Ирина Г. Дровникова[1], Елена С. Овчинникова[2], Евгений А. Рогозин[3]
[1,2,3]Воронежский институт министерства внутренних дел Российской федерации,
пр-т 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
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

ФОРМИРОВАНИЕ ОСНОВНЫХ ПОКАЗАТЕЛЕЙ ОПАСНОСТИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DOI: http://dx.doi.org/10.26583/bit.2020.3.01

Аннотация. Целью статьи является анализ существующих показателей, используемых при оценивании опасности реализации угроз информационной безопасности в автоматизированных системах, для выявления их достоинств, недостатков и возможностей применения при проведении количественной оценки опасности реализации сетевых атак на автоматизированные системы, эксплуатируемые в защищенном исполнении на объектах информатизации органов внутренних дел. Для достижения поставленной цели применен метод системного анализа показателей опасности угроз на основе исследования открытых литературных источников, международных и отраслевых стандартов Российской Федерации по защите информации в автоматизированных системах, методических, руководящих документов и приказов Федеральной службы по техническому и экспертному контролю России по проблеме оценивания опасности реализации угроз несанкционированного доступа в автоматизированные системы, а также нормативной базы МВД России, регламентирующей эксплуатацию автоматизированных систем органов внутренних дел в защищенном исполнении. Для осуществления корректного выбора адекватных показателей при проведении количественного анализа риска нарушения информационной безопасности проанализирована риск-модель автоматизированной системы. Для проведения количественной оценки опасности реализации сетевых атак и исследования их в динамическом режиме предложены основные направления совершенствования выявленных показателей с учетом реально существующих особенностей и недостатков эксплуатации защищенных автоматизированных систем органов внутренних дел. Разработка динамического интегрального показателя опасности атак, отражающего реальные динамические свойства процесса реализации множества типовых сетевых атак на автоматизированную систему, и совершенствование существующего математического обеспечения оценки опасности сетевых атак путем определения вероятностно-временных характеристик множественных параллельно реализуемых типовых атак на основе имитационного моделирования позволит провести количественную оценку опасности и повысить реальную защищенность автоматизированных систем в процессе их эксплуатации на объектах информатизации органов внутренних дел.

Ключевые слова: автоматизированная система, сетевая атака, информационный риск, динамический интегральный показатель опасности, количественная оценка опасности.
Для цитирования: ДРОВНИКОВА, Ирина Г.; ОВЧИННИКОВА, Елена С.; РОГОЗИН, Евгений А. ФОРМИРОВАНИЕ ОСНОВНЫХ ПОКАЗАТЕЛЕЙ ОПАСНОСТИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 6–17, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1288>. Дата доступа: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.01.

Irina G. Drovnikova[1], Elena S. Ovchinnikova[2], Evgeni A. Rogozin[3]
[1,2,3]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
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Network attacks main danger indicators formation in Internal Affairs Bodies automated systems

DOI: http://dx.doi.org/10.26583/bit.2020.3.01

Abstract. The purpose of this study is to analyze the existing indicators used in information security implementing threats risk assessing in automated systems. The goal is to identify its advantages, disadvantages and application possibilities, when conducting implementing danger network attacks quantitative assessment on automated systems operated in a secure execution at the Internal Affairs Bodies informatization objects. To achieve this goal we use the method of system analysis of threat hazard indicators based on research of open literature sources, international and industry standards of the Russian Federation for information protection in automated systems, methodological and guiding documents and orders of the Federal service for technical and expert control of Russia on the problem of assessing the risk of unauthorized access to automated systems, as well as the regulatory framework of the Ministry of internal Affairs of Russia, regulating the operation of automated systems of internal Affairs bodies in a protected version. The risk model of the automated system is analyzed to make a correct choice of adequate indicators when conducting a quantitative analysis of the risk of information security violations. To conduct network attacks danger quantitative assessment and study them in a dynamic mode, the main directions for improving the identified indicators are proposed, taking into account Internal Affairs Bodies protected automated systems operation actual features and disadvantages. Development of a dynamic integral attack hazard indicator that reflects the real dynamic properties of the process of implementing a set of typical network attacks on an automated system, and improvement of existing mathematical software for assessing the risk of network attacks by determining the probability-time characteristics of multiple parallel attacks implemented model-based simulation will allow to quantify risk and increase the real security of the automated systems in process of their operation on the objects of Informatization of Internal Affairs bodies.

Keywords: automated system, network attack, information risk, dynamic integral danger indicator, quantitative danger assessment.

For citation: DROVNIKOVA, Irina G.; OVCHINNIKOVA2, Elena S.; ROGOZIN, Evgeni A. Network attacks main danger indicators formation in Internal Affairs Bodies automated systems. IT Security (Russia), [S.l.], v. 27, n. 3, p. 6–17, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1288>. Date accessed: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.01.

