ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 519.7: 004.05
DOI:10.21822/2073-6185-2021-48-4-55-63

Оригинальная статья/Original Paper

Методика анализа рисков нарушения информационной безопасности на основе количественной оценки ущербов в информационно-технических системах органов внутренних дел

И.В.Алехин
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. Оценка последствий наступления случаев ущерба в информационно-технических системах (ИТС) органов внутренних дел (ОВД) требует применения анализа рисков наступления ущерба в результате реализации угроз информационной безопасности. **Метод.** Исследование основано на методах аналитического и математического моделирования с применением аппарата систем массового обслуживания. Для ИТС из-за высокой технологической сложности, высоких затрат на приобретение, обслуживание оборудования и выплаты заработной платы сотрудникам необходимо применение процедуры анализа рисков ИТС ОВД. Применяемый подход к определению мер безопасности информации, обеспечивающих определенный уровень защищенности функционирования ИТС ОВД, является нормативным, поскольку на данный момент в недостаточной степени развит метод количественной оценки ущербов. Развитие данного научного применения позволило бы установить целесообразное значение показателя допустимого риска реализации угроз безопасности информации. **Результат.** Приведена методика анализа рисков нарушения информационной безопасности на основе количественной оценки ущербов ИТС ОВД. **Вывод.** Направление данного исследования актуально и требует дальнейшей проработки с целью совершенствования метода оценки наступления ущерба в ИТС органов внутренних дел.

Ключевые слова: информационно-техническая система органа внутренних дел, система массового обслуживания, вероятность наступления ущерба, ресурс, угроза

Для цитирования: И.В. Алехин. Методика анализа рисков нарушения информационной безопасности на основе количественной оценки ущербов в информационно-технических системах органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2021; 48(4): 55-63. DOI:10.21822/2073-6185-2021-48-4-55-63

Methodology of information security risk analysis based on quantitative assessment of damages in information and technical systems bodies of the internal affairs

I.V. Alekhin
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. Assessment of the consequences of the occurrence of damage cases in the information and technical systems (ITS) of the internal affairs bodies (ATS) requires the use of an analysis of the risks of damage as a result of the implementation of information security threats. **Method.** In order to analyze the processes occurring in the ITS, as a rule, mathematical modeling is used. For ITS, due to the high technological complexity, high costs for the acquisition, maintenance of equipment and payment of wages to employees, it is necessary to apply the procedure for analyzing the risks of ITS ITS. The security of the functioning of the ITS ITS is normative, since at the moment the method of quantitative assessment of damages is insufficiently developed. The development of this scientific application would make it possible to establish the appropriate value of the indicator of the

permissible risk of the implementation of threats to information security. Analytical and mathematical modeling using the apparatus of queuing systems. **Result.** A technique for analyzing the risks of information security violations based on a quantitative assessment of the damages of the ITS of ATS is given. **Conclusion.** The direction of this study is relevant and requires further elaboration in order to improve the method for assessing the occurrence of damage in the ITS of the internal affairs bodies.

Keywords: information and technical system of the internal affairs body, queuing system, probability of damage, resource, threat

For citation: I.V. Alekhin. Methodology of information security risk analysis based on quantitative assessment of damages in information and technical systems bodies of the internal affairs. Herald of the Daghestan State Technical University. Technical Science. 2021; 48 (4): 55-63. DOI: 10.21822 / 2073-6185-2021-48-4-55-63

Введение. В практической деятельности возникают обстоятельства, при которых отдельные государственные информационные системы остаются неаттестованными из-за недостаточного финансирования [3], что является обязательным в соответствии с [4]. В [5] право и обязанность определения актуальных типов угроз лежит на операторе персональных данных, либо организации подрядчике. Заметим также, что в п. 10 [6] указано, что возможна корректировка отдельных выбранных мер по обеспечению безопасности персональных данных. Кроме того, в процессе эксплуатации аттестованной информационной системы также возникают нештатные ситуации. Так, при использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональным данным, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры, например, средства виртуализации. В [4] рассматривается понятие ущерба, разбивая его на три категории, что создает небольшую матричную градацию и ставит определение ущерба в прямую зависимость от мнения экспертов.

Широкое использование информационных систем в различных государственных организациях Российской Федерации влечет за собой обязательное выполнение требований по защите информации, содержащейся в таких системах. Из федерального закона № 3-ФЗ «О полиции» от 07.02.2011, следует, что Министерство внутренних дел обязано использовать в процессе выполнения возложенных государственных функций широкий набор информационных технологий и информационных систем с целью получения, накопления и обработки информации. В соответствии с положениями Методики оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021, на этапе определения негативных последствий от реализации (возникновения) угроз безопасности информации исходными данными выступают результаты оценки рисков (ущерба). Затем, на основе анализа исходных данных определяются событие или группы событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) организации.

