УДК 004.056

Исследование технологий создания и управления сетевыми ресурсами кредитно-финансовых организаций

Исследованы технологии создания и управления сетевыми ресурсами (сайтами) на примере 24 кредитно-финансовых организаций (КФО) Республики Беларусь. Проведено тестирование уровня информационной безопасности (ИБ) библиотек JavaScript, а также алгоритмов реализации шифрования на основе SSL-сертификатов для сайтов КФО.

Ключевые слова:
вредоносное программное обеспечение, SSL-сертификат, библиотеки JavaScript.

В.В. МАЛИКОВ,
канд. техн. наук, доцент,
начальник цикла технических и специальных дисциплин УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь

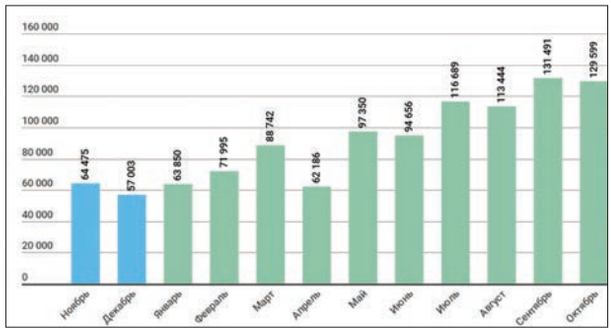
Введение. В настоящее время в мире и Республике Беларусь значительно активизировалась криминальная деятельность преступников, связанная с правонарушениями в сфере высоких технологий [1, 2] (рис. 1). Для осуществления такой противоправной деятельности активно используются недостатки/уязвимости в алгоритмах/технологиях создания и управления различными сетевыми ресурсами, размещенными в глобальной сети интернет. Особый интерес у киберпреступников вызывают сетевые ресурсы/сервисы КФО, выполняющие задачи как по информированию населения, так и функции непосредственного осуществления финансовых платежей.

Приведенные в рамках данной статьи материалы носят исключительно научно-исследовательский характер. Исследование проводилось автором строго в научных целях, его результаты не являются и не могут признаваться руководством к совершению каких-либо противоправных действий. При проведении исследования автор действовал в рамках законодательства Республики Беларусь. Автор не несет ответственности за инциденты в сфере информационной безопасности, имеющие отношение к тематике исследования.

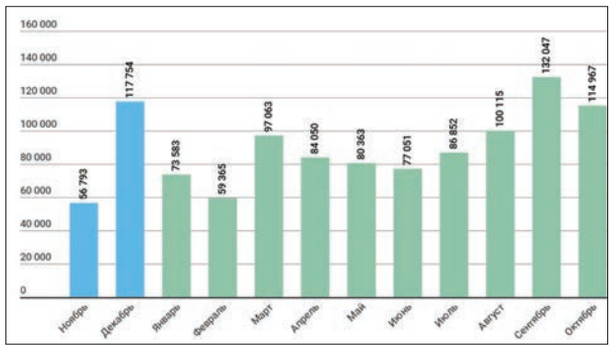
Содержательная постановка задачи. Согласно данным исследований [2], Республика Беларусь входит в число 20 стран, в которых пользователи: подвергались наибольшему риску заражения вредоносным программным обеспечением (ВПО) через интернет (2-е место) и наибольшему риску локального заражения ВПО (17-е место).

Для оценки технологического уровня и степени безопасности сервисов/ресурсов в сети интернет проведем тестирование технологий создания и управления сетевыми ресурсами (сайтами) на примере КФО Республики Беларусь. С этой целью были выбраны 24 белорусские КФО из реестра Национального банка Республики Беларусь, имеющие специальные разрешения (лицензии) на осуществление банковской деятельности [3]. Названия КФО заменены порядковыми номерами для сохранения конфиденциальности.

