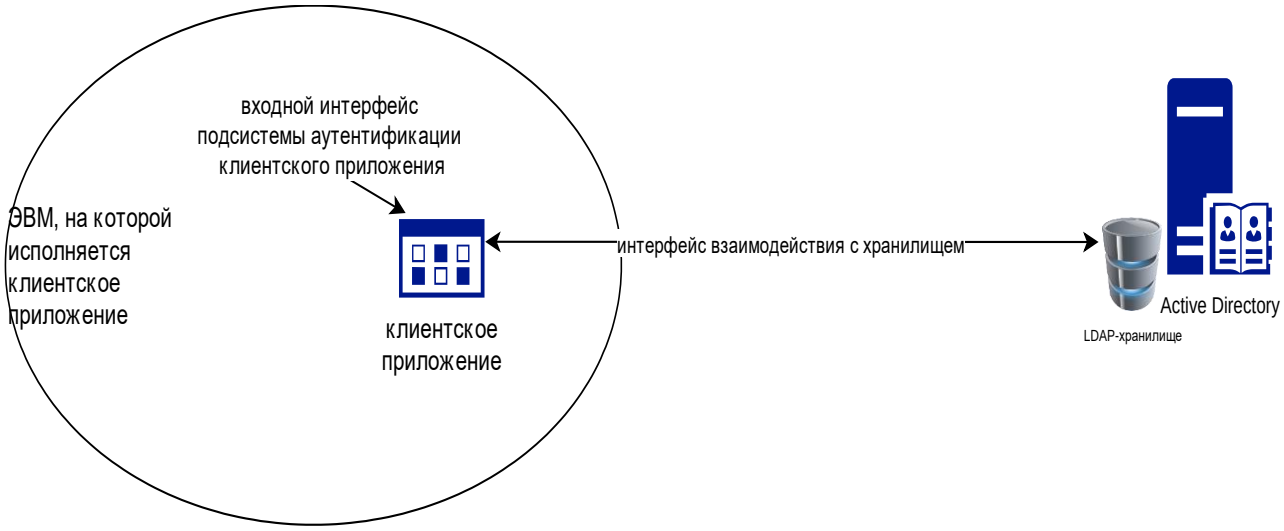

Рис. 1. Информационная система, в которой будет проводиться анализ уязвимостей
(Fig. 1. Informatization system, in which the analysis of vulnerabilities will be carried out)

1. Уязвимости, возникающие при аутентификации пользователей с использованием Active Directory

Общие угрозы процедуры аутентификации известны и приведены в [2]. Для рассматриваемой системы характерны следующие угрозы:

1. Так как ЭВМ, на которой исполняется клиентское приложение в общем случае не является доверенной, возникает угроза несанкционированного доступа к переменному окружению среды исполнения клиентского приложения. В результате процесс аутентификации в клиентском приложении может быть обойден злоумышленником.
2. Клиентское приложение обращается к LDAP-хранилищу AD с использованием интерфейса взаимодействия. Поскольку предполагается, что клиентское приложение работает в ЭВМ, не являющейся контроллером домена Active Directory, возникает угроза обеспечения конфиденциальности передаваемых данных между клиентским приложением и контроллером домена AD. (Подробно об угрозе нарушения конфиденциальности данных приведено в [2 с. 64–65]).
3. Угроза нарушения целостности данных LDAP-хранилища AD является актуальной, поскольку целостность базы данных является фактором, влияющим на процесс аутентификации клиентского приложения в целом. (Подробнее об угрозе нарушения целостности данных LDAP-хранилища в [3 с. 163]).
4. Угроза нарушения свойства доступности данных LDAP-хранилища AD также является актуальной, поскольку доступность базы данных является фактором, влияющим на процесс аутентификации клиентского приложения в целом. (Подробнее об угрозе нарушения доступности LDAP-хранилища в [4 с. 152]).
5. Стоит также упомянуть об угрозе нарушения подлинности контроллера домена Active Directory, на котором расположено LDAP-хранилище учетных данных пользователей. (Подробнее об угрозе нарушения подлинности контроллера домена в [5 с. 4478]).

2. Разработка модели угроз информационной безопасности ИС

Для построения модели угроз информационной безопасности ИС используются методики и каталог угроз из методических документов ФСТЭК [6], стандартов Банка России [7].

