Аналитическая статья
УДК 621.39; 004.056; DOI: 10.61260/2218-13X-2023-4-99-108

ФОРМАЛЬНЫЙ ПОДХОД К ВЫЯВЛЕНИЮ НАИБОЛЕЕ «ОПАСНЫХ» СВОЙСТВ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОЗИЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

✉Буйневич Михаил Викторович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия.
Леонов Николай Викторович.
Государственный научно-исследовательский институт прикладных проблем, Санкт-Петербург, Россия.
Хорошенко Виктория Сергеевна.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия
✉bmv1958@yandex.ru

Аннотация. Работа посвящена изучению взаимосвязей между свойствами информационной системы, угрозами ее информационной безопасности и последствиями их реализации. Для этого в текстовой и аналитической форме предлагается авторский подход, заключающийся в выделении единого терминологического базиса предметной области и состоящий из следующих шагов: анализ текстового названия угроз из базы данных; деление его на слова; их нормализация и выделение ключевых (то есть отражающих суть); отожествление ключевых слов со свойствами информационной системы; сбор статистики встречаемости ключевых слов в названиях угроз, приводящих к нарушениям (по отдельности) конфиденциальности, целостности и доступности информации. Описывается разработанный программный прототип, автоматизирующий данный подход для «Банка данных угроз безопасности информации» Федеральной службы по техническому и экспертному контролю России и выдающий результат в виде трех списков последствий, согласно нарушениям информационной безопасности, отранжированных по количеству слов в соответствующих угрозах. Производится анализ Топ-10 наиболее «опасных» свойств информационной системы для каждого из списков и делаются соответствующие выводы.

Основным научным результатом является подход к изучению взаимосвязей между сущностями предметной области на примере угроз информационной безопасности и реализации их последствий для отдельных свойств абстрактной информационной системы. Новизна результата состоит в полном отсутствии субъективного мнения эксперта на этапе анализа описания угроз информационной безопасности и получения взаимосвязей. Теоретическая значимость заключается в переводе подхода в формализованную плоскость и установлении возможности его применения к другим сущностям, а практическая состоит в получении прототипа, который позволяет формально выделять наиболее «опасные» свойства информационной системы с позиции различных последствий от связанных с ними угроз информационной безопасности, что, таким образом, указывает на ее наиболее критичные части.

Ключевые слова: информационная безопасность, информационная система, угроза, Банк данных угроз безопасности информации Федеральной службы по техническому и экспертному контролю России, статистика, программный прототип

Для цитирования: Буйневич М.В., Леонов Н.В., Хорошенко В.С. Формальный подход к выявлению наиболее «опасных» свойств информационной системы с позиции угроз безопасности информации // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 4. С. 99–108. DOI: 10.61260/2218-13X-2023-4-99-108.

Analytical article

FORMAL APPROACH TO THE MOST INFORMATION SYSTEM «DANGEROUS» PROPERTIES IN TERMS OF INFORMATION SECURITY THREATS IDENTIFYING

✉**Buinevich Mikhail V.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia.
Leonov Nikolay V.
State research institute of applied problems, Saint-Petersburg, Russia.
Khoroshenko Victoria S.
Bonch-Bruevich Saint-Petersburg state university of telecommunications,
Saint-Petersburg, Russia
✉***bmv1958@yandex.ru***

Abstract. The work is devoted to the study of interrelations between the characteristics of an information system, threats to its information security and consequences of their realization. For this purpose, the author's approach in textual and analytical form is proposed, which consists in the allocation of a unified terminological base of the subject area and consists of the following steps: analysis of the textual names of threats from the database; their division into words; their normalization and selection of keywords (i.e. reflecting the essence); identification of keywords with the properties of the information system; collection of statistics on the occurrence of keywords in the names of threats leading to violations (separately) of confidentiality, integrity and availability of information. The developed software prototype is described, which automates this approach for the «Information Security Threats Database» of Federal service for technical and expert control of Russia and produces the result in the form of three lists of consequences according to information security violations, ranked by the number of words in the corresponding threats. The top 10 most «dangerous» properties of the information system for each of the lists are analyzed and the corresponding conclusions are drawn.