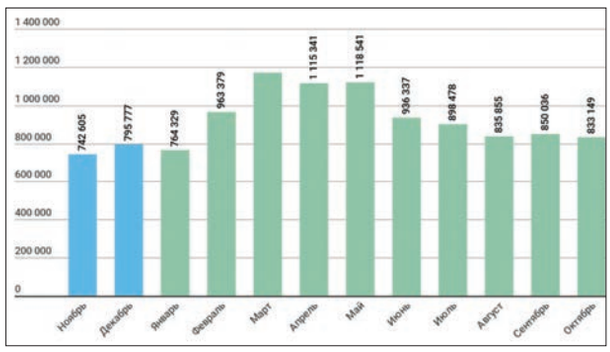
Результаты и обсуждение. Недостаточный уровень технологических решений, выбранных для реализации алгоритмов создания и управления сетевыми ресурсами (сайтами), приводит к наличию значительного числа программных ошибок и уязвимостей ИБ при эксплуатации таких сайтов, что в свою очередь эффективно используется киберпреступниками для осуществления несанкционированного доступа и кражи информации/финансовых средств [4, 5].



а) Количество пользователей, атакованных банковским ВПО



б) Количество пользователей, атакованных троянцами-шифровальщиками



в) Количество пользователей, атакованных майнерами

Рисунок 1 – Статистические данные по информационной безопасности (ноябрь 2017 г. – октябрь 2018 г.) [2]

Для оценки технологического уровня и степени безопасности сетевых ресурсов 24 КФО Республики Беларусь проведем их комплексное тестирование сетевым сканером Lighthouse (рис. 2) [6].

В качестве основных параметров технологического уровня (диапазон соответствия параметров измерения к эталонному уровню: 0÷100 у.е., где 100 у.е. – высший уровень соответствия) [6] сайтов КФО, подлежащих исследованию, использовались:

Performance – интервал времени, требуемый для отображения контента, пригодного для непосредственного использования;

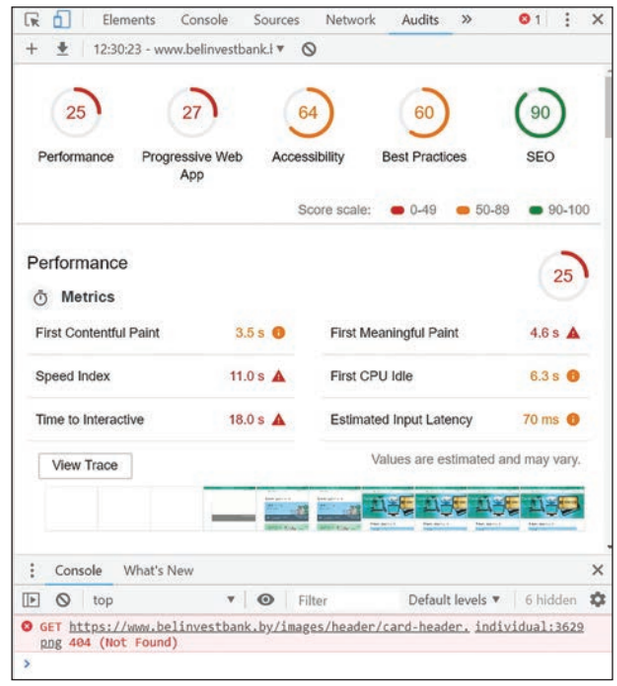
Progressive Web App – степень соответствия стандарту прогрессивного веб-приложения;

Accessibility – степень адаптации для использования сайта людьми с ограниченными возможностями;

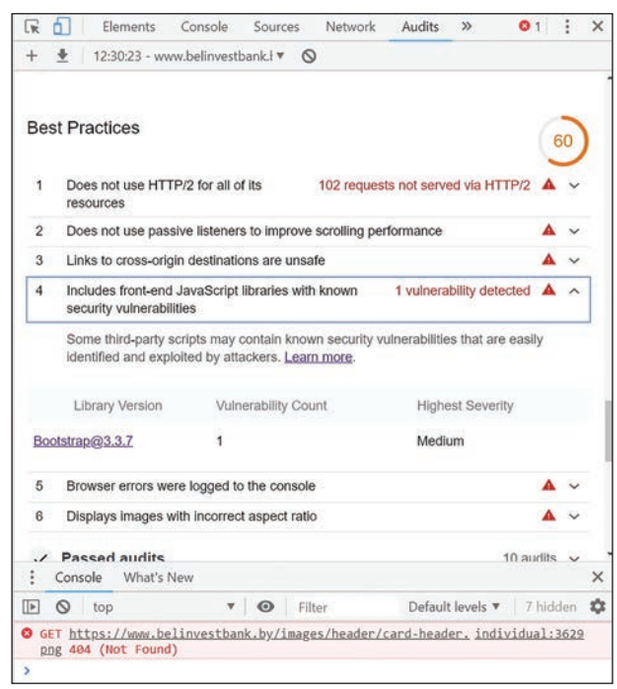
Best Practices – уровень соответствия лучшим практикам современной веб-разработки;

SEO – степень оптимизации для ранжирования результатов поиска.

