Научная статья
УДК 004.056.57
DOI: 10.17072/1993-0550-2023-1-77-83

О некоторых вопросах оценки опасности деструктивного воздействия вредоносных программ на автоматизированные системы

Николай Сергеевич Кобяков[1], Александр Владимирович Мельников[2], Сергей Николаевич Горячев[3]
[1, 3] Пермский военный институт войск национальной гвардии Российской Федерации, Пермь, Россия
[2] Воронежский институт Министерства внутренних дел Российской Федерации, Воронеж, Россия
[1] kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879
[2] meln78@mail.ru, https://orcid.org/0000-0001-5080-1162
[3] sergory@mail.ru, https://orcid.org/0000-0002-6994-8559

Аннотация. В работе рассматривается проблема оценки опасности деструктивного воздействия вредоносных программ на автоматизированные системы. Изучены классификация вредоносных программ и подходы к оценке опасности деструктивного воздействия. Произведен анализ существующих алгоритмов оценки опасности деструктивного воздействия, также определен показатель опасности вредоносных программ при эксплуатации нескольких уязвимостей.

Ключевые слова: *вредоносные программы; деструктивное воздействие; уязвимости; угрозы информационной безопасности; CVSS*

Для цитирования: *Кобяков Н. С., Мельников А. В., Горячев С. Н.* О некоторых вопросах оценки опасности деструктивного воздействия вредоносных программ на автоматизированные системы // Вестник Пермского университета. Математика. Механика. Информатика. 2023. Вып. 1(60). С. 77–83. DOI: 10.17072/1993-0550-2023-1-77-83.

Статья поступила в редакцию 29.11.2022; одобрена после рецензирования 27.01.2023; принята к публикации 16.03.2023.

Research article

About Some Consequences of Destructive Influence Software Virus for Automatic Systems

Nikolay S. Kobyakov[1], Alexander V. Melnikov[2], Sergei N. Goryachev[3]
[1, 3] Perm Military Institute of National Guard Troops, Perm, Russia
[2] Voronezh Institute of the Ministry of the Interior of Russia, Voronezh, Russia
[1] kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879
[2] meln78@mail.ru, https://orcid.org/0000-0001-5080-1162
[3] sergory@mail.ru, https://orcid.org/0000-0002-6994-8559

Abstract. The paper deals with the problem of assessing the danger of the destructive impact of malicious programs on automated systems. The classification of malicious programs and approaches to assessing the danger of destructive impact are studied. An analysis of existing algorithms for assessing the danger

of destructive impact was made, and an indicator of the danger of malware when exploiting several vulnerabilities was also determined.

Keywords: *malware; destructive impact; vulnerabilities; information security threats; CVSS*

For citation: *Kobyakov N. S., Melnikov A.V., Goryachev S. N.* About Some Consequences of Destructive Influence Software Virus for Automatic Systems. Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2023;1(60):77-83. (In Russ.). DOI: 10.17072/1993-0550-2023-1-77-83.

The article was submitted 29.11.2022; approved after reviewing 27.01.2023; accepted for publication 16.03.2023.

Введение

Для обеспечения информационной безопасности автоматизированных систем необходимо исключить угрозы безопасности информации, которые могут быть в ней реализованы. Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [1].

Для реализации деструктивных функций вредоносных программ необходимо использование уязвимостей. Уязвимость – это недостаток программного, программно-технического обеспечения информационной системы в целом, который может быть использован для реализации угроз безопасности информации [1].

В рамках данной работы осуществляется анализ вредоносных программ, подход к оценке опасности деструктивного воздействия вредоносных программ на автоматизированные системы, а также алгоритмов оценки уровня опасности эксплуатации уязвимостей. Результаты исследования будут использованы как исходные данные для дальнейших исследований, в том числе создания комплекса программ для оценки опасности деструктивного воздействия вредоносных программ на автоматизированные системы.

Рассмотрим классификацию и основные показатели вредоносных программ.

1. Вредоносные программы

Вредоносная программа: Программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы [2]. Реализация деструктивных функций программ направлена на нарушение конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки [3].