The main scientific result is an approach to the study of interrelations between entities of the subject area on the example of information security threats and the realization of their consequences for individual properties of an abstract information system. The novelty of the result consists in the complete absence of subjective expert opinion at the stage of analyzing the description of information security threats and obtaining interrelations. The theoretical significance consists in translating the approach to a formalized level and establishing the possibility of its application to other entities, and the practical significance consists in obtaining a prototype that allows to formally identify the most «dangerous» properties of an information system from the position of various consequences of information security threats associated with them, thus indicating its most critical parts.

Keywords: information security, information system, threat, Information Security Threat Data Bank of Federal service for technical and expert control of Russia, statistics, software prototype

For citation: Buinevich M.V., Leonov N.V., Khoroshenko V.S. Formal approach to the most information system «dangerous» properties in terms of information security threats identifying // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2023. № 4. P. 99–108. DOI: 10.61260/2218-13X-2023-4-99-108.

Введение

Обеспечение безопасности информационных систем (ИС), как главного хранилища и обработчика информационных ресурсов, является приоритетным направлением деятельности любого современного государства. Связано это с тем, что последствия от реализации угроз безопасности информации могут вести как к существенным

финансовым или репутационным потерям, так и к человеческим жертвам. Отсюда любое всестороннее изучение данной предметной области является, безусловно, актуальным.

Существует достаточно большое количество исследований, посвященных таким вопросам, как анализ причин появления отдельных (или групп) угроз и последствий их реализации, синтез способов противодействия, систематизация угроз в целые базы данных. Так, в работе [1] изучается появление новых информационных угроз, в том числе связанных с кибертерроризмом. В качестве примеров областей выделяются все, в которых присутствуют предпосылки для борьбы; например, политической или финансовой. Последствия же угроз в первом приближении указываются не столь значительными, за которыми, впрочем, могут идти довольно критические (например, гражданские конфликты, человеческие жертвы и пр.). В статье [2] рассматриваются угрозы иного рода, имеющие коммуникативный характер и направленные на «подавление» отдельных людей; приводятся методы такого рода «кибербуллинга» (*от англ.* bullying – запугивание, психологическое или физическое насилие, травля с использованием цифровых технологий), как использование личной информации, анонимные угрозы, преследование, «флейминг» (*от англ.* flame – пламя; это кибербуллинг, который начинается с оскорблений и перерастает в быстрый обмен репликами, обычно на страницах в социальных сетях) и «хеппислепинг» (*от англ.* happy slapping – *досл.* счастливое хлопанье или радостное избиение; здесь – насилие с видео-фиксацией на камеру мобильного телефона с последующим выставлением на различных интернет ресурсах). Работа [3] посвящена систематизации угроз программного обеспечения с выделением их характеристик. В частности, все рассмотренные угрозы разделяются по следующим категориальным парам: инициируемые случайными или злонамеренными действиями, действующие через человека или напрямую на ИС, реализуемые посредством уязвимостей в программном или аппаратном обеспечении. В работе [4] кратко рассматриваются базы данных для хранения уязвимостей, такие как CVE, NVD, VulnDB, OSVBD, а также «Банк данных угроз безопасности информации» Федеральной службы по техническому и экспертному контролю России (ФСТЭК).

Тем не менее практически отсутствуют исследования, посвященные концептуальным вопросам взаимосвязей между угрозами и другими сущностями предметной области. Так, например, до конца не ясно, насколько в принципе наличие аппаратных составляющих ИС влияет на нарушение конфиденциальности данных; или же к чему, как правило, приводит наличие доступа (как абстрактного свойства) к информационному ресурсу – к нарушениям его целостности или доступности.

Исходя из вышесказанного, можно сформулировать одно из противоречий предметной области, как частный характер существующих исследований для выявления лишь отдельных связей между ее сущностями при необходимости понимания общих закономерностей между ними. В интересах разрешения противоречия далее будет предложен подход, позволяющий определять закономерности между свойствами (физическими и логическими, статическими и динамическими и т.д.) ИС (свойства ИС), возникающими угрозами (как существующими, так и гипотетическими) и последствиями их реализации.

