Ирина Г. Дровникова[1], Елена С. Овчинникова[2]
[1,2]Воронежский институт министерства внутренних дел Российской Федерации,
пр-кт Патриотов, 53, Воронеж, 394065, Россия
[1]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524

ОБОСНОВАНИЕ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПРОВЕДЕНИЯ НАТУРНОГО ЭКСПЕРИМЕНТА

DOI: http://dx.doi.org/10.26583/bit.2021.3.02

Аннотация. Целью статьи является обоснование законов распределения времени на различных этапах реализации сетевых атак в защищенных автоматизированных системах органов внутренних дел. Для достижения поставленной цели применен метод натурного эксперимента по исследованию динамики протекания информационного конфликта «Сетевая атака – система защиты» с учетом различий изначальных и потенциальных возможностей конфликтующих сторон на основе разработанной обобщенной графовой модели. Результаты натурного эксперимента представлены в виде количественных значений времен запуска и реализации типовой сетевой атаки, воздействующей на информационные ресурсы и элементы защищенной автоматизированной системы органов внутренних дел, времен загрузки и функционирования системы защиты информации от несанкционированного доступа. Рассчитано количество итераций экспериментов, проводимых над сетевой атакой и системой защиты, достаточное для адекватного обоснования законов распределения времени на различных этапах конфликтного взаимодействия. Для обоснования нормального закона распределения времени на начальном этапе протекания информационного конфликта использован χ^2-критерий К. Пирсона, а для обоснования экспоненциального закона на последующем его этапе – λ-критерий А.Н. Колмогорова. Результаты эмпирического распределения значений времен реализации сетевой атаки и функционирования системы защиты представлены в табличной форме и наглядно отображены графически. Знание законов распределения позволит разработать аналитическую модель информационного конфликта «Сетевая атака – система защиты» на основе графовой модели динамики реализации типовой сетевой атаки и обобщенной графовой модели динамики протекания конфликта. Перспективы использования разработанной аналитической модели связаны с расчетом вероятностно-временных характеристик и проведением точной количественной оценки опасности реализации сетевых атак в автоматизированных системах, эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел.

Ключевые слова: сетевая атака, система защиты информации от несанкционированного доступа, информационный конфликт, натурный эксперимент, закон распределения времени.
Для цитирования: ДРОВНИКОВА, Ирина Г.; ОВЧИННИКОВА, Елена С. ОБОСНОВАНИЕ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПРОВЕДЕНИЯ НАТУРНОГО ЭКСПЕРИМЕНТА. Безопасность информационных технологий, [S.l.], т. 28, №. 3, с. 28–43, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1360. DOI: http://dx.doi.org/10.26583/bit.2021.3.02.

Irina G. Drovnikova[1], Elena S. Ovchinnikova[2]
[1,2]Voronezh Institute of the Ministry of the Interior,
Prospect Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524

Justification of network attacks time distribution in automated systems of internal affairs bodies based on a full-scale experiment

DOI: http://dx.doi.org/10.26583/bit.2021.3.02

Abstract. The goal of the paper is to substantiate the laws of time distribution at various stages of the implementation of network attacks in protected automated systems of internal affairs bodies. To achieve this goal, a full-scale experiment to study the dynamics of the "Network attack-protection system" information conflict was carried on taking into account the differences in the initial and potential capabilities of the conflicting parties on the basis of the developed generalized graph model. The results of the full-scale experiment are presented in the form of quantitative values of the start and implementation times of typical network attack affecting information resources and elements of a protected automated system of internal affairs bodies, the times of loading and functioning of the information protection system. The number of iterations of experiments with a network attack and security system sufficient for an adequate justification of the laws of time distribution at various stages of conflict interaction is calculated. To justify the normal law of time distribution at the initial stage of the information conflict, the χ^2-criterion of K. Pearson was used, while to justify the exponential law at its subsequent stage the λ-criterion of A.N. Kolmogorov was used. The results of the empirical distribution of the values of the time of the implementation of a network attack and the functioning of the protection system are presented in tabular form and graphically displayed. Knowledge of the distribution laws will allow us to develop an analytical model of the"Network attack-protection system" information conflict based on a graph of the dynamics of the implementation of a typical network attack and a generalized graph of the dynamics of the conflict. The prospects of using the developed analytical model are associated with the calculation of probabilistic-temporal characteristics and an accurate quantitative assessment of the danger of implementing network attacks in automated systems operated in a protected version at the informatization objects in internal affairs bodies.

Keywords: network attack, information protection system against unauthorized access, information conflict, full-scale experiment, law of time distribution.

For citation: DROVNIKOVA, Irina G.; OVCHINNIKOVA, Elena S. Justification of network attacks time distribution in automated systems of internal affairs bodies based on a full-scale experiment. IT Security (Russia), [S.l.], v. 28, n. 3, p. 28–43, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1360. DOI: http://dx.doi.org/10.26583/bit.2021.3.02.

Введение

Получение точных количественных оценок опасности угроз удаленного несанкционированного доступа (НСД), реализуемых посредством сетевых атак в автоматизированных системах (АС), эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД), в соответствии с требованиями международных и отраслевых стандартов Российской Федерации[1,2,3], нормативных и методических документов ФСТЭК России[4,5,6] и руководящих документов МВД России, посвященных вопросам информационной безопасности АС[7], приводит к необходимости разработки аналитической модели оценки вероятности реализации сетевых атак в защищенных АС ОВД. Построение такой модели подразумевает обоснование закона распределения времени реализации сетевых атак.

Проведенный анализ открытых литературных источников, посвященных данной

[1]ISO/IEC 15408-2012. Common Criteria for Information Technology Security Evaluation.
[2]ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении.
[3]ГОСТ 34.601-90. Автоматизированные системы. Стадии создания.
[4]ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
[5]ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
[6]ФСТЭК России. Методический документ. Методика оценки угроз безопасности информации. (утв. ФСТЭК России 5 февраля 2021 г.).
[7]Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169.

проблеме, позволяет констатировать, что при разработке аналитической модели закон распределения времени реализации сетевых атак в АС традиционно полагается экспоненциальным [1–4]. При этом процесс реализации атаки рассматривается либо независимо от функционирования системы защиты информации (СЗИ) от НСД в АС [1, 2], либо принимается допущение, что в конфликтном взаимодействии изначальные возможности сторон равны и конфликтные действия начинаются ими одновременно [3, 4], что в реальной практике эксплуатации защищенных АС ОВД выполняется крайне редко [5–7].

В данной статье представлено обоснование различных законов распределения времени в процессе поэтапной реализации типовых сетевых атак в защищенных АС ОВД, основанное на проведении экспериментального исследования динамики их конфликтного взаимодействия с СЗИ от НСД с учетом различий изначальных и потенциальных возможностей конфликтующих субъектов.