Конфиденциальность – это свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов [4]. Целостность – свойство сохранения правильности и полноты активов. Доступность – свойство быть доступным и готовым к использованию по запросу авторизованного субъекта. Неотказуемость – способность удостоверять имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение. Подотчетность – ответственность субъекта за его действия и решения. Аутентичность – свойство, гарантирующее, что субъект или ресурс идентичен заявленному. Достоверность – свойство соответствия предусмотренному поведению и результатам.

1.1. Развитие угроз безопасности информации

В третьем квартале 2022 г. решения "Лаборатории Касперского" предотвратили запуск одного или нескольких зловредов, предназначенных для кражи денежных средств с банковских счетов, на компьютерах 99 989 уникальных пользователей [5], рис. 1.

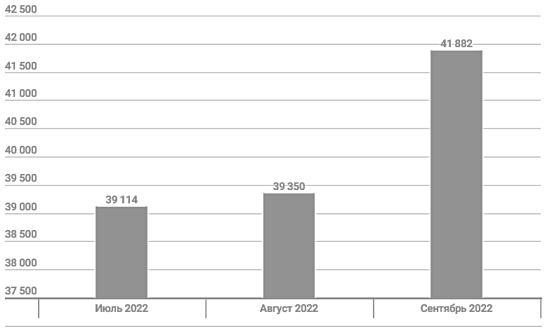

Рис. 1. *Количество уникальных пользователей, атакованных финансовыми зловредами*

В третьем квартале 2022 г. были обнаружены 17 новых семейств шифровальщиков и 14 626 новых модификаций зловредов этого типа. Из них более 11 тысяч получили вердикт Trojan-Ransom.Win32.Crypmod [5], рис. 2.

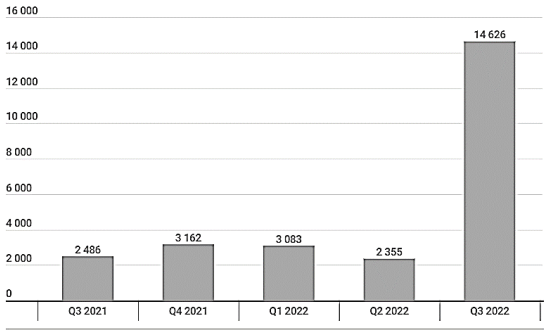

Рис. 2. *Количество новых модификаций*

В третьем квартале 2022 г. продукты и технологии "Лаборатории Касперского" защитили от атак шифровальщиков 72 941 пользователя [5], рис. 3.

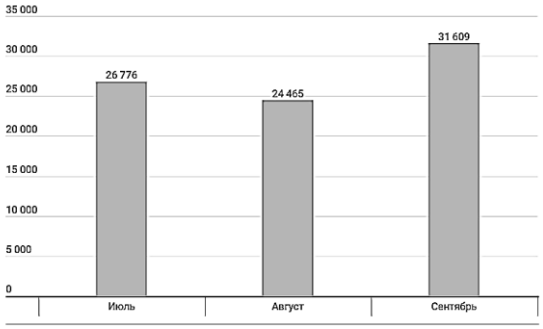

Рис. 3. *Количество пользователей, атакованных троянцами-шифровальщиками*

В третьем квартале 2022 г. решения "Лаборатории Касперского" обнаружили 153 773 новые модификации майнеров. Из них более 140 тысяч нашли в июле и августе, что в сочетании с результатом июня (более 35 тысяч новых модификаций) свидетельствует об аномально высокой летней активности создателей майнеров, рис. 4.

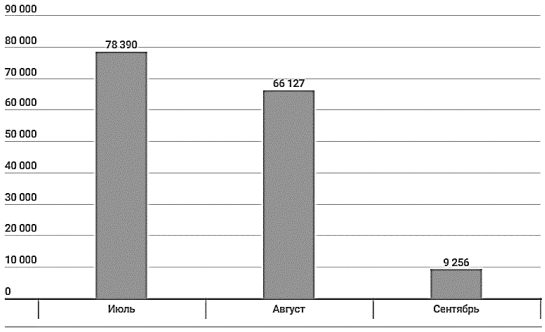

Рис. 4. *Количество новых модификаций майнеров*

В третьем квартале мы обнаружили атаки с использованием программ-майнеров на компьютерах 432 363 уникальных пользователей продуктов "Лаборатории Касперского" по всему миру. После спада, произошедшего в конце весны – начале осени, мы снова наблюдаем рост активности такого вида угроз [5], рис. 5.