Подход к исследованию

Опишем кратко предлагаемый подход (подход) по выявлению угроз и последствий их реализации, исходя из свойств ИС. Максимально абстрактная взаимосвязь данных сущностей отражается следующим образом: «угрозы, связанные с определенными свойствами ИС, приводят к некоторым комбинациям последствий их (угроз) реализации». Конкретизация связи между свойством ИС и угрозой может быть получена исходя из использования в их названиях (очевидно, отражающих кратко их суть) общих элементов терминологического базиса предметной области, например, ключевых слов; конкретизация же связи между угрозой и последствием ее реализации – на основании различных баз угроз. Так, «Банк данных угроз безопасности информации» ФСТЭК России (Банк) содержит

в табличном виде такие характеристики угроз, как название и «флаги» нарушений конфиденциальности, целостности и доступности информации [5]; в самом же названии присутствуют слова, отражающие свойства ИС. Например, название 2-й угрозы из Банка звучит как «Угроза агрегирования данных, передаваемых в грид-системе», которая приводит только к нарушению конфиденциальности. Таким образом, ключевыми словами-элементами, на которых определена угроза и которые, соответственно, отражают особенности ИС, являются следующие: агрегирование, данные и грид-система. Следовательно, свойства агрегирования в ИС, обрабатываемые в ней данные и построение грид-вычислений вносят некоторый вклад только в нарушение конфиденциальности при реализации данной угрозы.

Подсчитав для каждого ключевого слова из названий количество использующих эти слова угроз, приводящих к каждому из нарушений, а затем, отранжировав полученные значения по убыванию, можно выделить наиболее «опасные» свойства ИС (тождественные в данном случае ключевым словам).

В аналитическом виде данный подход, применительно к Банку (с учетом его конкретной внутренней структуры), можно записать следующим образом.

Предположим, имеется следующая база данных с характеристиками угроз:

$$DB \equiv \bigcup T_i,$$

где DB (*аббр. от англ.* DataBase) – база данных угроз; T_i (*аббр. от англ.* Threat) – *i* угроза в базе (далее, без необходимости, нижний индекс «*i*» будет опускаться).

С каждой угрозой связан набор характеристик, часть из которых может быть использована в интересах подхода:

$$\begin{cases} T \equiv \langle T^N, T^R \rangle \\ T^R \equiv \langle T^C, T^I, T^A \rangle' \end{cases}$$

где T^N (*N – аббр. от англ.* Name) – название угрозы; T^R (*R – аббр. от англ.* Realization) – последствия реализации угрозы, состоящие из нарушений конфиденциальности T^C (*C – аббр. от англ.* Confidentiality), целостности T^I (*I – аббр. от англ.* Integrity) и доступности T^A (*A – аббр. от англ.* Availability).

Название угрозы состоит из последовательности слов, часть из которых является ключевой в терминологическом базисе и отражает ее суть (то есть существительные и прилагательные):

$$T^{Name} = \bigcup W_j^T,$$

где W_j^T (*W – аббр. от англ.* Word) – *j*-е ключевое слово, используемое в названии угрозы T.

Нарушения же являются булевскими флагами, то есть:

$$\begin{cases} T^C \in \{0,1\} \\ T^I \in \{0,1\}, \\ T^A \in \{0,1\} \end{cases}$$

где $\{0,1\}$ – множество булевских значений, состоящее из 0 для обозначения отсутствия нарушения и 1 для его наличия.

Таким образом, терминологический базис предметной области состоит из множества всех ключевых слов, используемых в названиях угроз:

$$\begin{cases} TB = \bigcup W_l = \bigcup W_{i,j}^T \\ \forall\, l1, l2, l1 \neq i2 \colon W_{l1} \neq W_{l2} \end{cases},$$

где TB (*аббр. от англ.* Terminology Basis) – терминологический базис определения; W_l – l-е слово из терминологического базиса; $W_{i,j}^T$ – j-е слово из названия i угрозы; а последняя запись в системе уравнений означает, что все W_l слова из базиса являются уникальными (то есть не может быть двух одинаковых слов).