1. Постановка задачи

Процесс обоснования распределения времени реализации типовых сетевых атак на основе проведения экспериментального исследования динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД» в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, включает следующие этапы:

1. Построение обобщенной графовой модели динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД» в АС ОВД с выделением основных этапов конфликтного взаимодействия.
2. Проведение натурного эксперимента и представление его результатов в табличной форме в виде количественных значений времен запуска и реализации сетевой атаки, времен загрузки и функционирования СЗИ от НСД на основе разработанной модели.
3. Расчет достаточного количества итераций экспериментов, проводимых над сетевой атакой и СЗИ от НСД на различных этапах их конфликтного взаимодействия в АС ОВД.
4. Обоснование законов распределения времени реализации сетевой атаки и функционирования СЗИ от НСД на различных этапах их конфликтного взаимодействия на основе χ^2-критерия К. Пирсона и λ-критерия А.Н. Колмогорова с достаточностью 0,05.
5. Графическое представление количества реализаций сетевой атаки и функционирований СЗИ от НСД в защищенной АС ОВД в зависимости от времени для основных этапов обобщенной графовой модели динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД».

2. Метод исследования

Методом исследования является натурный эксперимент, описывающий динамику протекания информационного конфликта «Сетевая атака – СЗИ от НСД» в АС ОВД. Для его проведения был развернут лабораторный стенд, состоящий из сервера и трех автоматизированных рабочих мест (АРМ) со следующими характеристиками: процессор Intel Core i3-2100 с тактовой частотой 3.1 ГГц, оперативная память (ОЗУ) 4 Гб, дисковая память (HDD) 500 Гб, функционирующими под управлением 32-разрядной операционной системы (ОС) Windows 7. Вне локальной сети на отдельном персональном компьютере (ПК) установлена ОС Kali Linux с целью реализации деструктивных воздействий в виде сетевых атак.

Практическая составляющая поэтапного удаленного НСД к информационным

ресурсам и элементам защищенной АС ОВД реализовалась в виде скриптов, написанных на языке Bash. Запуск данных скриптов проводился с ПК, функционирующего под управлением ОС Kali Linux, посредством разработанного для каждого типа атаки программного кода.

Инсталляция и настройка СЗИ от НСД в АС ОВД основывались на рекомендациях разработчика. При этом была развернута полная версия СЗИ от НСД на трех АРМ и совместно с нею установлено прикладное программное обеспечение в виде пакета Microsoft Office 13 и антивируса «Kaspersky». В качестве СЗИ от НСД использована широко применяемая в АС ОВД СЗИ от НСД «Dallas Lock 8.0-С»[8], являющаяся сертифицированным программным комплексом средств защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну, в локальных и сетевых АРМ под управлением ОС семейства Windows с возможностью подключения аппаратных идентификаторов.

3. Модель и результаты исследования

Для обеспечения успешности реализации сетевой атаки или защиты информационных ресурсов и элементов АС ОВД необходимо оценить возможности обеих сторон в информационном конфликте «Сетевая атака – СЗИ от НСД». На рис. 1 приведена предложенная в [8] обобщенная графовая модель динамики протекания указанного конфликта в виде ориентированного графа состояний и переходов моделирующего его конечного полумарковского процесса (КПМП) с выделением основных этапов взаимодействия конфликтующих субъектов.

В качестве изначальных возможностей конфликтующих сторон, по которым осуществляется их сравнение в представленной графовой модели для определения начальных условий конфликта, рассматриваются производительности и объемы памяти сетевой атаки и СЗИ от НСД, определяемые в ходе проведения натурного эксперимента.

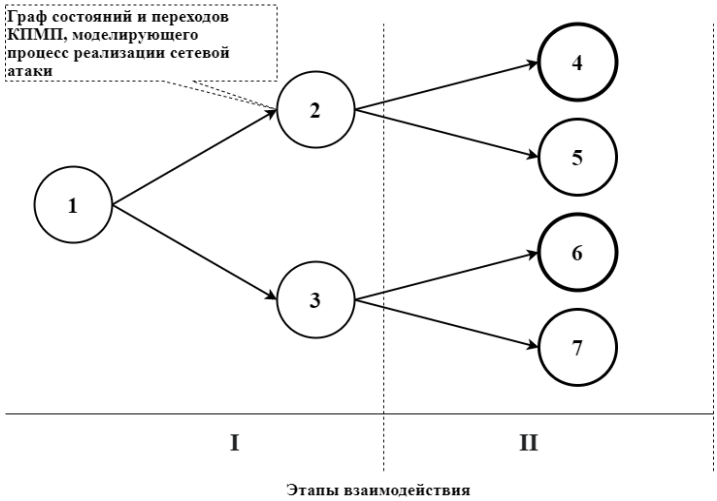
В [9–12] определены и проанализированы восемь наиболее опасных и часто реализуемых в настоящее время (типовых) сетевых атак, воздействующих на информационные ресурсы и элементы защищенных АС ОВД. Для каждой из указанных атак осуществлено обоснование распределения времени ее реализации в АС ОВД на основе эмпирических данных натурного эксперимента. Полученные результаты представлены на примере одной из типовых атак – парольной атаки.

Для расчета достаточного количества итераций N экспериментов, проводимых над сетевой атакой и СЗИ от НСД, с целью адекватного обоснования законов распределения времени на различных этапах их конфликтного взаимодействия в АС ОВД использована формула [13, 14]:

$$N = \frac{t_\varphi{}^2 \sigma^2}{\varepsilon^2}, \quad (1)$$

где: t_φ – квантиль нормального распределения вероятностей порядка $\varphi = \frac{1+Q}{2}$ (находится в таблицах Лапласа); Q – достоверность оценки; $\sigma = \sqrt{D}$ – среднеквадратическое отклонение исследуемых времен; $D = \sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2$ – дисперсия; $n = 10$ – объем первоначальной выборки; ε – заданная точность (достаточность) решения.

[8]Система защиты информации от несанкционированного доступа «Dallas Lock 8.0». Руководство по эксплуатации. URL: https://dallaslock.ru/upload/medialibrary/cp/documents/C%20ИК5%202017/RU.48957919. 501410-02%2092%20Руководство%20по%20 эксплуатации.pdf. Яз. рус. (дата обращения: 11.04.2021).



1 – производительности и объемы памяти сетевой атаки и СЗИ от НСД заданы;
2 – сетевая атака изначально имеет преимущество;
3 – СЗИ от НСД изначально имеет преимущество;
4, 6 – финальные состояния: победа сетевой атаки;
5, 7 – финальные состояния: победа СЗИ от НСД.

I этап – определение начальных условий конфликта;
II этап – процесс конфликтного взаимодействия сетевой атаки и СЗИ от НСД.

Рис. 1. Обобщенная графовая модель динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД»
Fig. 1. Generalized graph model of the dynamics of the information conflict "Network attack – SPI from NSD"

Результаты расчета достаточного количества итераций экспериментов, проводимых над сетевой атакой на первом этапе конфликтного взаимодействия ($\varepsilon = 0{,}05$) приведены в табл. 1, где x_i – эмпирические значения времен запуска сетевой атаки (получены в результате проведения натурного эксперимента).