Введение

Оценивание опасности реализации угроз несанкционированного доступа (НСД), осуществляемых через удаленное взаимодействие с автоматизированной системой (АС) (сетевые атаки), является одним из ключевых моментов в процессе оценивания эффективности функционирования систем защиты информации (СЗИ) от НСД на этапе эксплуатации АС в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД). Это, в свою очередь, необходимо для формирования требований по защите информации (ЗИ) в АС ОВД с целью разработки адекватных существующим атакам перспективных образцов СЗИ от НСД[1,2].

Обеспечение достаточной степени защищенности АС ОВД для их эффективного функционирования в условиях сетевых атак предполагает проведение процедуры оценивания опасности реализации атак как в процессе разработки СЗИ от НСД с целью формирования на этой основе частной модели актуальных атак для конкретной АС на объекте информатизации ОВД, так и при мониторинге и переоценке атак в ходе эксплуатации СЗИ от НСД, что приводит к необходимости разработки адекватных

[1]ISO/IEC 17000:2004. Conformity assessment. Dictionary and General principles.
[2]ГОСТ Р ИСО/МЭК 17021-2012. Национальный стандарт Российской Федерации. Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента.

показателей опасности сетевых атак на защищаемые АС ОВД[3].

Необходимость разработки показателей опасности сетевых атак на АС, эксплуатируемые в защищенном исполнении на объектах информатизации ОВД, подтверждается требованиями приказа МВД России от 14.03.2012 № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года», в котором определены цели, задачи, принципы и основные направления обеспечения информационной безопасности (ИБ) ОВД. В приказе отмечается, что одним из механизмов реализации Концепции является разработка критериев и методов оценки эффективности систем обеспечения ИБ ОВД, однако не рассматриваются конкретные критерии (показатели) опасности сетевых атак, необходимые для последующего формирования показателей и проведения количественной оценки эффективности функционирования СЗИ от НСД в АС ОВД. В то же время, данный документ во многом подтверждает актуальность проблемы разработки показателей опасности сетевых атак и определяет перспективные аспекты научных исследований в данной области применительно к объектам информатизации ОВД – АС, эксплуатируемым в защищенном исполнении.

1. Постановка задачи

В связи с недостаточностью научных исследований, посвященных разработке показателей опасности сетевых атак на АС ОВД, проанализируем показатели, используемые в настоящее время при оценивании опасности реализации угроз ИБ в АС с целью выявления их достоинств, недостатков и возможностей применения для проведения количественной оценки опасности реализации сетевых атак на защищенные АС, эксплуатируемые на объектах информатизации ОВД.

2. Теоретический анализ показателей опасности угроз информационной безопасности автоматизированных систем

Оценивание опасности реализации угрозы осуществляется по размеру информационного риска [1–3]. Анализ нормативной документации, раскрывающей понятие «риск», показал отсутствие единой трактовки данного термина[4,5,6,7]. Максимально соответствующим тому, что понимается под риском в большинстве публикаций, следует считать определение, согласно которому риск рассматривается как сочетание вероятности нанесения ущерба и тяжести этого ущерба[8].

С учетом выше изложенного под информационным риском будем понимать количественную величину, характеризующую возможность нанесения АС некоторого ущерба, а под показателем опасности угрозы – меру размера информационного риска от ее реализации.

---

[3]ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные компоненты безопасности.

[4]ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

[5]ГОСТ Р 51897-2011. Национальный стандарт Российской Федерации. Менеджмент риска. Термины и определения.

[6]О техническом регулировании: федеральный закон от 27.12.2002 № 184-ФЗ.

[7]ГОСТ Р 22.0.02-2016. Национальный стандарт Российской Федерации. Безопасность в чрезвычайных ситуациях. Термины и определения.

[8]ГОСТ Р 51898-2002. Национальный стандарт Российской Федерации. Аспекты безопасности. Правила включения в стандарты.

Таким образом, информационный риск в условиях сетевых атак следует рассматривать как сочетание двух характеристик: величины возможного ущерба от реализации атак и оценки возможности этой реализации (т.е. нанесения ущерба) [4].

Задачи анализа, обоснования и разработки показателей опасности угроз ИБ АС не являются новыми и решены в ряде методических документов Федеральной службы по техническому и экспертному контролю (ФСТЭК) России[9,10] и работах [4–9]. Представленные в [4] результаты анализа четырех наиболее популярных подходов, используемых в настоящее время при оценивании опасности реализации угроз ИБ в АС (экспертного, шкального, балльного, вероятностного), позволяют констатировать отсутствие среди авторов единства в выделении основных показателей опасности угроз (табл. 1).