Для повышения точности измерений при проведении тестирования учитывался режим Throttling – моделирование нагрузочной способности эмулируемой ЭВС.



а) Общий результат теста



б) Результат теста библиотек JavaScript

Рисунок 2 – Пример тестирования сайта типовой КФО сканером Lighthouse [6]

Таблица 1 – Результаты тестирования технологического уровня сайтов КФО

№ КФО	Версия сайта основного домена КФО									
	Mobile-версия / № параметра					Desktop-версия / № параметра				
	№1	№2	№3	№4	№5	№1	№2	№3	№4	№5
	Performance	Progressive Web App	Accessibility	Best Practices	SEO	Performance	Progressive Web App	Accessibility	Best Practices	SEO
1	33	31	65	73	100	17	27	73	73	100
2	19	46	38	73	70	31	46	38	73	70
3	19	31	52	60	90	16	27	64	60	90
4	51	31	42	53	80	69	31	42	60	80
5	16	27	36	73	90	15	27	36	80	90
6	16	31	66	73	91	18	27	50	73	91
7	26	31	54	60	90	21	27	56	60	90
8	12	26	52	60	80	21	54	65	67	80
9	44	46	83	67	82	41	46	83	67	82
10	38	58	62	67	100	36	27	56	67	100
11	6	35	70	60	100	6	31	70	60	100
12	1	19	44	60	80	10	19	44	60	80
13	3	31	54	60	100	2	27	54	60	100
14	42	31	58	73	100	30	27	61	73	100
15	18	31	62	60	100	11	27	62	60	100
16	35	58	66	73	91	54	54	78	80	91
17	20	31	47	67	100	5	27	50	67	100
18	59	54	29	60	100	13	54	29	60	100
19	22	31	74	73	100	26	27	76	73	100
20	31	31	71	67	100	17	27	82	73	100
21	70	31	41	47	70	64	31	41	47	70
22	59	58	66	67	100	60	54	35	67	100
23	2	31	72	73	100	15	27	56	73	100
24	15	58	70	87	89	21	54	70	80	89

Результаты тестирования технологического уровня сайтов 24 КФО приведены в таблице 1, а также показаны в виде 3D surface -поверхности (с дополнительной контурной диаграммой) (рис. 3) [7]. По результатам исследования (табл. 1, рис. 3) можно сделать следующий вывод: все 24 сайта (100 %) основного домена КФО (Mobile/Desktop-версии) по 4 тестируемым параметрам (исключение – параметр №5 SEO) имеют относительно низкий уровень соответствия эталонным значениям, что проявляется в значительном числе ошибок программного кода, использовании устаревших технологических решений, конфликтах при обработке запросов и др. [6]. Указанные недостатки позволяют киберпреступниками проводить эффективную эксплуатацию уязвимостей в программном коде для осуществления несанкционированного доступа и кражи информации/финансовых средств.

Проведенное углубленное тестирование библиотек JavaScript сайтов основного домена КФО [6], позволило выявить более детальный перечень уязвимостей ИБ (табл. 2), которые уже были внесены в базы экспертных знаний и описаны в них (тип потенциальных атак: Regular Expression Denial of Service, Cross-site Scripting, Cross-site Scripting in dialog close Text) [8, 9, 10, 11]. Следует отметить, что только 4 сайта основного домена КФО (17 %) не имеют уязвимостей библиотек JavaScript.

Для исследования уровня ИБ сайтов основного домена КФО дополнительно оценивались (табл. 3):

наличие и тип используемого SSL-сертификата;

качество реализации алгоритма защищенного соединения на основе SSL-сертификата (уровни оценки безопасности: A/A+, B, C, F; где A/A+ – высший уровень, F – низший уровень) [12].