Таблица 1. Результаты расчета достаточного количества итераций экспериментов над сетевой атакой на первом этапе конфликтного взаимодействия с СЗИ от НСД

x_i, с	$\overline{x_i}$, с	D	σ	N
15,016	15,0094	0,013505	0,116211	≈ 21
15,02				
15,015				
15				
14,699				
15,171				
15,039				
15,015				
15,003				
15,116				

Адекватные результаты эксперимента, проведенного 21 раз, представлены в табл. 2. Приведенные в табл. 2 характеристики позволили определить и обосновать закон распределения времени реализации сетевой атаки на первом этапе конфликтного взаимодействия (x_i – количественные значения случайных времен реализации атаки на

первом этапе, n_i – количественные значения соответствующих частот их появления).

Предполагая, что распределение времени реализации сетевой атаки на первом этапе соответствует нормальному закону, проведено доказательство согласования полученного эмпирического распределения с законом нормального распределения. Нормальное распределение имеет место в случае, когда формирование времен реализации сетевой атаки подвержено влиянию бесконечного числа случайных факторов.

Таблица 2. Расчетная таблица нахождения критерия $x^2_{\text{набл}}$ для процесса реализации сетевой атаки на первом этапе конфликтного взаимодействия с СЗИ от НСД

x_i, с	n_i	n'_i	$n_i - n'_i$	$(n_i - n'_i)^2$	$(n_i - n'_i)^2/n_i$
14,8	1	0,763640583	0,236359417	0,055865774	0,073157157
14,9	3	2,738242592	0,261757408	0,068516941	0,025022232
15	5	5,508436673	-0,508436673	0,25850785	0,04692944
15,1	6	6,128295556	-0,128295556	0,01645975	0,002685861
15,2	4	3,94281372	0,05718628	0,003270271	0,000829426
15,3	2	1,402670359	0,597329641	0,3568027	0,254373879
					$x^2_{\text{набл}} = 0{,}402997994$

В рассматриваемом информационном конфликте такими факторами являются производительности и объемы памяти сетевой атаки и СЗИ от НСД, влияние которых отчетливо прослеживается на начальном этапе протекания конфликта, когда время конфликтного взаимодействия напрямую зависит от входных параметров обеих сторон. С учетом вышеизложенного для первого этапа необходимо проверить нулевую гипотезу H_0: генеральная совокупность распределена по нормальному закону.

Проверка гипотезы о предполагаемом нормальном распределении проводилась с использованием критерия согласия: x^2 («хи квадрат») К. Пирсона (то есть при помощи специально подобранной случайной величины) [15]. Для этого сравнивались эмпирические значения частот n_i (наблюдаемые в ходе проведения эксперимента) и их теоретические значения n'_i (вычисляемые в предположении нормального распределения). x^2-критерий Пирсона не доказывает справедливость гипотезы, а устанавливает согласие или несогласие с данными наблюдений на принятом уровне значимости.

Критерий проверки нулевой гипотезы, определяемый случайной величиной, имеет вид:

$$x^2_{\text{набл}} = \sum (n_i - n'_i)^2 / n'_i. \quad (2)$$

Чем меньше различия эмпирических и теоретических частот, тем меньше полученная величина критерия. Доказано, что при $n \to \infty$ закон распределения случайной величины независимо от того, какому закону распределения подчинена генеральная совокупность, стремится к закону распределения x^2 с k степенями свободы, где: $k = s - 1 - r$; s – число групп выборки; r – число параметров выборки.

Односторонний критерий с большей вероятностью, чем двусторонний отклоняет нулевую гипотезу, поэтому исходя из требования вероятности P попадания критерия в исследуемую область с уровнем значимости ε строилась правосторонняя критическая область:

$$P\left[x^2_{\text{набл}} > x^2_{\text{кр}}(\varepsilon;\ k)\right] = \varepsilon, \quad (3)$$

где: $x^2_{\text{набл}}$ – значение критерия, вычисляемое по данным наблюдений.

Таким образом, для того чтобы при заданном уровне значимости проверить нулевую гипотезу H_0: генеральная совокупность распределена нормально, необходимо

сначала вычислить теоретические частоты, затем – наблюдаемое значение критерия $x^2_{\text{набл}}$ по формуле (2) и далее по таблице критических точек распределения x^2 для заданного уровня значимости ε и числа степеней свободы k найти критическую точку $x^2_{\text{кр}}(\varepsilon; k)$.

При $x^2_{\text{набл}} < x^2_{\text{кр}}$ нулевая гипотеза подтверждается (n_i и n'_i различаются незначимо – случайно), в противном случае – отвергается (n_i и n'_i различаются значимо).

Для процесса реализации сетевой атаки на первом этапе ее конфликтного взаимодействия с системой защиты алгоритм расчетов по полученным эмпирическим данным, представленным в табл. 2, имеет вид [15]:

1) методом произведений вычисляются выборочная средняя ($\overline{x_{\text{в}}} = 15{,}07142857$) и выборочное среднее квадратичное отклонение ($\sigma_{\text{в}} = 0{,}131449274$);

2) рассчитываются теоретические значения частот n'_i по формуле:

$$n'_i = \frac{nh}{\sigma_{\text{в}}} \cdot \varphi(u_i),$$

где $n = \sum n_i$ – объем выборки ($n = 21$), h – шаг ($h = 0{,}1$), $u_i = \frac{x_i - \overline{x_{\text{в}}}}{\sigma_{\text{в}}}$, $\varphi(u_i) = \frac{1}{\sqrt{2\pi}} e^{-u_i^2/2}$;

3) с помощью x^2-критерия Пирсона сравниваются эмпирические и теоретические значения частот:

– составляется расчетная табл. 2 для вычисления наблюдаемого значения критерия $x^2_{\text{набл}}$;

– по таблице критических точек распределения x^2 [15] для уровня значимости $\varepsilon = 0{,}05$ и числа степеней свободы $k = 6 - 1 - 2 = 3$ обозначается критическая точка правосторонней критической области $x^2_{\text{кр}}(0{,}05; 3) = 7{,}8$ (в рассматриваемом случае $s = 6$ и для предполагаемого нормального распределения $r = 2$, поскольку оцениваются два параметра – математическое ожидание и среднее квадратичное отклонение).

Выполнение неравенства $x^2_{\text{набл}} < x^2_{\text{кр}}$ подтверждает нулевую гипотезу H_0 о предполагаемом нормальном законе распределения времени реализации сетевой атаки на первом этапе конфликтного взаимодействия.

График распределения количества реализаций рассматриваемой сетевой атаки в зависимости от времени на первом этапе конфликтного взаимодействия с системой защиты представлен на рис. 2.