Таблица 1. Представление показателей опасности угроз ИБ в АС

№ п/п	Название подхода	Показатели опасности угроз ИБ
1	Экспертный – основан на экспертном методе оценки, представленном в Методических документах ФСТЭК России	Уровень защищенности АС Потенциал нарушителя, необходимый для реализации угрозы ИБ в АС Максимальные размеры видов возможного ущерба[9]
		Коэффициент реализуемости угрозы Вербальный показатель опасности угрозы для АС[10]
2	Шкальный – основан на методе оппозиционных (полярных) шкал	Коэффициент опасности угрозы – свертка коэффициента опасности несанкционированного действия и вероятности реализации угрозы [7, 8]
3	Балльный – основан на балльном (табличном) методе оценки	Степень угрозы Степень уязвимости Показатель цены потери [9]
4	Вероятностный – основан на математическом моделировании процессов реализации угроз	Вероятность возникновения угрозы Вероятность реализации угрозы Вероятность нанесения ущерба реализацией угрозы Величина нанесенного ущерба [8]

Так в рамках экспертного подхода применяются следующие показатели опасности угрозы: уровень защищенности АС и потенциал нарушителя, необходимый для реализации данной угрозы ИБ в заданной АС (для оценивания возможности реализации угрозы); максимальные размеры каждого вида возможного ущерба, связанного с нарушением конфиденциальности, целостности или доступности каждого вида информации (для оценивания итоговой величины возможного ущерба)[9]. При оценивании опасности реализации угрозы персональным данным (ПДн) и определении актуальных угроз безопасности ПДн в АС ПДн предлагаются два показателя: коэффициент реализуемости угрозы и вербальный показатель опасности угрозы для рассматриваемой АС ПДн[10].

При использовании шкального подхода [7, 8] оценивание опасности реализации угрозы ИБ основывается на применении комплексного динамического показателя –

[9]ФСТЭК России. Методический документ. Методика определения угроз безопасности информации в информационных системах.

[10]ФСТЭК России. Методический документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

коэффициента опасности угрозы K_{thu}, который определяется в виде свертки коэффициента опасности несанкционированного действия K_g и вероятности реализации угрозы $P_{thu}(t)$:

$$K_{thu} = K_g \cdot P_{thu}(t), \quad (1)$$

где K_g представляет собой отношение максимального значения величины нанесенного ущерба к предельно допустимому его значению (применительно к общему объему информационного ресурса, для которого может быть реализовано данное несанкционированное действие)

$$K_g = \frac{\bar{u}}{u_{np}}. \quad (2)$$

При использовании балльного подхода для оценивания опасности реализации угроз ИБ в АС в [9] предлагаются три показателя опасности угрозы: степень (уровень) угрозы, степень (уровень) уязвимости, показатель цены потери (в зависимости от ценности ресурсов и вида возможного ущерба).

Очевидным недостатком показателей опасности угроз, выделенных в рамках изложенных подходов, применительно к оцениванию опасности реализации сетевых атак на АС ОВД является их недостаточная точность, обусловленная необходимостью экспертного участия в процессе оценивания.

Указанного недостатка лишен четвертый подход (вероятностный), используемый при оценивании опасности реализации угроз ИБ в АС, основанный на математическом моделировании (аналитическом, имитационном) процессов реализации угроз. Данный подход применяется для описания случайных событий, в частности, на основе определения их вероятностно-временных характеристик (ВВХ), что дает возможность проводить количественную оценку опасности реализации угроз обеспечения ИБ в АС и исследовать их в динамическом (временном) режиме [8, 10–13].

Модель риск-анализа АС, разрабатываемая в рамках вероятностного подхода, представляет собой математическую модель, учитывающую, во-первых, воздействие на систему всего множества типовых угроз и, во-вторых, применение различных средств и систем ЗИ. Выходным параметром рассматриваемой риск-модели является интегральный информационный риск для функционирующей в заданных условиях АС. Следовательно, вариация средств и систем ЗИ представляет собой способ регулирования рисков АС. Полученные значения риска для каждой исследуемой АС позволяют оптимизировать комплекс мер защиты.

Для осуществления корректного выбора адекватных параметров при проведении количественного анализа риска нарушения ИБ в [8] рассматривается схема воздействия угрозы на защищаемую АС, включающая следующие элементы:

1) *субъект угрозы* (ее источник) – активная составляющая процесса, способная посредством выполнения каких-либо действий оказывать влияние на другие составляющие;

2) *процесс реализации угрозы* – конкретный сценарий (операция), осуществляемый субъектом для достижения поставленной цели;

3) *объект угрозы* – пассивная составляющая процесса, подверженная влиянию субъекта;

4) *предмет угрозы* – цель действий субъекта (характеристика объекта или ее определенное значение, какое-либо свойство объекта).