Свойства ИС могут быть построены на том же терминологическом базисе, что и угрозы:

$$\begin{cases} \mathrm{IS} \equiv \langle \mathrm{IS}_\mathrm{k}^\mathrm{P} \rangle \\ \mathrm{IS}_\mathrm{k}^\mathrm{P} \in \mathrm{TB} \end{cases}, \quad (1)$$

где IS (*аббр. от англ.* Information System) – ИС, описываемая с помощью ее свойств; IS_k^P – k свойство ИС из терминологического базиса; P (*аббр. от англ.* Property) – атрибут свойства ИС. Таким образом, свойства ИС соответствуют элементам терминологического базиса (1).

Сама взаимосвязь между свойствами ИС, угрозами и последствиями их реализации, может быть записана следующим образом:

$$\forall l, \forall i (W_l \in T_i^N) \exists k (W_l = IS_k^P) : IS_k^P \to T_i \to T_i^R,$$

где «→» оператор взаимосвязи. Суть записи заключается в том, что каждое свойство ИС связано как со множеством угроз через ключевые слова в их названиях, так и с последствиями реализации этих угроз через соответствующую классическую триаду нарушений информационной безопасности, заданную в базе данных.

Прототип

Для решения задачи исследования был разработан программный прототип «Программа для ранжирования элементов терминологического базиса угроз информационной безопасности»[1] (прототип), позволяющий (как видно из названия) ранжировать слова в названии угроз и свойства ИС в зависимости от убывания количества, связанных с ними последствий реализации для всех угроз. Код прототипа написан на языке программирования Python с использованием библиотек pymorphy2, pandas и nltk; также на него подана заявка на получение свидетельства о регистрации программы для ЭВМ. Логика работы прототипа является линейной и состоит из следующих шагов:

Шаг 1. Загрузка характеристик угроз из внешнего Excel-файла во внутреннюю таблицу (с применением библиотеки pandas).

Шаг 2. Выделение в загруженной таблице необходимых столбцов с названием и последствиями реализации угроз.

Шаг 3. Токенизация[2] названий угроз путем их перевода в массив отдельных слов с отсечением знаков пунктуации (с применением библиотеки ntlk).

Шаг 4. Удаление из массива слов, не влияющих на суть угрозы – то есть всех, кроме ключевых, состоящих из существительных и прилагательных (с применением библиотеки pymorphy2).

Шаг 5. Перевод слов в нормализованную форму – то есть без склонений (с применением библиотеки pymorphy2).

Шаг 6. Сбор статистики касательно того, насколько каждое из токенизированных слов приводит к каждому из последствий (через соответствующее название угрозы).

Шаг 7. Ранжирование токенизированных слов по количеству связанных с ними последствий реализации угроз.

Шаг 8. Вывод на экран трех отранжированных списков (список).

[1] Подана заявка в Роспатент на государственную регистрацию программы для ЭВМ.

[2] Токенизация – *от англ.* token, разновидность жетона, заменявшая мелкие монеты; здесь иносказательно – замещение названий угроз на отдельные слова (токены).

Эксперимент

В качестве источника с описанием угроз был взят Банк, имеющий вид таблицы с 222 записями (на момент начала декабря 2023 г.). Применение прототипа к Банку позволило сформировать три списка из 417 слов, содержание которых для Топ-10 наиболее «опасных» свойств ИС (то есть слов из названий угроз с наибольшим количеством нарушений) приведено в таблице.