В рамках настоящей статьи будем применять следующие типы валидации SSL-сертификатов [13]:

SSL-сертификаты, которые подтверждают только доменное имя (Domain Validation – DV);

SSL-сертификаты, которые подтверждают домен и организацию (Organization Validation – OV);

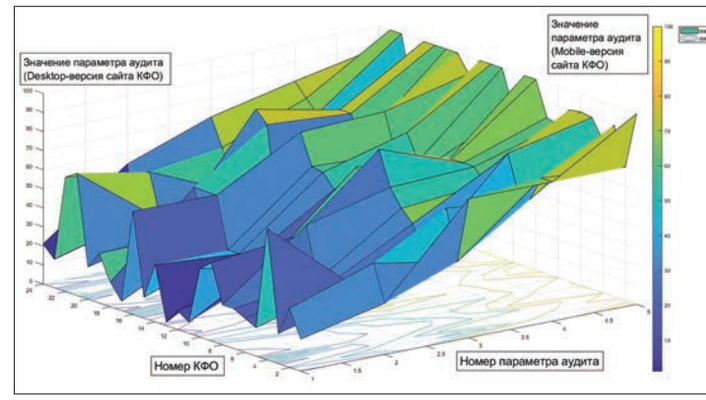


Рисунок 3 – Результаты тестирования КФО в виде 3D surface-поверхности (с дополнительной контурной диаграммой) [7]

Таблица 2 – Результаты тестирования библиотек JavaScript сайтов КФО [6]

№ КФО	Количество уязвимостей библиотек JavaScript	Уровень риска (оценка CVSS / тип CWE) [8, 9]	Описание выявленных уязвимостей / номер CVE или SNYK ID/[10, 11]
1	3	Средний (5,3 / CWE 400)	Regular Expression Denial of Service (ReDoS) /SNYK ID npm:moment:20161019/
		Средний (5,9 / CWE 400)	ReDoS /SNYK ID npm:moment:20160126/
		Низкий (3,7 / CWE 400)	ReDoS /CVE-2017-18214/
2	2	Средний (5,4 / CWE 79)	Cross-site Scripting (XSS) / CVE-2015-9251, CVE-2017-16012/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
3	1	Средний (6,5 / CWE 79)	XSS / CVE-2016-10735, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2019-8331/
4	2	Средний (5,4 / CWE 79)	XSS / CVE-2012-6708, CVE-2015-9251, CVE-2017-16011, CVE-2017-16012/
5	Уязвимостей не выявлено		
6	4	Средний (5,4 / CWE 79)	XSS / CVE-2013-4939, CVE-2013-4940, CVE-2015-9251, CVE-2017-16012/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
7	1	Средний (5,4 / CWE 79)	XSS /CVE-2015-9251, CVE-2017-16012/
8	4	Средний (6,5 / CWE 79)	XSS /CVE-2016-10735, CVE-2018-14042, CVE-2018-14040, CVE-2018-20676, CVE-2018-20677, CVE-2019-8331/
		Средний (5,4 / CWE 79)	XSS /CVE-2015-9251, CVE-2017-16012/
		Низкий (3,7 / CWE 400)	ReDoS /CVE-2017-18214/
		Средний (5,9 / CWE 400)	ReDoS /SNYK ID npm:moment:20161019/
9	3	Средний (5,4 / CWE 79)	XSS /CVE-2011-4969, CVE-2014-6071, CVE-2015-9251, CVE-2017-16012/
10	2	Средний (5,4 / CWE 79)	XSS /CVE-2015-9251, CVE-2017-16012/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
11	2	Средний (6,5 / CWE 79)	XSS / CVE-2016-10735, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2018-20677, CVE-2019-8331/
		Средний (5,4 / CWE 79)	XSS /CVE-2015-9251, CVE-2017-16012/
12	4	Средний (5,4 / CWE 79)	XSS / CVE-2015-9251, CVE-2017-16012/
		Средний (4,3 / CWE 79)	XSS /CVE-2010-5312/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
		Средний (4,3 / CWE 79)	XSS via Tooltip / CVE-2012-6662/
13	7	Средний (6,5 / CWE 79)	XSS /CVE-2016-10735, CVE-2018-6341, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2018-20677, CVE-2019-8331/
		Средний (5,4 / CWE 79)	XSS / CVE-2012-6708, CVE-2015-9251, CVE-2017-16011, CVE-2017-16012/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
		Низкий (3,7 / CWE 185, CWE 400)	ReDoS /SNYK ID npm:vue:20180222 /
		Средний (6,5 / CWE 79)	XSS /SNYK ID npm:vue:20170829/
14	2	Средний (6,5 / CWE 79)	XSS / CVE-2016-10735, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2018-20677, CVE-2019-8331/
		Низкий (3,7 / CWE 400)	ReDoS /CVE-2017-18214/
15	5	Средний (6,5 / CWE 79)	XSS /CVE-2016-10735, CVE-2018-6341, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2018-20677, CVE-2019-8331/
		Средний (5,4 / CWE 79)	XSS / CVE-2015-9251, CVE-2017-16012/
		Низкий (3,7 / CWE 400)	ReDoS /CVE-2017-18214/
		Средний (5,3 / CWE 400)	ReDoS /SNYK ID npm:moment:20161019/
		Средний (5,9 / CWE 400)	ReDoS /SNYK ID npm:moment:20160126/
16	3	Средний (5,4 / CWE 79)	XSS /CVE-2012-6708, CVE-2015-9251, CVE-2017-16011, CVE-2017-16012/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
17	Уязвимостей не выявлено		
18	2	Низкий (3,7 / CWE 400)	ReDoS /CVE-2016-10707/
		Средний (5,4 / CWE 79)	XSS /CVE-2011-4969/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
19	Уязвимостей не выявлено		
20	3	Средний (6,5 / CWE 79)	XSS / CVE-2016-10735, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2018-20677, CVE-2019-8331/
		Средний (5,4 / CWE 79)	XSS / CVE-2015-9251, CVE-2017-16012/
		Высокий (7,3 / CWE 79)	XSS in dialog close Text / CVE-2016-7103/
21	1	Средний (5,4 / CWE 79)	XSS / CVE-2011-4969, CVE-2015-9251, CVE-2017-16012/
22	1	Низкий (3,7 / CWE 400)	ReDoS /CVE-2017-18214/
23	2	Средний (5,4 / CWE 79)	XSS /CVE-2012-6708, CVE-2015-9251, CVE-2017-16011, CVE-2017-16012/
24	Уязвимостей не выявлено		