Согласно [6, 8 с. 1052] модель угроз должна включать в себя:

- Описание информационной системы и особенностей ее функционирования.
- Модель нарушителя.
- Актуальные угрозы информационной безопасности.

Хорошо построенная модель угроз позволит сформулировать требования, выполнение которых приведет к обеспечению защищенности системы от рассматриваемых угроз.

В рамках данной работы воспользуемся объектно-ориентированным подходом, описанным в [9] для построения проекта модели угроз.

Для корректного построения модели необходимо принимать во внимание все особенности ИС, ее свойства. Однако, в данной работе не было цели рассмотреть все возможные угрозы для ИС данного вида (см. рис. 1). Входными данными модели будут являться функциональные особенности клиентского приложения: выполнение аутентификации пользователей с использованием Active Directory, зависимость доступности пользователю определенного функционала приложения от авторизации пользователя, исполнение приложения в недоверенной среде. Для рассматриваемого объекта анализа имеет смысл выбрать стандартные источники угроз [7]: внутренний

пользователь системы, внешний пользователь (злоумышленник, не имеющий санкционированного доступа к системе). Угрозы, отражаемые в модели, состоят из угроз, характерных для рассматриваемого объекта анализа [10 с. 61], а также базовых угроз приложений ИС [7]. Благодаря рассмотрению ИС под углом ее функциональных особенностей можно считать данный список угроз исчерпывающим.

На рис. 2 показана концептуальная модель угроз.

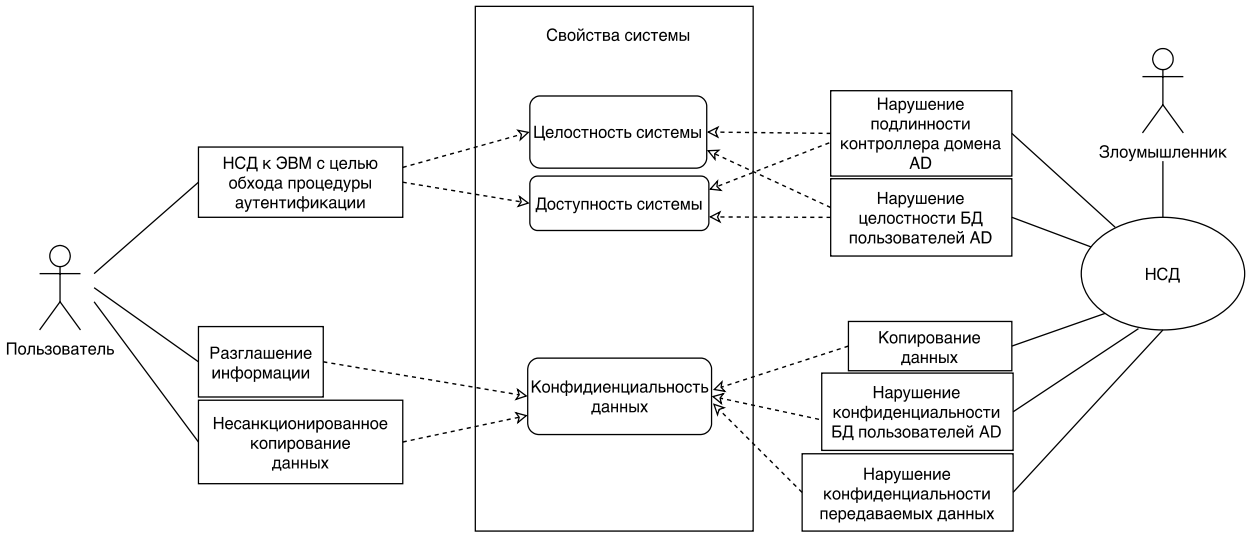

Рис. 2. Концептуальная модель угроз
(Fig. 2. Conceptual Threat Model)

В данном представлении *системой* является клиентское приложение. Под целостностью системы понимается целостность базы данных пользователей из активного каталога, а также подлинность ЭВМ, на котором данная база данных хранится. Под доступностью системы понимается доступность соответствующего (данному пользователю) функционала и данных клиентского приложения конкретному авторизованному пользователю.

Критически важными свойствами системы являются ее целостность, конфиденциальность и доступность данных. Схема позволяет визуализировать способы реализации рассматриваемых угроз для каждого из свойств системы. Пунктиром показана связь между рассматриваемыми угрозами их влиянием на свойства системы. Сплошной линией показаны возможные действия для источников угроз.