Постановка задачи. В ИТС ОВД существует потенциальная опасность наступления случаев ущерба от реализации уязвимостей. Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (Концепция), утвержденная приказом МВД России от 14.03.2012 № 169, указывает направление деятельности по обеспечению информационной безопасности ОВД проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки. В соответствии Концепцией целью обеспечения информационной безопасности ОВД является достижение с использованием методов технической защиты информации необходимого уровня защиты, а основной задачей обеспечения информационной безопасности ОВД является создание и развитие информационной безопасности ОВД с учетом технологии «облачной архитектуры». Проблемой, требующей решения, является количественная оценка рисков наступления ущерба, потому что она влияет на дальнейшие мероприятия по обработке риска.

Таким образом, целесообразно разработать методику оценки рисков наступления ущерба в ИТС ОВД, учитывающую финансовые затраты на организационно-технические мероприятия по обеспечению информационной безопасности. Эффективное использование финансовых ресурсов позволит поддерживать на достаточном уровне показатель допустимого риска. На этапе ввода в эксплуатацию, а также последующего использования, требуются значительные финансовые затраты, включающие: оплату труда ведомственных специалистов; оплату услуг привлекаемых лицензированных юридических лиц; закупку лицензированного программного обеспечения; закупку средств защиты информации; оплату технической поддержки и обновлений программного обеспечения.

Методы исследования. Анализ [7] позволил привести схему, которую целесообразно усовершенствовать финансовым показателем затрат (рис.1).

Одним из аспектов совершенствования методики является дополнение стандартной цепочки жизни ИТС ОВД ежегодным анализом рисков классов угроз. В блоке «Результаты оценки риска», подчиненных какому-либо закону распределения плотности вероятности наступления ущерба, можно существенно повысить защищенность ИТС ОВД, актуализируя риски в наиболее значимом интервале риска и сопоставляя с объемом финансовых средств в текущем году.

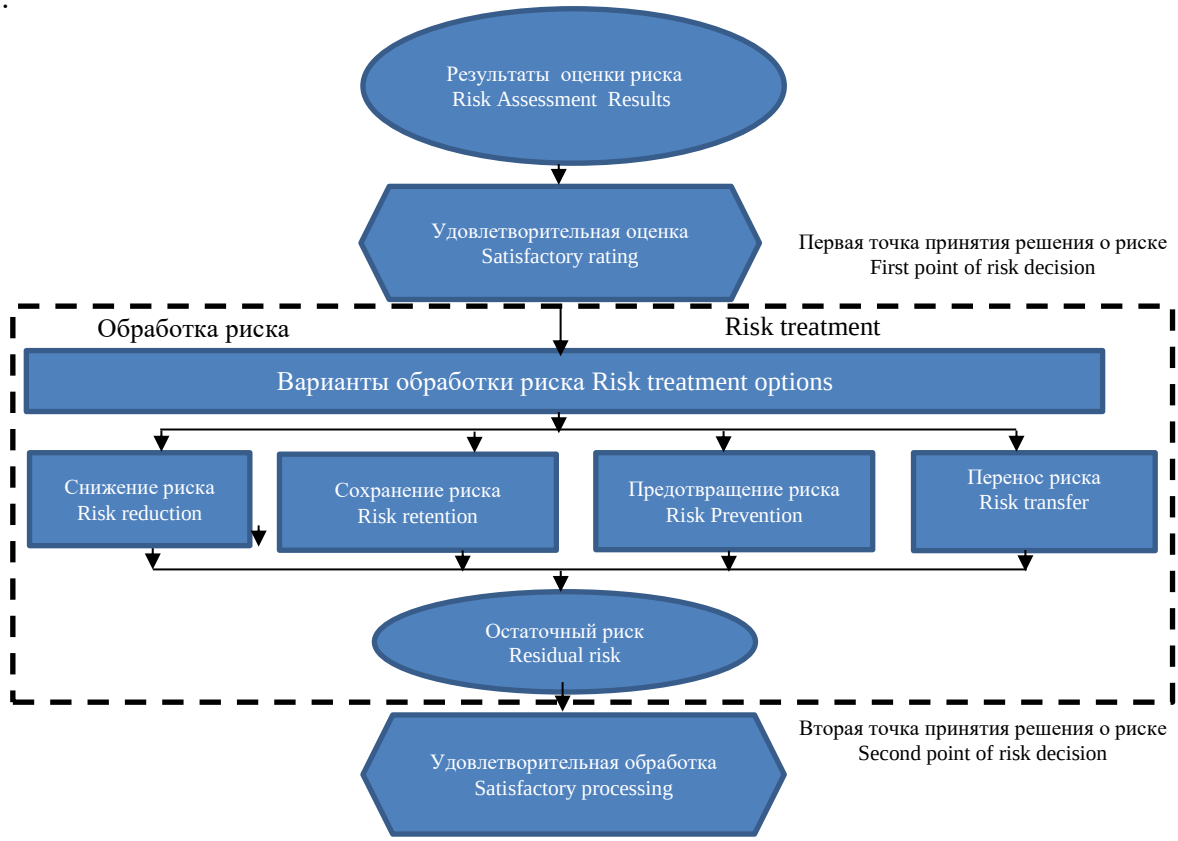

Рис. 1. Процесс обработки риска
Fig. 1. Risk treatment process

Такой подход позволит повысить реальную защищенность информационных ресурсов. Как показывает практика, вирусные атаки успешно происходят в криптографически защищенных сетях [8]. Необходимо проводить постоянные мероприятия, для которых требуются человеческие и финансовые ресурсы.