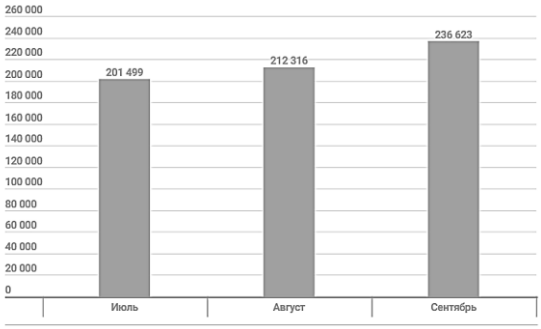

Рис. 5. *Количество пользователей, атакованных майнерами*

Таким образом, исходя из анализа развития угроз безопасности можно сделать вывод, что вредоносные программы развиваются с каждым днем, следовательно, необходимо совершенствовать средства защиты и способы их обнаружения.

В более ранних исследованиях [4, 6] были проведены исследования вредоносных программ. Исходя из результатов данных исследований укрупненными видами вредоносных программ с явно выраженными деструктивными функциями можно выделить: программы, способные к самораспространению (вирусы); программы, проникающие в компьютер под видом легитимного программного обеспечения (трояны); программы, самостоятельно распространяющиеся через локальные и глобальные компьютерные сети, программы, блокирующие доступ к компьютерной системе или предотвращающие считывание записанных в постоянном запоминающем устройстве данных (часто с помощью методов шифрования), а затем требующие от пользователя денежные средства для восстановления исходного состояния (шифровальщики) [6].

Вредоносные программы можно разделить на следующие группы:

1. По среде обитания:
   – файловые;
   – макро;
   – загрузочные;
   – сетевые.

2. По заражаемым операционным системам:
   – ВП, заражающая файлы одного типа ОС;
   – ВП, заражающая более одного типа ОС.
3. По особенностям алгоритма работы и в зависимости от сложности кода:
   – активизирующиеся при загрузке ОС;
   – резидентные;
   – файлы-двойники;
   – сетевые;
   – полиморфные.
4. По деструктивным возможностям:
   – направлены на изменение свойств файла конфиденциальности;
   – направлены на изменение свойств файла целостности;
   – направлены на изменение свойств файла доступности.
5. По использованию интернет-технологий:
   – Трояны;
   – HTML;
   – Java;
   – Черви.
6. По способу проникновения в систему:
   – распространяемые через внешние носители;
   – распространяемые через сеть;
   – по локальной сети;
   – по региональной сети;
   – по глобальной сети.

Все представленное в классификации вредоносные программы реализуют угрозы безопасности информации.

Угроза (безопасности информации): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [7].

В работе [6] предлагается классифицировать угрозы на следующие уровни:

Средний уровень – угрозы, направленные на предпосылки к внедрению вредоносных программ элементам автоматизированных систем;

Высокий уровень – угрозы, не обезвреженные на среднем уровне и направленные на предпосылки к инсталляции вредоносных программ на автоматизированных рабочих местах пользователей и серверов автоматизированных систем;

Критический уровень – угрозы, не обезвреженные на высоком уровне и направленные на нарушение целостности, доступности, конфиденциальности данных автоматизированных систем.

Данный подход к оценке опасности деструктивного воздействия вредоносных программ на автоматизированные системы может быть использован, но в нем отсутствуют численные характеристики оценки угроз для определения их опасности.

В банке данных угроз ФСТЭК [8] представлена информация об основных угрозах безопасности информации и уязвимостях. Кроме того, данный ресурс позволяет рассчитать с использованием CVSS метрик количественную оценку уязвимости. Различают CVSS версии 2.0 и версии 3.0, на рис. 6 представлено сравнение количественных оценок опасности уязвимостей CVSS v 2.0 и CVSS v 3.0.