Переход от данного представления к детальному описанию атак для рассматриваемого процесса не вызывает трудностей, поскольку становятся явно видны связи между источниками угроз, угрозами и активами системы.

Результаты анализа атак для процесса аутентификации пользователей приведены в табл. 1.

Построенная таблица позволяет выявить критические места безопасности системы и сформировать требования, необходимые для повышения уровня безопасности систем, использующих AD для аутентификации.

Таблица 1. Перечень атак для рассматриваемого процесса аутентификации пользователей

Номер атаки	Описание атаки	Уязвимости	Последствия
1	НСД к ЭВМ-исполнителю клиентского приложения с целью обхода процедуры аутентификации	Отсутствие возможности контроля целостности ПО ЭВМ-исполнителя клиентского приложения	Обход процедуры аутентификации в клиентском приложении
2	Пассивный НСД к передаваемым данным между клиентским приложением и контроллером домена AD с целью дальнейшего НСД к клиентскому приложению	Отсутствие шифрования передаваемых данных	Утечка АИП пользователей с последующим НСД к клиентскому приложению
3	Активный НСД к передаваемым данным между клиентским приложением и контроллером домена AD с целью обхода процедуры аутентификации; нарушения доступности функционала клиентского приложения	Отсутствие взаимной аутентификации контроллера домена AD и клиентского приложения	Обход процедуры аутентификации клиентского приложения. Запрет доступа для легальных пользователей.
4	Активный НСД к LDAP-хранилищу КД с целью обхода процедуры аутентификации; нарушения доступности функционала клиентского приложения	Отсутствие контроля целостности содержимого LDAP-хранилища на контроллере домена AD.	Обход процедуры аутентификации с помощью модификации состояния БД пользователей. Запрет доступа для легальных пользователей.
5	Пассивный НСД к LDAP-хранилищу КД с целью обхода процедуры аутентификации	Отсутствие шифрования содержимого LDAP-хранилища КД AD.	Обход процедуры аутентификации с последующим использованием АИП легального пользователя

В результате детального рассмотрения атаки 1, можно сформировать следующее требование безопасности: нарушитель, имеющий возможность контролировать среду исполнения клиентского приложения, не должен иметь возможности обойти процедуру аутентификации клиентского приложения. Данное требование может быть реализовано разными способами, например на уровне архитектуры процессора ЭВМ, на которой исполняется приложения [2 с. 106, 11 с. 6076].

В результате детального рассмотрения атаки 3, можно сформулировать следующее требование безопасности: необходимо выполнять проверку подлинности контроллера домена Active Directory при каждой процедуре аутентификации. Данное требование может

быть реализовано с помощью инфраструктуры открытых ключей в объединении с концепцией РКБ [12].

В результате детального рассмотрения атаки 2, можно сформулировать следующее требование безопасности: необходимо обеспечить конфиденциальность передаваемых данных по каналу связи клиентского приложения с контроллером домена AD. Данное требование может быть реализовано с помощью криптографических средств [13 с. 196] защиты информации; либо за счет установки доверенного сеанса связи между данными объектами [14 с. 46949, 15].

В результате детального рассмотрения атаки 4, можно сформулировать следующее требование безопасности: необходимо обеспечить целостность LDAP-хранилища AD. Данное требование может быть реализовано с использованием СДЗ, имеющего функциональность контроля целостности системы.

В результате детального рассмотрения атаки 5, можно сформулировать следующее требование безопасности: необходимо обеспечить конфиденциальность хранимых данных в LDAP-хранилище. Данное требование может быть реализовано с помощью криптографических методов защиты информации.

Итого, с учетом проведенного выше анализа и лучших практик в области информационной безопасности процессов аутентификации сформулируем следующие требования безопасности:

1. Нарушитель с соответствующими привилегиями контроля среды клиентского приложения не должен иметь возможности обойти процедуру аутентификации клиентского приложения.
2. Должна быть обеспечена конфиденциальность данных, передаваемых между клиентским приложением и контроллером домена AD.
3. Должна быть обеспечена конфиденциальность данных, находящихся в LDAP-хранилище.
4. Должна быть обеспечена целостность LDAP-хранилища AD.
5. Должна быть обеспечена подлинность контроллера домена AD.