Таблица

Топ-10 (на сером фоне) наиболее «опасных» свойств ИС с позиции нарушений информационной безопасности

Рейтинг	Свойство ИС	Тип нарушения		
		конфиденциальность	целостность	доступность
	Ранжирование по нарушению конфиденциальности			
1	угроза	146	137	155
2	несанкционированный	31	30	28
3	доступ	24	15	19
4	информация	22	15	18
5	использование	21	16	16
6	виртуальный	17	14	18
7	данные	16	18	19
8	программный	11	16	11
9–10	управление	10	13	14
9–10	bios	10	14	10
…	…	…	…	…
12–14	сеть	9	6	8
…	…	…	…	…
296–417	входной	0	3	2
	Ранжирование по нарушению целостности			
1	угроза	146	137	155
2	несанкционированный	31	30	28
3	данные	16	18	19
4–5	программный	11	16	11
4–5	использование	21	16	16
6–7	доступ	24	15	19
6–7	информация	22	15	18
8–10	виртуальный	17	14	18
8–10	bios	10	14	10
8–10	обеспечение	10	14	12
…	…	…	…	…
22–25	сеть	9	6	8
…	…	…	…	…
48–69	входной	0	3	2
	Ранжирование по нарушению доступности			
1	угроза	146	137	155
2	несанкционированный	31	30	28
3–4	доступ	24	15	19
3–4	данные	16	18	19
5–6	виртуальный	17	14	18
5–6	информация	22	15	18
7	использование	21	16	16

Рейтинг	Свойство ИС	Тип нарушения		
		конфиденциальность	целостность	доступность
8	управление	10	13	14
9	система	8	12	13
10	облачный	9	10	12
…				
15–16	bios	10	14	10
…				
20–24	сеть	9	6	8
…	…	…	…	…
81–127	входной	0	3	2

Анализ ранжирования выделенных свойств ИС по различным последствиям реализации угроз (табл.) позволяет сделать некоторые предварительные выводы:

1. На первом месте во всех трех списках расположен элемент-слово «Угроза», что является закономерным, поскольку данное слово находится в каждом из названий угрозы в Банке. Тем не менее нарушения доступности выше, чем для конфиденциальности, у которой, в свою очередь, выше, чем для целостности. Впрочем, расхождения между статистикой ближайших нарушений составляет около 10 %, что говорит об отсутствии каких-либо качественных различий в них (с точки зрения предложенного подхода).

2. На втором месте во всех списках идет элемент-слово «Несанкционированный», что позволяет говорить об этом свойстве, как наиболее критичном во всей ИС [6]; отличия в расхождении статистики незначительные – менее 10 %. Следовательно, противодействие в части ограничения доступа и контроля над ним будет положительно влиять на все аспекты информационной безопасности.

3. На третьем месте в списках по нарушениям конфиденциальности и доступности идет элемент-слово «Доступ», что усиливает значимость расположенного ранее элемента «Несанкционированный». В списке же нарушения целостности третьим словом оказались «Данные»; следовательно, существует прямая (то есть достаточно сильная) связь между обработкой данных в ИС и угрозой их несанкционированного изменения. Необходимо отметить, что такая связь не является очевидной, поскольку, например, второй элемент таблицы хотя и содержит слово «Данные», однако он не оказывает влияния на нарушение их целостности.

4. В списках после третьего места одинаковые слова практически отсутствуют. Так, например, согласно четвертому элементу, нарушение конфиденциальности сильнее связано с информацией, целостности – с программной частью составляющих ИС, а доступности – с самими данными. Следовательно, практически все элементы оказывают уникальное влияние на возникающие нарушения.

5. Частный анализ нахождения довольно специфичного элемента-слова «bios» (предшественника UEFI, ответственного за прошивку оборудования [7]) показал его существенное влияние на конфиденциальность – 9–10-е место[3], а также целостность – 8–10-е место; при этом в списке нарушения доступности он расположен лишь на 15–16-ом. Следовательно, уязвимости (как правило) в программном обеспечении аппаратных составляющих, выполняемом до момента запуска основной операционной системы, сильнее влияют на утечку и изменение данных, менее затрагивая непрерывность доступа к ним.