Результаты расчета по формуле (1) достаточного количества итераций экспериментов, проводимых над СЗИ от НСД с целью адекватного обоснования закона распределения времени на первом этапе конфликтного взаимодействия с сетевой атакой в АС ОВД ($\varepsilon = 0{,}05$) [13, 14], представлены в табл. 3, где x_i – эмпирические значения времен загрузки системы защиты (получены в результате проведения натурного эксперимента).

Адекватные результаты эксперимента, проведенного 17 раз, представлены в табл. 4. Приведенные в табл. 4 характеристики позволили определить и обосновать закон распределения времени функционирования системы защиты на первом этапе конфликтного взаимодействия (x_i – количественные значения случайных времен функционирования СЗИ от НСД на первом этапе, n_i – количественные значения соответствующих частот их появления).

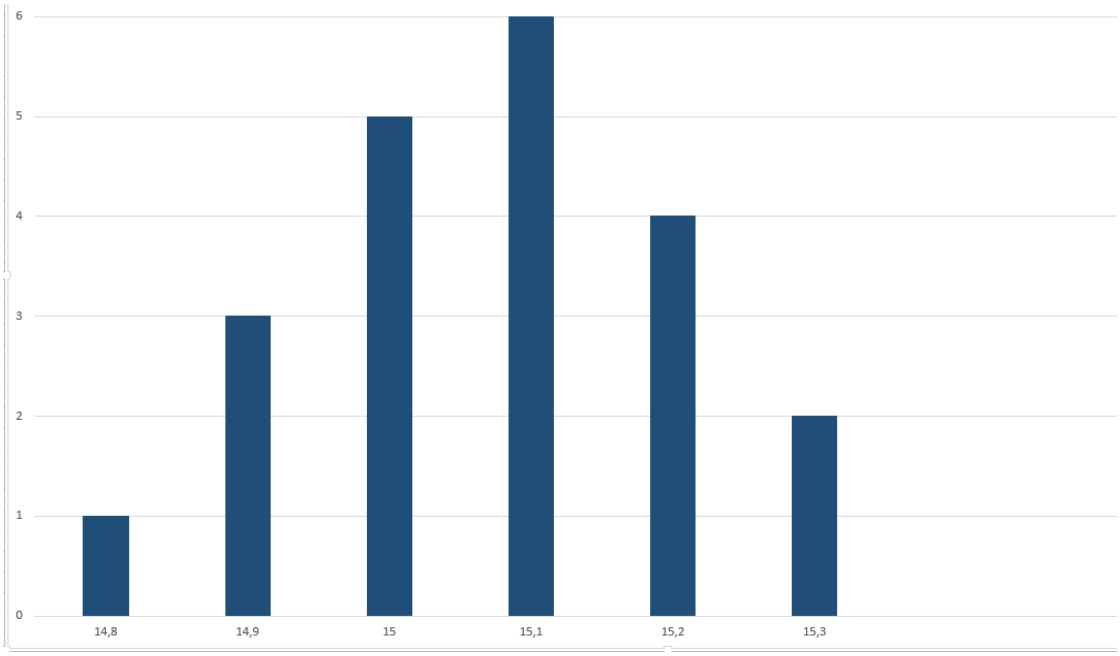


Рис. 2. График распределения количества реализаций сетевой атаки в зависимости от времени на первом этапе конфликтного взаимодействия с СЗИ от НСД
Fig. 2. Time distribution of the number of network attack implementations at the first stage of conflict interaction with the SPI from the NSD

Таблица 3. Результаты расчета достаточного количества итераций экспериментов над СЗИ от НСД на первом этапе конфликтного взаимодействия с сетевой атакой

x_i, с	$\overline{x_i}$, с	D	σ	N
1,71	1,732	0,010836	0,104096109	≈ 17
1,7				
1,89				
1,7				
1,61				
1,9				
1,83				
1,63				
1,6				
1,75				

Предполагая, что распределение времени функционирования СЗИ от НСД на первом этапе соответствует нормальному закону, проведено доказательство согласования полученного эмпирического распределения с законом нормального распределения с использованием критерия К. Пирсона аналогично первому этапу конфликтного взаимодействия при реализации сетевой атаки [15]. Результаты расчетов, проведенных по указанному выше алгоритму для $n = 17$, представлены в табл. 4.

По табл. 4 критических точек распределения x^2 [14] для уровня значимости ε = 0,05 и числа степеней свободы $k = 7 - 1 - 2 = 4$ обозначается критическая точка правосторонней критической области $x^2_{\text{кр}}(0{,}05;\ 4) = 9{,}5$ (в рассматриваемом случае $s = 7$, $r = 2$).

Таблица 4. Расчетная таблица нахождения критерия $x^2_{\text{набл}}$ для процесса функционирования СЗИ от НСД на первом этапе конфликтного взаимодействия с сетевой атакой

x_i	n_i	n'_i	$n_i - n'_i$	$(n_i - n'_i)^2$	$(n_i - n'_i)^2/n_i$
1,5	1	0,50209144	0,49790856	0,247912934	0,493760528
1,6	2	1,547841802	0,452158198	0,204447036	0,132085227
1,7	2	3,194132906	-1,194132906	1,425953397	0,446428949
1,8	3	4,315361066	-1,315361066	1,730174735	0,400933945
1,9	6	3,870151445	2,129848555	4,536254865	1,172113011
2	2	2,304807545	-0,304807545	0,09290764	0,040310368
2,1	1	0,894794766	0,105205234	0,011068141	0,012369475
					$x^2_{\text{набл}} = 2{,}698001503$

Выполнение неравенства $x^2_{\text{набл}} < x^2_{\text{кр}}$ подтверждает нулевую гипотезу H_0 о предполагаемом нормальном законе распределения времени функционирования СЗИ от НСД на первом этапе конфликтного взаимодействия.

График распределения количества функционирований СЗИ от НСД в зависимости от времени на первом этапе конфликтного взаимодействия с сетевой атакой представлен на рис. 3.