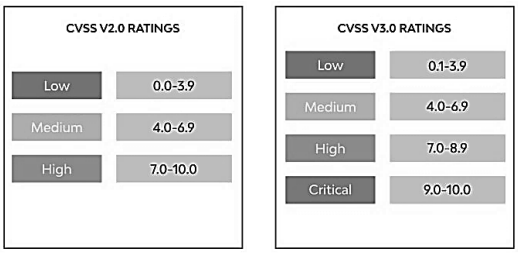

Рис. 6. *Сравнение CVSS v 3.0 и CVSS v 2.0*

Общая система оценки уязвимостей (CVSS) позволяет определить основные характеристики уязвимости и получить числовую оценку, отражающую ее серьезность. Затем числовой балл можно преобразовать в качественное представление (например: низкий, средний, высокий и критический), чтобы помочь организациям правильно оценить и расставить приоритеты в своих процессах управления уязвимостями [9].

2. Исследование оценки опасности деструктивного воздействия

В работе [10] проведено исследование, результатом которого стал алгоритм оценки относительного уровня опасности совместной эксплуатации уязвимостей информационной безопасности на основе CVSS v 2.0. В основе алгоритма лежат формулы расчета базовой, временной и контекстной оценки уровня опасности уязвимостей с нормировкой конечного результата и перехода к относительной шкале оценивания [10].

Пять этапов данного алгоритма раскрывают базовые, временные, контекстные метрики CVSS v 2.0.

На первом этапе пользователь проводит анализ объекта информатизации на наличие уязвимостей либо формирует запрос администратору безопасности некоторой информационной системы с указанием формы предоставления данных об уязвимостях. Формируется множество:

$$Y = \{y_1, y_2 \dots y_n\},$$

где $y_1, y_2 \dots y_n$ – уровень опасности каждой из уязвимостей [10].

На втором этапе определяются параметры уязвимости, которые обозначим следующим образом: I – влияние на свойства информации, $f(I)$ – значение функции от влияния на свойства информации, E – параметр эксплуатации уязвимости, e_1 – способ получения доступа, e_2 – сложность получения доступа, e_3 – аутентификация (множественная, единственная или не требуется), $\lambda_1, \lambda_2, \lambda_3$ – влияние уязвимости на конфиденциальность, целостность и доступность соответственно с целью присвоения базовой оценки уровня опасности B [10]. Рассчитывается базовая оценка уровня опасности анализируемой уязвимости по формуле (1):

$$B = \Big(\big((0.6 \times I) + (0.4 \times E) - 15\big) \times f(I)\Big). \quad (1)$$

На третьем этапе определяются параметры уязвимости с целью присвоения временной оценки T, t_1 – возможность использования, t_2 – уровень исправления доступа, t_3 – степень достоверности источника [10]. Производится расчет временной оценки по формуле (2):

$$T = (B \times t_1 \times t_2 \times t_3). \quad (2)$$

На четвертом этапе определяются параметры уязвимости с целью корректировки базовой и временной оценки с последующим присвоением контекстной оценки уровня опасности уязвимости φ, B' – скорректированная базовая оценка, z_1 – вероятность косвенного ущерба, z_2 – плотность целей, c_1, c_2, c_3 – требования к конфиденциальности, целостности и доступности соответственно [10]. Производится расчет контекстной оценки по формуле (3):

$$\varphi = \big((B' + (10 - B') \times z_1) \times z_2\big). \quad (3)$$

На пятом этапе происходит расчет общего относительного уровня опасности, формируется множество $X = \{x_0\, x_1, \dots x_n\}$, где $x_0 = 0$, а x_1,..., x_n – рассчитанный относительный уровень опасности уязвимостей [10]. Значение множества x является общим относительным уровнем опасности выявленных на объекте информатизации уязвимостей.

Расчет происходит согласно формуле (4):

$$x_i = (1 - x_{i-1}) \times \left({}^{y_i}/_{10}\right) + x_{i-1}, \text{где } i = 1, \dots, n. \quad (4)$$

Кроме того, данный алгоритм использует CVSS v 2.0, а сейчас более актуальным является CVSS v 3.0. В данной версии появились скорректированные базовые метрики, характеризующие эксплуатацию и потенциальный ущерб в условиях IT-инфраструктуры конкретной компании.

Стандарт CVSS v 3.0 позволяет описывать с помощью метрик цепочки уязвимостей, комбинируя характеристики эксплуатации одной уязвимости, с метриками воздействия другой [9]. К примеру:

Уязвимость 1 – Локальное повышение привилегий, не требующее взаимодействия с пользователем.