6. Аналогичный анализ элемента-слова «Сеть», связанного с обеспечением масштабирования и коммуникаций любой ИС, дает следующий диапазон распределения

[3] Диапазонное (например, 9–10-е) значение места в рейтинге говорит о том, что несколько слов («управление» и «bios») имеют одинаковое (здесь – 10-е) значение в списке нарушений конкретного свойства (здесь – конфиденциальности)

по местам: в списке нарушения конфиденциальности – 12–14-е, целостности – 22–25-е, доступности – 23-е. Следовательно, информационные «бреши» в сети (как и попросту ее наличие в ИС) сильнее отразятся на утечке информации, чем на ее изменении или недоступности. Аналогичная ситуация наблюдается и для подвижных устройств (элемент-слово – «Мобильный»).

7. Одним из элементов, не оказывающих какого-либо существенного влияния на все три нарушения, является слово «Входной», означающее работу с поступающими данными в ИС или ее модули [8]. Участие элемента в названиях угроз приводит к трем нарушениям целостности и двум нарушениям доступности без затрагивания конфиденциальности. Следовательно, в ИС без обработки конфиденциальных данных риски, связанные с применением программно-аппаратного обеспечения, активно обрабатывающего потоки входных данных, будут невысокими.

Заключение

Работа посвящена вопросу взаимосвязи между сущностями области информационной безопасности на примере свойств ИС, ее угроз информационной безопасности и их реализации последствий. Для этого производится сбор статистики использования ключевых слов в названиях угроз из «Банка данных угроз безопасности информации» ФСТЭК России с позиции их приведения к нарушениям конфиденциальности, целостности и доступности. Данные ключевые слова отождествляются с отличительными атрибутами ИС (то есть ее свойствами), что и позволяет построить требуемые закономерности. Для автоматизации процесса разработано программное средство, по результатам применения которого сделан ряд содержательных выводов.

Основным научным результатом является подход к изучению взаимосвязей между сущностями предметной области на примере угроз информационной безопасности и реализации их последствий для отдельных свойств ИС. Новизна результата состоит в полном отсутствии субъективного мнения эксперта на этапе анализа описания угроз информационной безопасности ИС и получения взаимосвязей.

Теоретическая значимость заключается в переводе подхода в формализованную плоскость и установлении возможности его применения к другим сущностям; например, для выявления связей между аппаратными составляющими ИС и степенью опасности уязвимостей в них и т.д.

Практическая значимость состоит в получении прототипа, который позволяет формально выделять наиболее «опасные» свойства ИС с позиции различных последствий от связанных с ними угроз информационной безопасности, что, таким образом, указывает на ее наиболее критичные части.

Продолжением работы будет получение и изучение результатов применения подхода для других предметных областей информационной безопасности, в которых имеются соответствующие базы данных с описаниями сущностей.

Список источников

1. Таран А.А.В. Причины появления и распространения новых форм информационных угроз в обществе // Вопросы гуманитарных наук. 2009. № 3 (41). С. 273–276.

2. Информационные угрозы коммуникативного характера / Е.А. Еремина [и др.] // Психолого-педагогический журнал Гаудеамус. 2012. Т. 2. № 20. С. 124–125.

3. Каратунова Н.Г. Информационные угрозы в программном обеспечении // Экономика. Право. Печать. Вестник КСЭИ. 2016. № 2-3 (70-71). С. 155–159.

4. Петров С.Н., Пулко Т.А. Анализ баз общеизвестных уязвимостей информационной безопасности // Управление информационными ресурсами: материалы XIX Междунар. науч.-практ. конф. Минск, 2023. С. 251–252.

5. Акиншин А.А., Ляпичева Н.Г., Ильменский М.Д. Анализ базы угроз в сфере информационной безопасности на примере Банка угроз ФСТЭК России // Вестник ЦЭМИ. 2022. Т. 5. № 4. DOI: 10.33276/S265838870022995-7.

6. Третьяков О.П. Концептуальная модель адаптивной защиты информации от несанкционированного доступа // Программные продукты и системы. 2009. № 3. С. 45.