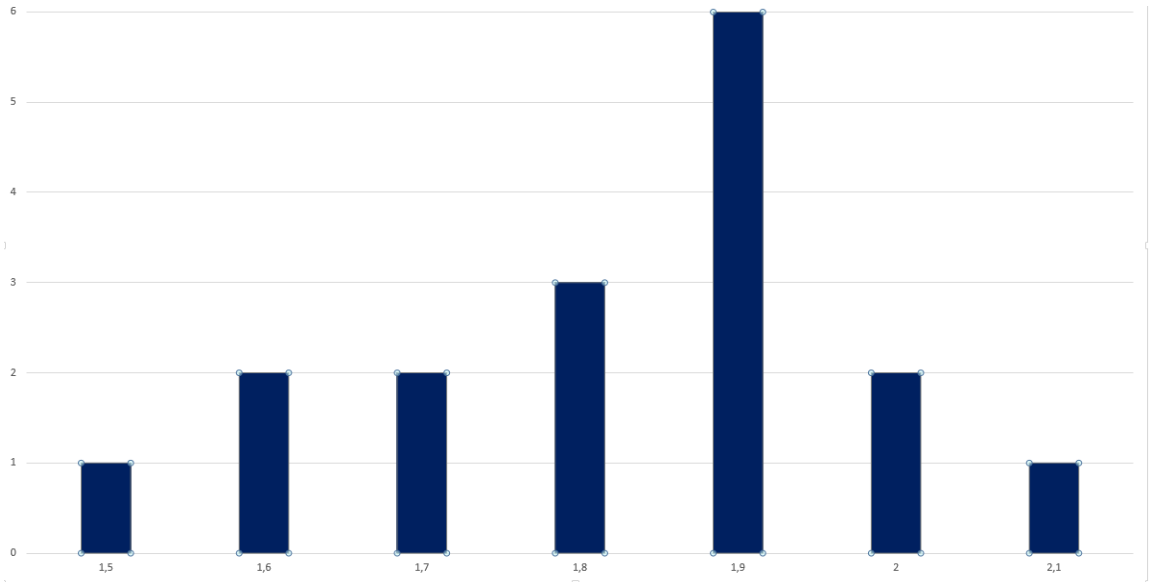


Рис. 3. График распределения количества функционирований СЗИ от НСД в зависимости от времени на первом этапе конфликтного взаимодействия с сетевой атакой
Fig. 3. Time distribution of the number of SPI from the NSD implementations at the first stage of conflict interaction with the network attack

Результаты расчета по формуле (1) достаточного количества итераций экспериментов, проводимых над сетевой атакой с целью адекватного обоснования закона распределения времени ее реализации на втором этапе конфликтного взаимодействия с системой защиты ($\varepsilon = 0{,}05$) [13, 14], приведены в табл. 5, где x_i – эмпирические значения времен реализации сетевой атаки (получены в результате проведения натурного эксперимента).

Адекватные результаты эксперимента, проведенного 25 раз, представлены в табл. 6. Приведенные в табл. 6 характеристики позволили определить и обосновать закон распределения времени реализации сетевой атаки на втором этапе конфликтного взаимодействия.

Таблица 5. Результаты расчета достаточного количества итераций экспериментов над сетевой атакой на втором этапе конфликтного взаимодействия с СЗИ от НСД

x_i, с	$\overline{x_i}$, с	D	σ	N
756,04	755,979	0,016009	0,126526677	≈ 25
756,08				
756,02				
755,64				
756,03				
756,01				
755,89				
755,95				
756,1				
756,03				

Таблица 6. Расчетная таблица нахождения критерия $\lambda_{\text{набл}}$ для процесса реализации сетевой атаки на втором этапе конфликтного взаимодействия с СЗИ от НСД

x_i	x_{i+1}	n_i	x_i^*	$x_i^* n_i$	$F^*(x_i^*)$	$F(x_i^*)$	$\lvert F^*(x_i^*) - F(x_i^*)\rvert$
755,7	755,8	10	755,75	7557,5	0,4	0,632052417	0,232052417
755,8	755,9	7	755,85	5290,95	0,28	0,632101091	0,352101091
755,9	756	2	755,95	1511,9	0,08	0,632149759	0,552149759
756	756,1	2	756,05	1512,1	0,08	0,63219842	0,55219842
756,1	756,2	2	756,15	1512,3	0,08	0,632247075	0,552247075
756,2	756,3	2	756,25	1512,5	0,08	0,632295723	0,552295723
				$\overline{x_в} = 755{,}89$			$\lambda_{\text{набл}} = 1{,}352842709$

Поскольку времена реализации сетевой атаки на данном этапе можно рассмотреть как непрерывную случайную величину, то их распределение может быть задано в виде последовательности конечных интервалов $x_i - x_{i+1}$ и соответствующих им частот n_i, что позволяет использовать λ-критерий А.Н. Колмогорова для подтверждения нулевой гипотезы H_0 о законе распределения времени.

В основе использования λ-критерия А.Н. Колмогорова лежит сравнение эмпирической $F^*(x)$ и гипотетической $F(x)$ функций распределения (для χ^2-критерия К. Пирсона – эмпирической и теоретической). Вместе с этим в λ-критерии теоретические значения гипотетического закона распределения известны (для χ^2-критерия – рассчитываются по результатам выборки). Указанные ограничения могут оказывать влияние на качество проводимого подтверждения гипотезы H_0. Несмотря на это λ-критерий А.Н. Колмогорова широко применяется на практике, кроме того для случая, когда параметры гипотетического закона распределения оцениваются по результатам выборки (как в данном случае) λ-критерий показывает лучшее согласие с эмпирическим законом распределения, чем χ^2-критерий [16].

Для проверки нулевой гипотезы о предполагаемом распределении с использованием λ-критерия А.Н. Колмогорова необходимо сначала расположить полученные результаты наблюдений в возрастающем порядке либо в виде интервального ряда, затем – рассчитать значения эмпирической функции распределения по формуле:

$$F^*(x) = \frac{n_i}{n}. \quad (4)$$

Далее, пользуясь гипотетической функцией распределения, следует определить значения теоретической функции распределения $F(x)$ (в рамках проведенного натурного эксперимента данные значения находятся по результатам выборки). Для каждого значения x_i необходимо вычислить модуль разности полученных значений эмпирической

и теоретической функций распределения:

$$|F^*(x) - F(x)|. \quad (5)$$

По результатам рассчитанных модулей разности определяется наблюдаемое значение λ выборочной статистики А.Н. Колмогорова:

$$\lambda = \max_x |F^*(x) - F(x)| \cdot \sqrt{n}. \quad (6)$$

В случае верности нулевой гипотезы выборочная статистика при $\lambda \to \infty$ имеет функцию распределения $K(\lambda)$ вида:

$$K(\lambda) = \sum_{k=-\infty}^{\infty} (-1)^k e^{-2k^2\lambda_\varepsilon^2}. \quad (7)$$

Задав уровень значимости ε, находятся квантили распределения А.Н. Колмогорова из соотношения:

$$P(\lambda \geq \lambda_\varepsilon) = 1 - \sum_{k=-\infty}^{\infty} (-1)^k e^{-2k^2\lambda^2} = \varepsilon. \quad (8)$$

Сравнивая $\lambda_{\text{набл}}$ с λ_ε, определяемом по таблице критических значений распределения А.Н. Колмогорова, делается вывод о согласовании выдвинутой нулевой гипотезы с полученными эмпирическими данными. При $\lambda_{\text{набл}} < \lambda_\varepsilon$ нулевая гипотеза подтверждается, в противном случае ($\lambda_{\text{набл}} \geq \lambda_\epsilon$) – отвергается.

Предполагая, что закон распределения времени реализации сетевой атаки на втором этапе является экспоненциальным (показательным) [9], осуществлялось обоснование данной гипотезы согласно методике, изложенной в [17].