Заключение

Построенная концептуальная модель угроз позволяет понять связь между источниками угроз, свойствами системы и угрозами. Слабым местом рассматриваемой системы являются уязвимости, связанные с отсутствием явного шифрования передаваемых и хранимых учетных данных пользователей; уязвимости, связанные с отсутствием контроля целостности и подлинности ЭВМ, принимающих участие в процедуре аутентификации пользователей в приложении. В результате анализа были сформулированы необходимые требования безопасности, направленные на обеспечение подлинности контроллера домена, а также обеспечение конфиденциальности передаваемых и хранимых данных. Основные требования могут быть удовлетворены с помощью использования криптографических методов защиты информации, а также использования РКБ на ЭВМ, участвующих в процессе аутентификации. Результаты данной работы позволяют проводить дальнейшие исследования в области аутентификации пользователей в распределенных системах.

Таким образом, проведен анализ уязвимостей и атак для рассматриваемого процесса аутентификации пользователей. Из анализа можно сделать вывод о целесообразности применимости (с точки зрения информационной безопасности) данного способа аутентификации при соблюдении требований безопасности, обозначенных выше.

СПИСОК ЛИТЕРАТУРЫ:

1. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты., М.: Книжный мир, 2009. – 352 с. URL: https://computer-museum.ru/books/computer_safety.pdf (дата обращения: 15.08.2020).
2. Конявский В.А., Конявская С.В. Доверенные информационные технологии: от архитектуры к системам и средствам. Москва: URSS, 2019. – 264 с.
3. Deepa G., Thilagam P. S. Securing web applications from injection and logic vulnerabilities: Approaches and challenges //Information and Software Technology. 2016. Vol. 74. P. 160–180. DOI: http://dx.doi.org/10.1016/j.infsof.2016.02.005.
4. Obimbo C. et al. Vulnerabilities of LDAP As An Authentication Service. J. Information Security. 2011. Vol. 2. No. 4. P. 151–157. DOI: http://dx.doi.org/10.4236/jis.2011.24015.
5. Binduf A. et al. Active Directory and Related Aspects of Security. 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018. P. 4474–4479. DOI: http://dx.doi.org/10.1109/NCG.2018.8593188.
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 15 февраля 2008 г. URL: https://fstec.ru/component/attachments/download/289 (дата обращения: 27.05.2020).
7. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014. Принят и введен в действие распоряжением Банка России от 17.05.2014 No Р-399. URL: http://cbr.ru/credit/Gubzi_docs/st-10-14.pdf (дата обращения: 27.05.2020).
8. Hoque M. A., Hasan R. Towards a Threat Model for Vehicular Fog Computing. 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2019. С. 1051–1057. DOI: http://dx.doi.org/10.1109/UEMCON47517.2019.8993064.
9. Грибанова-Подкина М.Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования. Вопросы безопасности. 2017. № 2. С. 25–34. DOI: http://dx.doi.org/10.7256/2409-7543.2017.2.22065. URL: https://nbpublish.com/library_read_article.php?id=22065.
10. Matsuda W., Fujimoto M., Mitsunaga T. Detecting apt attacks against active directory using machine leaning. 2018. IEEE Conference on Application, Information and Network Security (AINS). IEEE, 2018. С. 60–65. DOI: http://dx.doi.org/10.1109/AINS.2018.8631486.
11. Alhaidary M. et al. Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the offpad protocol. IEEE Access. 2018. Vol. 6. P. 6071–6081. DOI: http://dx.doi.org/10.1109/ACCESS.2017.2789301.
12. Конявский, В.А., Гадасин В.А. Основы понимания феномена электронного обмена информацией (Библиотека журнала «УЗИ»; Кн. 2). М.: Беллитфонд, 2004. – 282 с. URL: https://www.okbsapr.ru/upload/iblock/016/osnovi_ponim_el_obmen_inf.pdf.
13. Buchanan W.J., Li S., Asif R. Lightweight cryptography methods. Journal of Cyber Security Technology. 2017. Vol. 1. №. 3–4. С. 187–201. DOI: http://dx.doi.org/10.1080/23742917.2017.1384917.
14. Qian J. et al. A Trusted-ID Referenced Key Scheme for Securing SCADA Communication in Iron and Steel Plants. IEEE Access. 2019. Vol. 7. P. 46947–46958. DOI: http://dx.doi.org/10.1109/ACCESS.2019.2909011.
15. Конявский В. А. Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем – на старт, внимание, МАРШ! //Комплексная защита информации. Материалы XV международной научно-практической конференции (Иркутск (Россия), 1–4 июня 2010 г.). М.: 2010. С. 166–169; URL: http://www.accord.ru/konyavskiy_2010_1.htm1.