Представленная схема рассмотрена в [4] применительно к воздействию сетевой атаки на защищаемую АС (рис. 1). Элементы схемы характеризуются четырьмя параметрами, составляющими основу риск-модели: $p_{\text{ви}}$, $p_{\text{ри}}$ – вероятности возникновения и реализации u-й атаки соответственно, $p_{\text{уи}j}$ – вероятность нанесения ущерба вида j реализацией u-й атаки, d_j – величина нанесенного ущерба вида j. Указанные параметры предлагаются в виде показателей опасности u-й атаки.

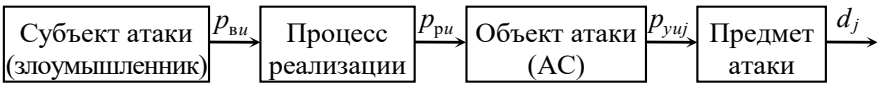

Рис. 1. Схема сетевой атаки на АС с параметрами, характеризующими ее элементы (Fig. 1. Scheme of network attack on the AS with parameters that characterize its elements)

Таким образом, величина интегрального информационного риска атакуемой АС определяется значением вероятности p нанесения общего ущерба реализацией множества типовых сетевых атак и количественным значением d этого ущерба.

При оценивании опасности реализации сетевых атак на АС вероятностный подход реализуется, как правило, в двух вариантах с использованием различных показателей опасности атаки (табл. 2).

Таблица 2. Взаимосвязь вариантов реализации вероятностного подхода с используемыми показателями опасности сетевой атаки на АС

№ п/п	Название варианта подхода	Показатели опасности сетевой атаки
1	Полностью вероятностный $(p \cdot p)$	$p_u(d)$ – вероятность нанесения ущерба *d* при реализации *u*-й атаки; $p_u(t)$ – вероятность реализации *u*-й атаки за время t
2	Частично вероятностный $(d \cdot p)$	$\overline{d_u}$ – средний размер возможного ущерба, наносимого в результате реализации *u*-й атаки; $p_u(t)$ – вероятность реализации *u*-й атаки за время t

Первый вариант – полностью вероятностный $(p \cdot p)$. Он сводится к проведению оценки риска R в виде нахождения произведения вероятности $p_u(d_{\min} < d < d_{\max})$ того, что при реализации конкретной u-й атаки будет нанесен ущерб d, размеры которого находятся в некотором заданном диапазоне $(d_{\min}, d_{\max})$ и вероятности $p_u(t)$ реализации такой атаки за заданное время t:

$$R(d_{\min}, d_{\max}, t) = p(d_{\min} < d \le d_{\max}) \cdot p_u(t). \quad (3)$$

Сложность использования такого варианта подхода заключается в том, что необходимо определить плотности распределения вероятностей $w(u)$ нанесения ущерба, по которой может быть рассчитана вероятность.

Для непрерывного закона распределения вероятностей эта вероятность рассчитывается по формуле

$$p(d_{\min} < d \le d_{\max}) = \int_{d_{\min}}^{d_{\max}} w(x)dx\ , \quad (4)$$

а для дискретного – по формуле

$$p(d_{\min} < d \le d_{\max}) = \sum_i d_i \cdot p(d_i) \quad (5)$$

для всех i, для которых $d_{\min} < d_i \leq d_{\max}$.

Однако, как непрерывное, так и дискретное распределение вероятностей нанесения ущерба в подавляющем большинстве случаев неизвестно и принимаются разные допущения относительно законов распределения возможного ущерба.

В связи с этим широкое применение нашел *второй вариант* – частично вероятностный $(d \cdot p)$, в котором используется оценка среднего размера $\overline{d_u}$ возможного ущерба, наносимого в результате реализации u-й атаки, и вероятность $p_u(t)$ реализации u-й атаки за заданное время t. При этом риск R оценивается как произведение:

$$R_u(t) = \overline{d_u} \cdot p_u(t)\,. \tag{6}$$

Для расчета должны быть известны (разработаны) модель оценки размеров ущерба и модель оценки вероятностей реализации сетевой атаки, в результате которой этот ущерб будет нанесен.

Для проведения количественной оценки размеров ущерба необходимо связать вид наносимого ущерба с предметом реализуемой на АС типовой сетевой атаки – нарушением конфиденциальности, целостности или доступности обрабатываемой в системе информации.

С теоретической точки зрения наилучшим для построения модели риск-анализа должен стать такой подход к оцениванию ущерба, в рамках которого к одинаковой единице измерения приводится любой ущерб, нанесенный АС реализацией сетевых атак различных типов. Однако в настоящее время вопрос оценивания ценности информации еще недостаточно изучен для возможности однозначного определения единого эквивалента ущерба нарушений ее конфиденциальности, целостности или доступности (например, финансового).