7. Израилов К.Е., Покусов В.В. Создание программной объектно-ориентированной платформы для разработки UEFI модулей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021): сб. науч. статей X Междунар. науч.-техн. и науч.-метод. конф. СПб., 2021. Т. 2. С. 246–250.

8. Порхун А.О., Гамаюнов Д.Ю. Фильтры обработки входных данных как источники уязвимостей в Веб-приложениях // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 59–63.

References

1. Taran A.A.V. Prichiny poyavleniya i rasprostraneniya novyh form informacionnyh ugroz v obshchestve // Voprosy gumanitarnyh nauk. 2009. № 3 (41). S. 273–276.

2. Informacionnye ugrozy kommunikativnogo haraktera / E.A. Eremina [i dr.] // Psihologo-pedagogicheskij zhurnal Gaudeamus. 2012. T. 2. № 20. S. 124–125.

3. Karatunova N.G. Informacionnye ugrozy v programmnom obespechenii // Ekonomika. Pravo. Pechat'. Vestnik KSEI. 2016. № 2-3 (70-71). S. 155–159.

4. Petrov S.N., Pulko T.A. Analiz baz obshcheizvestnyh uyazvimostej informacionnoj bezopasnosti // Upravlenie informacionnymi resursami: materialy XIX Mezhdunar. nauch.-prakt. konf. Minsk, 2023. S. 251–252.

5. Akinshin A.A., Lyapicheva N.G., Il'menskij M.D. Analiz bazy ugroz v sfere informacionnoj bezopasnosti na primere Banka ugroz FSTEK Rossii // Vestnik CEMI. 2022. T. 5. № 4. DOI: 10.33276/S265838870022995-7.

6. Tret'yakov O.P. Konceptual'naya model' adaptivnoj zashchity informacii ot nesankcionirovannogo dostupa // Programmnye produkty i sistemy. 2009. № 3. S. 45.

7. Izrailov K.E., Pokusov V.V. Sozdanie programmnoj ob"ektno-orientirovannoj platformy dlya razrabotki UEFI modulej // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2021): sb. nauch. statej X Mezhdunar. nauch.-tekhn. i nauch.-metod. konf. SPb., 2021. T. 2. S. 246–250.

8. Porhun A.O., Gamayunov D.Yu. Fil'try obrabotki vhodnyh dannyh kak istochniki uyazvimostej v Veb-prilozheniyah // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2015. № 4. S. 59–63.

Информация о статье:
Статья поступила в редакцию: 13.11.2023; одобрена после рецензирования: 09.12.2023;
принята к публикации: 11.12.2023
Information about the article:
The article was submitted to the editorial office: 13.11.2023; approved after review: 09.12.2023;
accepted for publication: 11.12.2023

Сведения об авторах:
Буйневич Михаил Викторович, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN-код: 9339-3750
Леонов Николай Викторович, начальник лаборатории Государственного научно-исследовательского института прикладных проблем (191167, Санкт-Петербург, наб. Обводного канала, д. 29), кандидат технических наук, доцент, e-mail: leonov-nv@yandex.ru, https://orcid.org/0000-0005-1295-5343
Хорошенко Виктория Сергеевна, аспирант кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (193232, Санкт-Петербург, пр-т Большевиков, 22/1), e-mail: xoroshenko.v@mail.ru, https://orcid.org/0000-0002-7268-0960, SPIN-код: 9705-9110

Information about the authors:
Buinevich Mikhail V., professor of the department of applied mathematics and information technologies of, Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022 SPIN: 9339-3750
Leonov Nikolay V., chief of the State research institute of applied problems laboratory (191167, Saint-Petersburg, Obvodny canal emb, 29), candidate of technical sciences, associate professor, e-mail: leonov-nv@yandex.ru, https://orcid.org/0000-0005-1295-5343
Khoroshenko Victoria S., postgraduate at the department of information systems security the of Bonch-Bruevich Saint-Petersburg state university of telecommunications (193232, Saint-Petersburg, Bolshevikov ave., 22/1), e-mail: xoroshenko.v@mail.ru, https://orcid.org/0000-0002-7268-0960, SPIN: 9705-9110