Для процесса реализации сетевой атаки на втором этапе ее конфликтного взаимодействия с системой защиты алгоритм расчетов по полученным эмпирическим данным имеет вид:

1) рассчитывается выборочная средняя эмпирического распределения $\overline{x_в} = \frac{\sum_{i=1}^{s} x_i^* n_i}{n} = 755{,}89$ где $s = 6$ – количество интервалов. Для этого в качестве «представителя» i-го интервала принимается его середина $x_i^* = (x_i + x_{i+1})/2$ и составляется последовательность равностоящих вариант и соответствующих им частот [18];

2) определяется величина оценки показателя экспоненциального распределения $\lambda = \frac{1}{\overline{x_в}} = 0{,}001322944$;

3) по формуле (4) для объема выборки $n = 25$ вычисляются значения эмпирической функции распределения $F^*(x_i^*)$;

4) рассчитываются значения теоретической функции распределения по формуле $F(x_i^*) = 1 - e^{-\lambda x_i^*}$;

5) проводится сравнение по модулю значений эмпирической и теоретической функций распределения для определения максимальной величины их разницы по формуле (5);

6) по формуле (6) находится наблюдаемое значение выборочной статистики $\lambda_{\text{набл}} = 1{,}352842709$.

Полученные результаты представлены в табл. 6.

По таблице квантилей распределения А.Н. Колмогорова [17] для уровня значимости $\varepsilon = 0{,}05$ обозначается критическая точка $\lambda_\varepsilon(0{,}05) = 1{,}358$.

Выполнение неравенства $\lambda_{\text{набл}} < \lambda_\varepsilon$ подтверждает нулевую гипотезу H_0 о предполагаемом экспоненциальном законе распределения времени реализации сетевой атаки на втором этапе конфликтного взаимодействия.

График распределения количества реализаций рассматриваемой сетевой атаки в зависимости от времени на втором этапе конфликтного взаимодействия с СЗИ от НСД представлен на рис. 4.

Результаты расчета по формуле (1) достаточного количества итераций экспериментов, проводимых над СЗИ от НСД с целью адекватного обоснования закона распределения времени на втором этапе конфликтного взаимодействия с сетевой атакой ($\varepsilon = 0{,}05$) [13, 14], приведены в табл. 7, где x_i – эмпирические значения времен функционирования системы защиты (получены в результате проведения натурного эксперимента).

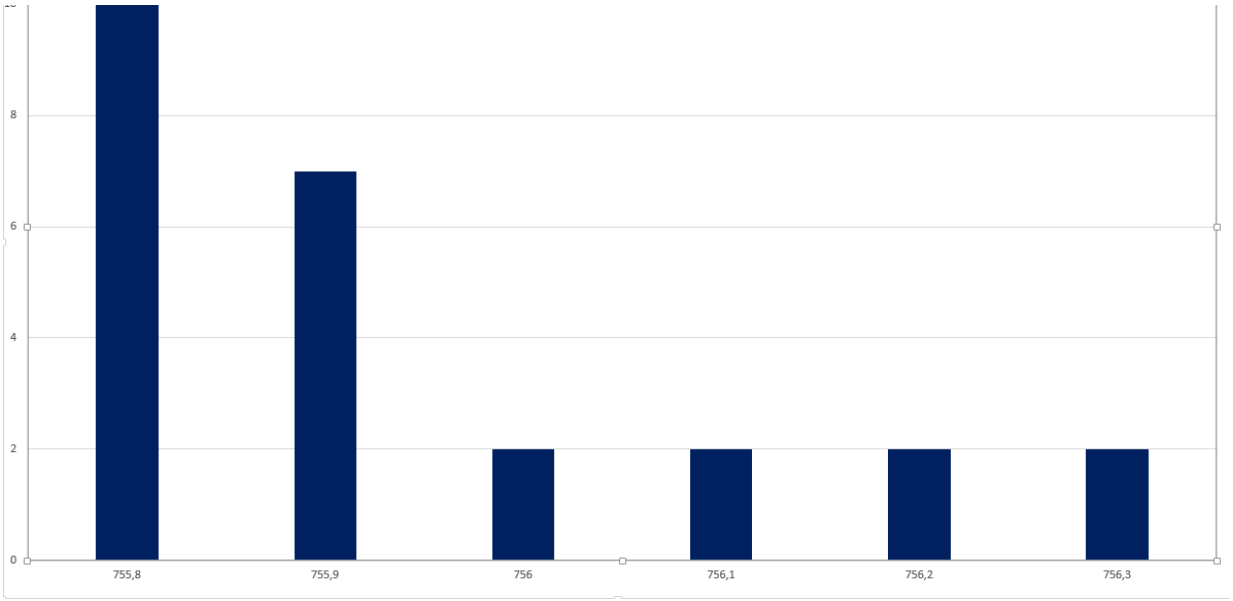


Рис. 4. График распределения количества реализаций сетевой атаки в зависимости от времени на втором этапе конфликтного взаимодействия с СЗИ от НСД
Fig. 4. Time distribution of the number of network attack implementations at the second stage of conflict interaction with the SPI from the NSD

Предполагая, что распределение времени функционирования СЗИ от НСД на втором этапе соответствует экспоненциальному закону, проведено доказательство согласования полученного эмпирического распределения с законом экспоненциального распределения с использованием критерия А.Н. Колмогорова аналогично второму этапу конфликтного взаимодействия при реализации сетевой атаки [17, 18]. Результаты расчетов, проведенных по указанному выше алгоритму для $s = 7$ и $n = 30$, представлены в табл. 8.

По таблице квантилей распределения Колмогорова [17] для уровня значимости $\varepsilon = 0{,}05$ обозначается критическая точка $\lambda_\varepsilon(0{,}05) = 1{,}358$.

Выполнение неравенства $\lambda_{\text{набл}} < \lambda_\alpha$ подтверждает нулевую гипотезу H_0 о предполагаемом экспоненциальном законе распределения времени функционирования системы защиты на втором этапе конфликтного взаимодействия.

Таблица 7. Результаты расчета достаточного количества итераций экспериментов над СЗИ от НСД на втором этапе конфликтного взаимодействия с сетевой атакой

x_i, с	$\overline{x_i}$, с	D	σ	N
912,96	912,963	0,019261	0,138784005	≈ 30
913,04				
912,93				
913,11				
913				
912,86				
913,02				
913,2				
912,81				
912,7				

Таблица 8. Расчетная таблица нахождения критерия $\lambda_{\text{набл}}$ для процесса функционирования СЗИ от НСД на втором этапе конфликтного взаимодействия с сетевой атакой

x_i	x_{i+1}	n_i	x_i^*	$x_i^* n_i$	$F^*(x_i^*)$	$F(x_i^*)$	$\lvert F^*(x_i^*) - F(x_i^*)\rvert$
912,7	912,8	5	912,75	4563,75	0,166666667	0,63200638	0,465339714
912,8	912,9	5	912,85	4564,25	0,166666667	0,632046683	0,465380016
912,9	913	4	912,95	3651,8	0,133333333	0,632086981	0,498753647
913	913,1	4	913,05	3652,2	0,133333333	0,632127274	0,498793941
913,1	913,2	4	913,15	3652,6	0,133333333	0,632167563	0,49883423
913,2	913,3	4	913,25	3653	0,133333333	0,632207848	0,498874514
913,3	913,4	4	913,35	3653,4	0,133333333	0,632248128	0,498914795
				$\overline{x_{\text{в}}} =$ 913,0333333			$\lambda_{\text{набл}} =$ 1,320004472

График распределения количества функционирований СЗИ от НСД в зависимости от времени на втором этапе конфликтного взаимодействия с сетевой атакой представлен на рис. 5.