Уязвимость 2 – Уязвимость, позволяющая удаленному неаутентифицированному атакующему модифицировать файлы уязвимого компонента. Уязвимость требует от пользователя выполнения каких-либо действий для успешной эксплуатации, например, перехода по ссылке.

В случае если при эксплуатации уязвимости 2 возможно модифицировать файлы приложения так, чтобы это могло привести к эксплуатации уязвимости 1, – можно говорить о наличии цепочки уязвимостей со следующими характеристиками.

Подробное описание представлено в табл. 1.

Таблица 1. *Описание цепочки уязвимостей*

Уязвимость	Вектор CVSSv3.0	Оценка
Уязвимость 1	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	8.4
Уязвимость 2	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N	4.3
Уязвимость 2 —> Уязвимость 1	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

Алгоритм, представленный в работе [11] и методика стандарта CVSS v 3.0 позволяет рассчитать уровень опасности при последовательной эксплуатации уязвимостей, но не позволяет вычислить уровень опасности в следующих случаях:

1. Когда необходимо использование нескольких уязвимостей для реализации угроз безопасности информации.

2. Когда достаточно использование одной из нескольких уязвимостей для реализации угроз безопасности.

Для решения данных проблем необходимо вычислить показатель, который будет характеризовать совокупный уровень опасности, при реализации угроз безопасности информации, с использованием нескольких уязвимостей, уровень опасности уязвимостей будет определяться на основе CVSS v 3.0.

Формула для расчета данного показателя представлена в формуле (5):

$$M = 10\left(1 - \prod_{i=1}^{n} \frac{(10 - y_i)}{10}\right), \qquad (5)$$

где y_i – опасность уязвимости.

Результаты вычислений для различных уязвимостей представлены в табл. 2.

Таблица 2. *Результаты вычислений*

№ п/п		Опасности уязвимости	Значение показателя
	Для 2 уязвимостей		
1.		8.0	9
2.		5.0	
	Для 3 уязвимостей		
1.		8.4	9.891
2.		4.3	
3.		8.8	
	Для 4 уязвимостей		
1.		8.0	9.235
2.		5.0	
3.		1.0	
4.		1.5	

Таким образом, определенный показатель характеризует совокупный уровень опасности при реализации угроз безопасности информации, с использованием любого количества уязвимостей.

Кроме того, для определения значения совокупного уровня опасности будет использован CVSS v 3.0.

Заключение

В данной статье рассмотрены вопросы классификации вредоносных программ, угроз безопасности информации. Изучены алгоритмы оценки опасности совместной эксплуатации уязвимостей информационной безопасности. Определен показатель, характеризующий уровень опасности, при реализации угроз безопасности информации, с использованием нескольких уязвимостей. Определены исходные данные и средства для дальнейших исследований.

Список источников

1. *ГОСТ Р* 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.
2. *ГОСТ Р* 51275-2006 Защита информации объект информатизации. Факторы, воздействующие на информацию.
3. *ГОСТ* Р 53113.1- 2008 Информационная технология защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1: общие положения.
4. *Горячев С.Н.* Оценка состояния защищенности информационных систем от вредоносных программ / С. Н. Горячев, Н. С. Кобяков // Безопасность информационных технологий. 2022. Т. 29. № 1. С. 44–56. DOI: 10.26583/bit.2022.1.05.
5. *Развитие* информационных угроз в третьем квартале 2022 года. Статистика по ПК. URL: https://securelist.ru/it-threat-evolution-in-q3-2022-non-mobile-statistics/106077/ (дата обращения: 16.10.2022).
6. *Горячев С.Н.* Анализ деструктивных функций и процессов реализации угроз вредоносных программ на ИС органов внутренних дел / С. Н. Горячев, Н. С. Кобяков // Защита информации. Инсайд. 2022. № 2(104). С. 42–45.
7. *ГОСТ* Р 53114-2008 Защита информации обеспечение информационной безопасности в организации основные термины и определения.
8. *Банк* данных угроз ФСТЭК URL: https://bdu.fstec.ru (дата обращения: 16.10.2022).
9. *Common* Vulnerability Scoring System SIG URL: https://www.first.org/cvss/ (дата обращения: 24.11.2022).