Таблица 3 – Результаты SSL-теста сайтов КФО

№	Наличие SSL-сертификата			Результат SSL-теста (тип потенциальных атак) [12]
	Нет	Да		
		SSL	EV SSL	
1				A+
2				A
3				A+
4		Тестирование не проводилось		
5				A+
6				A
7				B (Forward Secrecy)
8				B (Diffie-Hellman key exchange parameters)
9				B (Forward Secrecy, Diffie-Hellman key exchange parameters)
10				A
11				A+
12				A
13				A
14				B (Forward Secrecy)
15				A
16				A
17				B (Forward Secrecy)
18				B (Forward Secrecy)
19				A
20				A
21		Тестирование не проводилось		
22				A
23				B (Forward Secrecy)
24				A

SSL-сертификаты с расширенной проверкой (Extendet Validation – EV).

Результаты исследования (табл. 3) показали:

на 2 сайтах КФО (8 %) нет SSL-сертификата (не реализуется защищенное соединение);

на 7 сайтах КФО (29 %) имеются уязвимости при реализации защищенного соединения на основе SSL-сертификата (тип потенциальных атак: Forward Secrecy, Diffie-Hellman key exchange parameters) [12].

При сравнении полученных результатов тестирования (таблица 3) с сопоставимыми результатами за 2015 [14] и 2018 гг. [15] следует отметить значительное повышение уровня ИБ сетевых ресурсов КФО Республики Беларусь.

Заключение. На основании проведенных исследований можно сделать следующие выводы:

1. Владельцы КФО уделяют недостаточное внимание уровню технологических решений,

выбранных для реализации алгоритмов создания и управления сетевыми ресурсами (сайтами), что приводит к наличию значительного числа программных ошибок и уязвимостей ИБ при эксплуатации таких ресурсов (таблицы 1 и 2).