При расчете размеров ущерба необходимо учитывать важность каждого из предметов атаки для каждой конкретной АС, исходя из ее специфики и предназначения. Следовательно, за основу величины нанесенного ущерба при построении риск-модели АС целесообразно принять количество успешно реализованных сетевых атак определенного типа, рассчитывая отдельно риск для каждого из предметов этих атак.

Для адекватного оценивания рисков при реализации сетевых атак на АС необходимо проанализировать функционирование системы на некотором временном интервале $t_1 \leq t \leq t_2$. С точки зрения рисков для АС данный промежуток времени характеризуется количеством и типом атак, реализованных в течение указанного периода.

С учетом выше изложенного величина информационного риска от реализации множества сетевых атак, относящихся к типу m, может быть рассчитана по формуле

$$R_m(t) = N_m \cdot p_m(t), \tag{7}$$

где N_m – количество успешно реализованных атак типа m, приводящих за время t к нанесению ущерба АС, соответствующего предмету атаки; $p_m(t)$ – вероятность реализации атаки типа m.

В результате величина интегрального информационного риска атакуемой АС от параллельной реализации множества сетевых атак, приводящих за заданное время t к нанесению определенного вида ущерба АС, определится по формуле

$$R(t) = \sum_{m=1}^{K} N_m \cdot \prod_{m=1}^{K} p_m\,(t), \tag{8}$$

где K – количество типов успешно реализованных атак.

3. Основные аспекты совершенствования показателей опасности сетевых атак на защищенные автоматизированные системы органов внутренних дел

Рассмотренный частично вероятностный вариант реализации вероятностного подхода может быть использован при формировании основных показателей для оценивания опасности сетевых атак на АС ОВД при условии учета особенностей и недостатков эксплуатации данных систем в защищенном исполнении на объектах информатизации ОВД.

Особенности и реально существующие недостатки эксплуатации защищенных АС ОВД раскрыты в [10]. Выделим те их них, которые оказывают максимальное влияние на опасность реализации сетевых атак и, соответственно, должны быть учтены при выборе и обосновании основных показателей опасности сетевых атак на защищенные АС, эксплуатируемые на объектах информатизации ОВД.

Опыт эксплуатации современных АС в защищенном исполнении на объектах информатизации ОВД показал, что из указанных в [10] особенностей максимальное влияние на опасность реализации сетевых атак оказывают: территориальная распределенность АС, интеграция служебной информации АС в единый массив банков данных различного уровня конфиденциальности, хранение больших массивов данных. Следовательно, в АС ОВД осуществляется распределенная обработка больших объемов служебной информации различных уровней конфиденциальности, влекущая значительное количество параллельно реализуемых сетевых атак различных типов. Поэтому при расчете интегрального информационного риска от параллельной реализации множества сетевых атак на АС ОВД необходимо учесть их взаимовлияние в процессе реализации.

Из представленных в [10] недостатков эксплуатации защищенных АС на объектах информатизации ОВД максимальное влияние на эффективность функционирования их СЗИ от НСД оказывает непосредственная зависимость ресурсоемкости СЗИ от НСД от вычислительного ресурса АС (процессорного времени, оперативной памяти, дискового пространства).

Таким образом, в качестве основного показателя опасности сетевых атак на защищенные АС, эксплуатируемые на объектах информатизации ОВД, целесообразно использовать напрямую зависимый от времени динамический интегральный показатель опасности атак $V_{\text{иоп ат}}$, обратно пропорциональный показателю временной эффективности функционирования СЗИ от НСД АС $V_{\text{вэ СЗИ}}$ ($V_{\text{иоп ат}} = \frac{1}{V_{\text{вэ СЗИ}}}$) и выражающий, соответственно, меру размера интегрального информационного риска атакуемой АС ОВД от параллельной реализации множества типовых сетевых атак. При этом под временной эффективностью СЗИ от НСД понимается ее способность выполнять заданные действия в интервал времени, отвечающий заданным требованиям[11]. Следовательно, показатель $V_{\text{вэ СЗИ}}$ отражает спектр свойств СЗИ от НСД с учетом динамики ее функционирования в АС ОВД.

Взаимосвязь интегрального показателя опасности сетевых атак и выявленного недостатка эксплуатации АС в защищенном исполнении на объектах информатизации ОВД представлена в таблице 3.

Интегральный показатель опасности сетевых атак $V_{\text{иоп ат}}$ сводит за счет процедуры агрегирования в единый показатель частные показатели опасности атак $V_{\text{оп ат}\,m}$ различных типов $(m = 1, \dots, k)$, выражающие размеры информационного риска от их реализации в АС ОВД.