REFERENCES:

[1] Shherbakov, A.Ju. Modern computer security. Theoretical bases. Practical aspect., M.: Knizhnyi mir, 2009. – 352 p. URL: https://computer-museum.ru/books/computer_safety.pdf (accessed: 15.08.2020) (in Russian).
[2] Konjavskij V.A., Konjavskaja S.V. Trusted information technologies: from architecture to systems and tools. Moskva: URSS, 2019. – 264 p. (in Russian).
[3] Deepa G., Thilagam P. S. Securing web applications from injection and logic vulnerabilities: Approaches and challenges //Information and Software Technology. 2016. Vol. 74. P. 160–180. DOI: http://dx.doi.org/10.1016/j.infsof.2016.02.005.
[4] Obimbo C. et al. Vulnerabilities of LDAP As An Authentication Service. J. Information Security. 2011. Vol. 2. No. 4. P. 151–157. DOI: http://dx.doi.org/10.4236/jis.2011.24015.
[5] Binduf A. et al. Active Directory and Related Aspects of Security //2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018. P. 4474–4479. DOI: http://dx.doi.org/10.1109/NCG.2018.8593188.

[6] The basic model of threats to the security of personal data during their processing in personal data information systems. February 15, 2008. URL: https://fstec.ru/component/attachments/download/289 (accessed: 27.05.2020) (in Russian).
[7] Standard of the Bank of Russia " ensuring information security of organizations of the banking system of the Russian Federation. Generalities» STO BR IBBS-1.0-2014. Adopted and put into effect by the order of the Bank of Russia from May 17, 2014 No R-399. URL: http://cbr.ru/credit/Gubzi_docs/st-10-14.pdf (accessed: 27.05.2020) (in Russian).
[8] Hoque M. A., Hasan R. Towards a Threat Model for Vehicular Fog Computing. 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2019. P. 1051–1057. DOI: http://dx.doi.org/10.1109/UEMCON47517.2019.8993064.
[9] Gribanova-Podkina M.Ju. Building a model of threats to information security of an information system using the methodology of object-oriented design. Voprosy bezopasnosti. M.: 2017. No 2. P. 25–34. DOI: http://dx.doi.org/10.7256/2409-7543.2017.2.22065 (in Russian).
[10] Matsuda W., Fujimoto M., Mitsunaga T. Detecting apt attacks against active directory using machine leaning. 2018 IEEE Conference on Application, Information and Network Security (AINS). IEEE, 2018. P. 60–65. DOI: http://dx.doi.org/10.1109/AINS.2018.8631486.
[11] Alhaidary M. et al. Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the offpad protocol. IEEE Access. 2018. Vol. 6. P. 6071–6081. DOI: http://dx.doi.org/10.1109/ACCESS.2017.2789301.
[12] Konjavskij, V. A., Gadasin V. A. Fundamentals of understanding the phenomenon of electronic information exchange (Library of the magazine "UZI"; Book 2). M.: Bellitfond, 2004. – 282 p. URL: https://www.okbsapr.ru/upload/iblock/016/osnovi_ponim_el_obmen_inf.pdf (in Russian).
[13] Buchanan W. J., Li S., Asif R. Lightweight cryptography methods //Journal of Cyber Security Technology. – 2017. Vol. 1. №. 3–4. P. 187–201. DOI: http://dx.doi.org/10.1080/23742917.2017.1384917.
[14] Qian J. et al. A Trusted-ID Referenced Key Scheme for Securing SCADA Communication in Iron and Steel Plants. IEEE Access. 2019. Vol. 7. P. 46947–46958. DOI: http://dx.doi.org/10.1109/ACCESS.2019.2909011.
[15] Konjavskij V.A. A trusted communication session. Development of the paradigm of trusted computing systems - at the start, attention, MARSh! Comprehensive information protection. Materials of the XV International scientific and practical conference (Irkutsk (Russia), 1–4 June 2010). M.: 2010. P. 166–169; URL: http://www.accord.ru/konyavskiy_2010_1.htm1 (in Russian).

Поступила в редакцию – 15 августа 2020 г. Окончательный вариант – 01 ноября 2020 г.
Received – August 15, 2020. The final version – November 01, 2020.