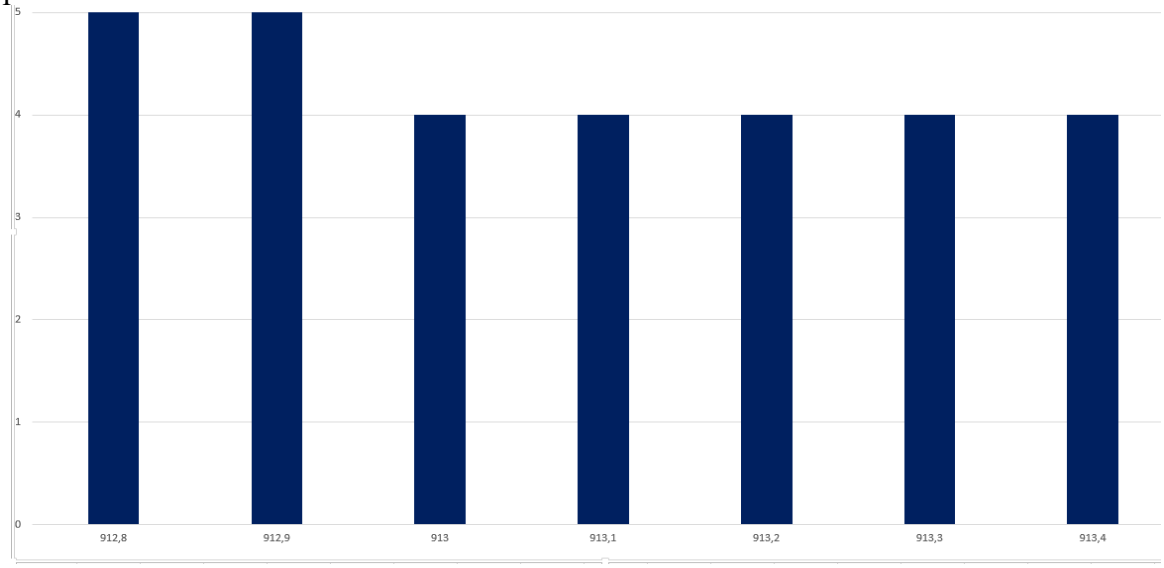


Рис. 5. График распределения количества функционирований СЗИ от НСД в зависимости от времени на втором этапе конфликтного взаимодействия с сетевой атакой
Fig. 5. Time distribution of the number of SPI from the NSD implementations at the second stage of conflict interaction with the network attack

Заключение

На основе построения обобщенной графовой модели, описывающей механизм информационного конфликта «Сетевая атака – СЗИ от НСД» в защищенной АС ОВД, и проведения натурного эксперимента обоснованы законы распределения времени реализации типовой сетевой атаки и функционирования СЗИ от НСД на различных этапах их конфликтного взаимодействия. на различных этапах

На основе использования χ^2-критерия К. Пирсона и -критерия А.Н. Колмогорова с достаточностью 0,05 представлено математическое подтверждение нормального (на первом этапе конфликтного взаимодействия) и экспоненциального (на втором этапе) законов распределения, а также их графическое отображение.

Полученные результаты позволят разработать аналитическую модель динамики реализации сетевой атаки в конфликтном взаимодействии с СЗИ от НСД, рассчитать вероятностно-временные характеристики и провести точную количественную оценку опасности реализации сетевых атак на этапах всего жизненного цикла функционирования, защищенных АС ОВД.

СПИСОК ЛИТЕРАТУРЫ:

1. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: РадиоСофт, 2010. – 232 с. URL: https://bookree.org/reader?file=1213197 (дата обращения: 15.04.2021).
2. Радько Н.М., Язов Ю.К., Корнеева Н.Н. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа. Воронеж: Воронеж. госуд. технич. ун-т, 2013. – 265 с.
3. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография. Воронеж: Кварта, 2018. – 588 с.
4. Язов Ю.К., Анищенко А.В. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография. Воронеж: Кварта, 2020. – 173 с.
5. Concept for increasing security of national information technology infrastructure and private clouds / D.A. Melnikov, A.P. Durakovsky, S.V. Dvoryankin, V.S. Gorbatov // Proceedings-2017 IEEE 5th International Conference on Future Internet of Things and Cloud, FiCloud 2017: 5, Prague, August 21-23, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
6. Stages and procedures for forming a method to assess reliability of the information security systems in automated systems and main areas of its implementation in the normative-technical documentation / O.I. Bokova, A.S. Etepnev, E.A. Rogozin, O.M. Bulgakov // Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, November 11-13, 2019. Voronezh: Institute of Physics Publishing, 2020. – P. 012022. DOI: https://doi.org/10.1088/1742-6596/1479/1/012022.
7. Михайлов Р.Л. Динамическая модель информационного конфликта информационно-телекоммуникационных систем специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 238–251. DOI: https://doi.org/10.24411/2410-9916-2020-10309.
8. Дровникова И.Г., Овчинникова Е.С., Рогозин Е.А., Калач А.В. Моделирование динамики информационного конфликта в защищенных автоматизированных системах органов внутренних дел на основе сети Петри-Маркова. Вестник Воронежского института ФСИН России. 2020. № 4. С. 37–44. URL: https://vi.fsin.gov.ru/upload/territory/Vi/nauchnaja_dejatelnost/v_fsin_2020_4.pdf (дата обращения: 01.04.2021).
9. Дровникова И.Г., Овчинникова Е.С. К вопросу моделирования процесса функционирования системы защиты информации в условиях реализации сетевых атак на объектах информатизации органов внутренних дел // Общественная безопасность, законность и правопорядок в III тысячелетии. 2020. № 6-2. С. 218–225. URL: https://www.elibrary.ru/download/elibrary_44250423_88392617.pdf (дата обращения: 01.04.2021).
10. Дровникова И.Г., Овчинникова Е.С., Конобеевских В.В. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47 (1): С. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85.
11. Bokova O.I. et al. Innovative technology in the research of implementation dynamics of network attacks on the digital educational resources. 2020 J. Phys.: Conf. Ser. 1691 012063.