[11]ГОСТ 28195-89. Оценка качества программных средств. Общие положения.

Таблица 3. Связь интегрального показателя опасности сетевых атак с основным недостатком применения СЗИ от НСД в защищенных АС ОВД

Показатель	**Смысловое значение показателя**	**Недостаток**	**Смысловое значение недостатка**
$V_{\text{иоп ат}}$ – интегральный показатель опасности сетевых атак	Неспособность СЗИ от НСД соответствовать заявленным требованиям (с точки зрения временных параметров ее функционирования), а также находить эффективное решение (разумный компромисс), связанное с совместным функционированием СЗИ от НСД и защищенной АС ОВД по ее прямому назначению (обработка, хранение и передача конфиденциальной информации)	Непосредственная зависимость ресурсоемкости СЗИ от НСД от вычислительного ресурса АС ОВД	Выполнение СЗИ от НСД защитных функций осуществляется в процессе функционирования защищенной АС ОВД, что приводит к снижению производительности системы за счет использования процедурой защиты части вычислительного ресурса АС в ущерб реализации ее целевых функций. Ограниченность вычислительного ресурса АС ОВД влечет за собой увеличение времени реализации СЗИ от НСД защитных Ограниченность вычислительного ресурса АС ОВД влечет за собой увеличение времени реализации СЗИ от НСД защитных функций и, как следствие, наблюдается несоответствие используемой СЗИ предъявляемым к ней требованиям по ЗИ

Задачу оценивания $V_{\text{иоп ат}}$ в математическом виде можно представить как нахождение отображения $F: V_{\text{иоп ат}} \to \{0,1\}$, где F определяет правила, реализуемые соответствующими моделями и алгоритмами.

Поскольку реализация сетевых атак на защищенные АС на объектах информатизации ОВД представляет собой сложный динамический процесс для его формального описания в настоящее время широко применяются модели, построенные на сетях Петри-Маркова (основанные на теории сетей Петри и марковских (полумарковских) процессах) [14-16], что позволяет определять ВВХ при исследовании реализации параллельных процессов с целью формирования показателей для проведения количественной оценки опасности реализации сетевых атак на информационный ресурс

защищенных АС ОВД [8, 10, 12].

Заключение

Анализ методической и научно-технической литературы по проблеме оценивания опасности реализации угроз НСД в АС, а также нормативной базы МВД России, регламентирующей эксплуатацию АС ОВД в защищенном исполнении, выявил ряд вопросов, требующих безотлагательного решения применительно к формированию основных показателей опасности сетевых атак на АС с целью повышения реальной защищенности данных систем при их эксплуатации на объектах информатизации ОВД:

1) существующие показатели опасности угроз ИБ, как правило, недостаточно адекватно отражают реальные свойства угроз удаленного доступа, реализуемых посредством сетевых атак на информационный ресурс защищенных АС на объектах информатизации ОВД, а, следовательно, не позволяют исследовать их в динамическом режиме и проводить количественную оценку опасности реализации угроз;

2) существующие показатели опасности сетевых атак не отражают особенности и реально существующие недостатки эксплуатации АС в защищенном исполнении на объектах информатизации ОВД, а, следовательно, не могут быть использованы при проведении количественной оценки опасности реализации сетевых атак на данные системы;

3) для проведения количественной оценки опасности реализации сетевых на защищенные АС ОВД и исследования их в динамическом режиме требуются: разработка динамического интегрального показателя опасности атак, отражающего реальные динамические свойства процесса реализации множества типовых сетевых атак на АС, эксплуатируемые в защищенном исполнении на объектах информатизации ОВД; совершенствование существующего математического обеспечения оценки опасности сетевых атак путем определения вероятностно-временных характеристик множественных параллельно реализуемых типовых атак на основе имитационного моделирования.

СПИСОК ЛИТЕРАТУРЫ:

1. Язов Ю.К. Защита информации в информационных системах от несанкционированного доступа / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2015. – 440 с.
2. Anisimov V.G. A risk-oriented approach to the control arrangement of security protection subsystems of information systems / V.G. Anisimov, P.D. Zegzhda, E.G. Anisimov, D.A. Bazhin // Automatic Control and Computer Sciences. 2016. Vol. 50. №. 8. P. 717–721. DOI: https://doi.org/10.3103/S0146411616080289.
3. Giannopoulos G. Risk assessment methodologies for Critical Infrastructure Protection / G. Giannopoulos, R. Filippini, M. Schimmer // European Commission Joint Research Centre Institute for the Protection and Security of the Citizen. Part I: A state of the art. Luxembourg: Publications Office of the European Union, 2017. – 45 p. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf (дата обращения: 19.01.2020).
4. Дровникова И.Г. Анализ существующих способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел и аспекты их совершенствования / И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Вестник Воронеж. ин-та МВД России. 2019. № 4. С. 51–63. URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik_4_2019.pdf (дата обращения: 19.01.2020).
5. Al Hadidi, Mazin & Al Azzeh, Jamil & Akhmetov, Berik & Korchenko, O. & Kazmirchuk, Svitlana & Zhekambayeva, M. (2016). Methods of Risk Assessment for Information Security Management. International Review on Computers and Software (IRECOS). DOI: https://doi.org/10.15866/irecos.v11i2.8233.
6. Lippmann R.P. Threat-based risk assessment for enterprise networks / R.P. Lippmann, J.F. Riordan // Lincoln Laboratory Journal. 2016. Vol. 22. № 1. P. 33–45. URL:https://www.ll.mit.edu/sites/default/files/publication/doc/threat-based-risk-assessment-enterprise-networks-lippmann-108609.pdf (дата обращения: 20.01.2020).
7. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2018. – 588 с. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_BIBL_A_012090330/ (дата обращения: 18.01.2020).

8. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: Воронеж. гос. тех. ун-т, 2013. – 265 с. URL: https://search.rsl.ru/ru/record/01007533232 (дата обращения: 18.01.2020).
9. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. М.: Компания АйТи; ДМК Пресс, 2016. – 384 с. URL: https://upravlenie-informaciodisus.ru/knigi/172587-1-petrenko-a-nnimi-riskami-ekonomicheski-opravdannaya-bezopasnost-petrenko-a-simonov-v-m-kompaniya.php (дата обращения: 22.01.2020).
10. Попов А.Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учетом их временных характеристик в автоматизированных системах органов внутренних дел: дис. канд. техн. наук: 05.13.19, Попов Антон Дмитриевич. Воронеж, 2018. – 163 с. URL:https://ви.мвд.рф/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (дата обращения: 22.01.2020).
11. Разработка моделей и алгоритмов оценки эффективности подсистемы защиты конфиденциальных сведений при ее проектировании в системах электронного документооборота ОВД: монография / Дровникова И.Г. и др. Воронеж: Воронеж. ин-т МВД России, 2019. – 116 с. URL:https://catalog.inforeg.ru/ Inet/GetEzineByID/325482 (дата обращения: 21.01.2020).
12. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. М: РадиоСофт, 2015. – 232 с. URL:http://www.sozvezdie.su/science/izdaniya/riskmodeli_informatsionnotelekommunikatsionnih/ (дата обращения: 24.01.2020).
13. Бокова, О.И., Дровникова, И.Г., Етепнев, А.С., Рогозин, Е.А., & Хвостов, В.А. (2019). Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах. Труды СПИИРАН, 18(6), 1301–1332. DOI: https://doi.org/10.15622/sp.2019.18.6.1301-1332.
14. M. El Hassan Charaf and S. Azzouzi, "A colored Petri-net model for control execution of distributed systems," 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, 2017. P. 0277–0282. DOI: https://doi.org/10.1109/CoDIT.2017.8102604.
15. L. Yao, P. Dong, T. Zheng, H. Zhang, X. Du and M. Guizani, "Network security analyzing and modeling based on Petri net and Attack tree for SDN," 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, 2016. P. 1–5. DOI: https://doi.org/10.1109/ICCNC.2016.7440631.
16. Дровникова И.Г. Создание модели информационного конфликта «нарушитель – система защиты» на основе сети Петри-Маркова / Вестник Воронеж. ин-та МВД России. 2019. № 2. С. 93–100. URL:https://ви.мвд.рф/upload/site132/document_journal/Vestnik_2_ 2019.pdf (дата обращения: 20.01.2020).

REFERENCES:

[1] Yazov Yu.K. Protection of information in information systems from unauthorized access Yu.K. Yazov, S.V. Solovyov. Voronezh: Quarter, 2015. – 440 p. (in Russian).
[2] Anisimov V.G. A risk-oriented approach to the control arrangement of security protection subsystems of information systems V.G. Anisimov, P.D. Zegzhda, E.G. Anisimov, D.A. Bazhin. Automatic Control and Computer Sciences. 2016. Vol. 50. №. 8. P. 717–721. DOI: https://doi.org/10.3103/S0146411616080289.
[3] Giannopoulos G. Risk assessment methodologies for Critical Infrastructure Protection G. Giannopoulos, R. Filippini, M. Schimmer. European Commission Joint Research Centre Institute for the Protection and Security of the Citizen. Part I: A state of the art. Luxembourg: Publications Office of the European Union, 2017. – 45 p. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf (accessed: 19.01.2020).
[4] Drovnikova I.G. Analysis of existing methods and procedures for assessing the risk of network attacks in automated systems of internal Affairs bodies and aspects of their improvement I.G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin. Vestnik of the Voronezh Institute of the Ministry of internal Affairs of Russia. 2019. № 4. P. 51–63. URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik_4_2019.pdf (accessed: 19.01.2020) (in Russian).
[5] Al Hadidi, Mazin & Al Azzeh, Jamil & Akhmetov, Berik & Korchenko, O. & Kazmirchuk, Svitlana & Zhekambayeva, M. (2016). Methods of Risk Assessment for Information Security Management. International Review on Computers and Software (IRECOS). DOI: https://doi.org/10.15866/irecos.v11i2.8233.
[6] Lippmann R.P. Threat-based risk assessment for enterprise networks R.P. Lippmann, J.F. Riordan. Lincoln Laboratory Journal. 2016. Vol. 22. № 1. P. 33–45. URL: https://www.ll.mit.edu/sites/default/files/publication/doc/threat-based-risk-assessment-enterprise-networks-lippmann-108609.pdf (accessed: 20.01.2020).
[7] Yazov Yu.K. Organization of information protection in information systems from unauthorized access: monograph Yu.K. Yazov, S.V. Solovyov. Voronezh: Kvarta, 2018. – 588 p. URL: https://rusneb.ru/catalog/

000200_000018_ RU_NLR_BIBL_A_012090330/ (accessed: 18.01.2020) (in Russian).

[8] Radko N.M. Penetration into the computer operating environment: models of malicious remote access N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh state technical University, 2013. – 265 p. URL: https://search.rsl.ru/ru/record/01007533232 (accessed: 18.01.2020) (in Russian).

[9] Petrenko S.A. Information risk management. Economically justified security S.A. Petrenko, S.V. Simonov. M: AiTi Company; DMK Press, 2016. – 384 p. URL: https://upravlenie-informaciodisus.ru/knigi/172587-1-petrenko-a-nnimi-riskami-ekonomicheski-opravdannaya-bezopasnost-petrenko-a-simonov-v-m-kompaniya.php (accessed: 22.01.2020) (in Russian).

[10] Popov A.D. Models and algorithms for evaluating the effectiveness of information protection systems against unauthorized access taking into account their time characteristics in automated systems of internal Affairs bodies: dis. cand. techn. sciences: 05.13.19, Popov Anton Dmitrievich. Voronezh, 2018. – 163 p. URL:https:// ви.мвд.рф/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (accessed: 22.01.2020) (in Russian).

[11] Development of models and algorithms for evaluating the effectiveness of the subsystem for protecting confidential information in its design in the electronic document management systems of ATS: monograph Drovnikova I.G. etc. Voronezh: Voronezh. in-t of the Ministry of internal Affairs of Russia, 2019. – 116 p. URL:https:// catalog.inforeg.ru/ Inet/GetEzineByID/325482 (accessed: 21.01.2020) (in Russian).

[12] Radko N.M. Risk models of information and telecommunication systems in the implementation of remote and direct access threats N.M. Radko, I.O. Skobelev. M: Radiosoft, 2015. – 232 p. URL:http://www.sozvezdie.su/science/izdaniya/riskmodeli_informatsionnotelekommunikatsionnih/ (accessed: 24.01.2020) (in Russian).

[13] Bokova, O. I., Drovnikova, I. G., Etepnev, A. S., Rogozin, E. A., & Khvostov, V. A. (2019). Methods of Estimating Reliability of Information Security Systems which Protect from Unauthorized Access in Automated Systems. SPIIRAS Proceedings, 18(6), 1301–1332. DOI: https://doi.org/10.15622/sp.2019.18.6.1301-1332 (in Russian).

[14] M. El Hassan Charaf and S. Azzouzi, "A colored Petri-net model for control execution of distributed systems," 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, 2017. P. 0277–0282. DOI: https://doi.org/10.1109/CoDIT.2017.8102604.

[15] L. Yao, P. Dong, T. Zheng, H. Zhang, X. Du and M. Guizani, "Network security analyzing and modeling based on Petri net and Attack tree for SDN," 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, 2016. P. 1–5. DOI: https://doi.org/10.1109/ICCNC.2016.7440631.

[16] Drovnikova I.G. Creating a model of information conflict «violator – protection system» based on the Petri-Markov network I.G. Drovnikova, M.S. Solomatin, E.A. Rogozin. Vestnik of the Voronezh Institute of the Ministry of internal Affairs of Russia. 2019. № 2. P. 93-100. URL:https://ви.мвд.рф/upload/site132/document_journal/Vestnik_2_2019.pdf (accessed: 20.01.2020) (in Russian).

Поступила в редакцию – 14 февраля 2020 г. Окончательный вариант – 17 августа 2020 г.
Received – February 14, 2020. The final version – August 17, 2020.