10. *Мельников А.В.* Алгоритм оценки относительного уровня опасности совместной эксплуатации уязвимостей информационной безопасности на основе CVSS / А.В. Мельников, В.Е. Чирков // Вестник Воронежского института МВД России. 2019. №1. С. 37–44.
11. *Оценка* уязвимостей CVSS 3.0 URL: https://www.securitylab.ru/analytics/474648.php (дата обращения: 24.11.2022).

References

1. *GOST R* 56545-2015 Zashchita informacii. Uyazvimosti informacionnyh sistem. Pravila opisaniya uyazvimostej. (In Russ.).
2. *GOST* R 51275-2006 Zashchita informacii ob"ekt informatizacii. Faktory, vozdejstvuyushchie na informaciyu. (In Russ.).
3. *GOST* R 53113.1- 2008 Informacionnaya tekhnologiya zashchita informacionnyh tekhnologij i avtomatizirovannyh sistem ot ugroz informacionnoj bezopasnosti, realizuemyh s ispol'zovaniem skrytyh kanalov. Ch. 1: obshchie polozheniya. (In Russ.).
4. *Goryachev S.N., Kobyakov. N.S.* Ocenka sostoyaniya zashchishchennosti informacionnyh sistem ot vredonosnyh program. Bezopasnost' informacionnyh tekhnologij. 2022;(29(1):44-56. (In Russ.). DOI: 10.26583/bit.2022.1.05.
5. *Razvitie* informacionnyh ugroz v tret'em kvartale 2022 goda. Statistika po PK URL: https://securelist.ru/it-threat-evolution-in-q3-2022-non-mobile-statistics/106077/ (data obrashcheniya: 16.10.2022). (In Russ.).
6. *Goryachev S.N., Kobyakov. N.S.* Analiz destruktivnyh funkcij i processov realizacii ugroz vredonosnyh programm na IS organov vnutrennih del. Zashchita informacii. Insajd. 2022;(2(104)):42-45. (In Russ.).
7. *GOST* R 53114-2008 Zashchita informacii obespe-chenie informacionnoj bezopasnosti v organizacii osnovnye terminy i opredeleniya (In Russ.).
8. *Bank* dannyh ugroz FSTEK URL: https://bdu.fstec.ru (data obrashcheniya: 16.10.2022). (In Russ.).
9. *Common* Vulnerability Scoring System SIG URL: https://www.first.org/cvss/ (data obrashcheniya: 24.11.2022). (In Russ.).
10. *Mel'nikov, A.V., Chirkov V.E.* Algoritm ocenki otnositel'nogo urovnya opasnosti sovmestnoj ekspluatacii uyazvimostej informacionnoj bezopasnosti na osnove CVSS. Vestnik Voronezhskogo instituta MVD Rossii. 2019;(1):37-44. (In Russ.).
11. Ocenka uyazvimostej CVSS 3.0 URL: https://www.securitylab.ru/analytics/474648.php (data obrashcheniya: 24.11.2022). (In Russ.).

Информация об авторах:

Н. С. Кобяков – начальник учебной лаборатории технической защиты информации кафедры вычислительных машин, комплексов, систем и сетей факультета связи, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д. 1), AuthorID: 1126165;

А. В. Мельников – доктор технических наук, доцент, профессор кафедры автоматизированных систем, Воронежский институт МВД России (394065, Россия, г. Воронеж, пр. Патриотов, д. 53), AuthorID: 771294;

С. Н. Горячев – начальник кафедры вычислительных машин, комплексов, систем и сетей факультета связи, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д. 1), AuthorID: 993073.

Information about the authors:

N. S. Kobyakov – Head of the Educational Laboratory of Technical Information Protection, Department of Computers, Complexes, Systems and Networks, Faculty of Communications, Perm Military Institute of National Guard Troops (1 Gremyachy Log Street, Perm, Russia, 614112), AuthorID: 1126165;

A. V. Melnikov – Doctor of Technical Sciences, Associate Professor, Professor of the Department of Automated Systems, Voronezh Institute of the Ministry of Internal Affairs of Russia (53 Patriotov Ave., Voronezh, Russia, 394065), AuthorID: 771294;

S. N. Goryachev – Head of the Department of Computers, Complexes, Systems and Networks, Faculty of Communications, Perm Military Institute of National Guard Troops (1 Gremyachy Log Street, Perm, Russia, 614112), AuthorID: 993073.