2. В целом имеется положительная динамика повышения уровня ИБ сетевых ресурсов КФО по сравнению с предыдущими анализируемыми периодами (таблица 3) [14, 15].

3. Владельцам сетевых ресурсов КФО необходимо постоянно осуществлять оперативные аудиты таких ресурсов на предмет наличия технологических/программных уязвимостей/ошибок, а также проводить систематическую работу по устранению выявленных недостатков.

ЛИТЕРАТУРА

1. Статистические сведения по итогам работы за 2018 год// mvd.gov.by [Электрон. ресурс]. – 20102018. – Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3311. – Дата доступа: 01.03.2019.
2. Kaspersky Security Bulletin 2018. Статистика // securelist.ru [Электрон. ресурс]. – 2019. – Режим доступа: https://threatpost.ru/ddg-botnet-miner-keeps-on-rapidly-evolving/30879/. – Дата доступа: 01.03.2019.
3. Банковская система // nbrb.by [Электрон. ресурс]. – 2000-2019. – Режим доступа: https://www.nbrb.by/system/banks/list. – Дата доступа: 02.03.2019.
4. National Cyber Awareness System // us-cert.gov [Электрон. ресурс]. – 2019. – Режим доступа: https://www.us-cert.gov/ncas. – Дата доступа: 02.03.2019.
5. Threats // ncsc.gov.uk [Электрон. ресурс]. – 2019. – Режим доступа: https://www.ncsc.gov.uk/threats. – Дата доступа: 02.03.2019.
6. Lighthouse // developers.google.com [Электрон. ресурс]. – 2019. – Режим доступа: https://developers.google.com/web/tools/lighthouse/. – Дата доступа: 03.03.2019.
7. MATLAB // mathworks.com [Электрон. ресурс]. – 1994-2019. – Режим доступа: https://www.mathworks.com/products/matlab.html?s_tid=hp_ff_p_matlab. – Дата доступа: 04.03.2019.
8. Common Vulnerability Scoring System Version 3.0 Calculator // first.org [Электрон. ресурс]. – 1995-2019. – Режим доступа: https://www.first.org/cvss/calculator/3.0. – Дата доступа: 04.03.2019.
9. Common Weakness Enumeration // cwe.mitre.org [Электрон. ресурс]. – 2006-2019. – Режим доступа: https://cwe.mitre.org/data/index.html. – Дата доступа: 04.03.2019.
10. Common Vulnerabilities and Exposures // cve.mitre.org [Электрон. ресурс]. – 1999-2019. – Режим доступа: https://cve.mitre.org/. – Дата доступа: 04.03.2019.
11. Vulnerability DB // snyk.io [Электрон. ресурс]. – 2019. – Режим доступа: https://snyk.io/vuln. – Дата доступа: 04.03.2019.
12. SSL Server Test // ssllabs.com [Электрон. ресурс]. – 2009-2019. – Режим доступа: https://www.ssllabs.com/ssltest/. – Дата доступа: 06.03.2019.
13. Цифровые SSL-сертификаты. Разновидности, как выбрать? // habrahabr.ru [Электрон. ресурс]. – 2006-2019. – Режим доступа: https://habrahabr.ru/company/tuthost/ blog/150433/. – Дата доступа: 05.03.2019.
14. **Маликов, В.В** Исследование несанкционированного доступа к системам безналичных электронных платежей / В.В. Маликов, И.И. Лившиц // Веснік сувязі. – 2015. – № 5 (133). – С. 52–56.
15. **Маликов, В.В.** Исследование уровня информационной безопасности сетевых ресурсов кредитно-финансовых организаций / В.В. Маликов, М.А. Бабич // Веснік сувязі.–2018. – № 3 (149). – С. 50–54.

The technologies of creation and management of network resources (sites) are investigated on the example of 24 credit and financial organizations (CFO) of the Republic of Belarus. Testing of the level of information security (IS) of the JavaScript libraries, as well as algorithms for the implementation of encryption based on SSL certificates for sites of the CFO was conducted.

Получено 11.03.2019.