DOI: https://doi.org/10.1088/1742-6596/1691/1/012063.
12. Бацких Анна В. и др. Анализ и классификация основных угроз информационной безопасности автоматизированных систем на объектах информатизации органов внутренних дел. Безопасность информационных технологий, [S.l.]. Т. 27, № 1. С. 40–50, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1250 (дата обращения: 10.02.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.04.
13. Советов Б.Я., Яковлев С.А. Моделирование систем. – 3-е изд., перераб. и доп. М.: Высшая школа, 2001. – 343 с.
14. Советов Б.Я., Яковлев С.А. Моделирование систем. Практикум. – 4-е изд., перераб. и доп. М.: Юрайт, 2014. – 295 с.
15. Гмурман В.Е. Теория вероятностей и математическая статистика // 9-е изд., стер. М.:Высшая школа, 2003. – 479 с. URL: https://bookree.org/reader?file=567344&pg=4 (дата обращения: 01.04.2021).
16. Nazarenko S.V., Grebenev V.N. Self-similar formation of the Kolmogorov spectrum in the Leith model of turbulence // Journal of Physics A: Mathematical and Theoretical. 2017. Vol. 50. No 3. P. 035501. DOI: https://doi.org/10.1088/1751-8121/50/3/035501.
17. Герасимович А.И., Матвеева Я.И. Математическая статистика. Минск: Вышэйшая школа, 1978. – 200 с. URL: https://booksee.org/book/637093 (дата обращения: 01.04.2021).
18. Kozera R., Noakes L., Szmielew P. (2013) Trajectory estimation for exponential parametrization and various samples. Saeed K., Chaki R., Cortes A., Wierzchoń S. (eds) Computer Information Systems and industrial management. SIM 2013. Lecture notes on Computer Science, vol. 8104. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-40925-7_40.

REFERENCES:

[1] Radko N.M., Skobelev I.O. Risk models of information and telecommunication systems in the implementation of threats of remote and direct access. M.: Radiosoft, 2010. – 232 p. URL: https://bookree.org/reader?file=1213197 (accessed: 15.04.2021) (in Russian).
[2] Radko N.M., Yazov Yu.K., Korneeva N.N. Penetration into the computer operating environment: models of malicious remote access. Voronezh: Voronezh state technical University, 2013. – 265 p. (in Russian).
[3] Yazov Yu K., Solovyov S.V. Organization of information protection in information systems from unauthorized access: monograph. Voronezh: Kvart, 2018. – 588 p. (in Russian).
[4] Yazov Yu.K., Anishchenko A.V. Petri-Markov networks and their application for modeling the processes of implementing information security threats in information systems: monograph. Voronezh: Kvart, 2020. – 173 p. (in Russian).
[5] Concept for increasing security of national information technology infrastructure and private clouds. D.A. Melnikov, A.P. Durakovsky, S.V. Dvoryankin, V.S. Gorbatov. Proceedings-2017 IEEE 5th International Conference on Future Internet of Things and Cloud, FiCloud 2017: 5, Prague, August 21-23, 2017. – Prague, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
[6] Stages and procedures for forming a method to assess reliability of the information security systems in automated systems and main areas of its implementation in the normative-technical documentation. O.I. Bokova, A.S. Etepnev, E.A. Rogozin, O.M. Bulgakov. Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, November 11-13, 2019. Voronezh: Institute of Physics Publishing, 2020. P. 012022. DOI: https://doi.org/10.1088/1742-6596/1479/1/012022.
[7] Mikhailov R.L. Dynamic model of information conflict of special purpose information and telecommunications systems. Control, communication and security systems. 2020. No. 3. P. 238–251. DOI: https://doi.org/10.24411/2410-9916-2020-10309 (in Russian).
[8] Drovnikova I.G., Ovchinnikova E.S., Rogozin E.A., Kalach A.V. Modeling of the dynamics of information conflict in protected automated systems of internal affairs bodies based on the Petri-Markov network. Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2020. No. 4. P. 37–44. URL: https://vi.fsin.gov.ru/upload/territory/Vi/nauchnaja_dejatelnost/v_fsin_2020_4.pdf (accessed: 01.04.2021) (in Russian).
[9] Drovnikova I. G., Ovchinnikova E. S. On the issue of modeling the process of functioning of the information protection system in the conditions of network attacks on the objects of informatization of internal affairs bodies. Public security, legality and law and order in the III millennium. 2020. No. 6-2. P. 218–225. URL: https://www.elibrary.ru/download/elibrary_44250423_88392617.pdf (accessed: 01.04.2021) (in Russian).
[10] Drovnikova I.G., Ovchinnikova E.S., Konobeevskikh V.V. Analysis of typical network attacks on automated systems of internal affairs bodies. Bulletin of the Dagestan State Technical University. Technical sciences. 2020; 47 (1): P. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85 (in Russian).
[11] Bokova O.I. et al. Innovative technology in the research of implementation dynamics of network attacks on the

digital educational resources. 2020 J. Phys.: Conf. Ser. 1691 012063. DOI: https://doi.org/10.1088/1742-6596/1691/1/012063.

[12] Batskikh Anna V. et al. Analysis and classification of the main threats to the information security of automated systems at the objects of informatization of internal affairs bodies. IT Security (Russia), [S. l.]. Vol. 27, no. 1. P. 40–50, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1250 (accessed: 10.02. 2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.04 (in Russian).

[13] Sovetov B.Ya., Yakovlev S.A. Modeling of systems. – 3rd ed., reprint. and add. M.: Higher School, 2001. – 343 p. (in Russian).

[14] Sovetov B.Ya., Yakovlev S.A. Modeling of systems. Practicum. – 4th ed., reprint. and add. M.: Yurayt, 2014. – 295 p. (in Russian).

[15] Gmurman V.E. Probability theory and mathematical statistics. 9th ed., ster. Moscow: Higher School, 2003. – 479 p. URL: https://bookree.org/reader?file=567344&pg=4 (accessed: 01.04.2021) (in Russian).

[16] Nazarenko S.V. Self-similar formation of the Kolmogorov spectrum in the Leith model of turbulence S.V. Nazarenko, V.N. Grebenev. Journal of Physics A: Mathematical and Theoretical. 2017. Vol. 50. No 3. P. 035501. DOI: https://doi.org/10.1088/1751-8121/50/3/035501 (in Russian).

[17] Gerasimovich A.I., Matveeva Ya.I. Mathematical statistics. Minsk: Higher School, 1978. – 200 p. URL: https://booksee.org/book/637093 (accessed: 01.04.2021) (in Russian).

[18] Kozera R., Noakes L., Szmielew P. (2013) Trajectory estimation for exponential parametrization and various samples. Saeed K., Chaki R., Cortes A., Wierzchoń S. (eds) Computer Information Systems and industrial management. SIM 2013. Lecture notes on Computer Science, vol. 8104. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-40925-7_40.

Поступила в редакцию – 25 апреля 2021 г. Окончательный вариант – 17 августа 2021 г.
Received – April 25,2021. The final version – August 17, 2021.