Вместе с тем, параметризация приведенных распределений [9] совместно с финансовой составляющей является крайне важным аспектом. Дополним данный алгоритм опубликованным ранее математическим аппаратом [9]. Введем новые понятия: коэффициент изменения риска:

$$K_{risk} \equiv K_R = \frac{Risk_2}{Risk_1} \equiv \frac{R_2}{R_1}, \tag{1}$$

где $Risk_1 \equiv R_1$ и $Risk_2 \equiv R_2$.

Это – значения риска, соответственно, первоначальные и после проведения организационно-технических мероприятий по защите информации (ОТМЗИ), что соответствует блоку обработка риска.

Отметим, что после проведения ОТМ при $K_R = 0$ угроза отсутствует полностью. Значение коэффициента изменения риска K_R для эффективной защиты от потенциальных угроз должен быть меньше, а желательно гораздо меньше единицы, т.е. $R_2 << R_1$.

$$K_R = \frac{R_2}{R_1} << 1, \tag{2}$$

В данном коэффициенте следует учесть затраты на ОТМЗИ. Данный параметр целесообразно использовать для анализа эффективности применения тех или иных ОТМЗИ, направленных на повышение защищенности информации, повышение информационной безопасности, уменьшение вероятности возникновения угроз и т.д.

$$K_R(u_1,u_2) \equiv K_R = \frac{R_2}{R_1} = \frac{u_2 P_2(u_2)}{u_1 P_1(u_1)}, \tag{3}$$

здесь R_u и $P_2(u_2)$ – соответственно вероятности наступления ущерба до и после реализации ОТМЗИ по ущербам u_1 и u_2.

Если величина ущерба не изменяется $u_1 = u_2 = u$ (изменяется только вероятность его наступления), то

$$K_R(u_1,u_2)\big|_{u_1 = u_2 = u} \equiv K_R = \frac{R_2}{R_1} = \frac{uP_2(u)}{uP_1(u)} = \frac{P_2(u)}{P_1(u)}. \tag{4}$$

Здесь целесообразно учесть материальные затраты на ОТМЗИ. Таким образом введем ещё один коэффициент изменения риска, учитывающий затраты на ОТМЗИ:

$$K_{RC} = \frac{u_2 P_2(u_2) + C}{u_1 P_1(u_1)} = \frac{R_2 + C}{R_1} = \frac{R_{2C}}{R_1}. \tag{5}$$

Затраты (С), например, в рублевом эквиваленте, можно включить (в общем смысле) в величину риска R_2 после ОТМЗИ, т.к. риск по затратам равен величине затрат, умноженной на вероятность возникновения затрат, которая равна единице. R_{2C} – это величина риска после ОТМЗИ, с учетом материальных затрат на ОТМЗИ.

Рассматривая класс угроз «отказ в обслуживании» применительно к деятельности ОВД, можно выделить ряд параметров, отражающих финансовые потери при успешной реализации угрозы – начальный и конечный интегральный показатель ущерба до и после реализации ОТМЗИ, соответственно, с учётом затрат $\sum_{i=1}^{n} u$.

В рамках данного научного исследования приведем классификацию ущербов от реализации актуального класса угроз для ИТС ОВД [2]:

1. Ущерб, обусловленный нарушением целостности и доступности пользовательской и технологической информации;

2. Финансовый (материальный) ущерб: упущенная выгода; уничтожение или вывод из строя оборудования; уничтожение иных материальных средств; финансовые затраты: затраты на повторное формирование пользовательских данных, разработку и (или) закупку и инсталляцию прикладного или системного программного обеспечения; затраты на защиту информации – закупку, установку, конфигурирование и сопровождение эксплуатации средств защиты, резервирование программных и аппаратных средств, организацию и проведение организационно-

технических мероприятий по защите, обучение персонала и др.; затраты на восстановление, ремонт или замену аппаратного обеспечения, вывод из строя которого вызван нарушениями безопасности информации.

3. Финансовые потери: потери в результате простоя и невозможности использования ИТС ОВД или её элементов; потери, вызванные использованием конфиденциальной информации во вред ОВД или преднамеренной несанкционированной модификацией данных или прикладных программ; штрафы за нарушения установленных договоренностей или правовых норм.

4. Ущерб здоровью людей, вызванный перебоями в управлении силами и средствами ОВД.

5. Экономический (дополнительные трудозатраты) ущерб: трудозатраты на восстановление, ремонт оборудования; трудозатраты на восстановление, настройку прикладного и системного ПО;

6. Моральный ущерб: от снижения или потери деловой репутации организации или физического лица; от невозможности выполнения взятых на себя обязательств перед третьей стороной; от разглашения персональных данных отдельных лиц; от дезорганизации деятельности организации или его отделений; от нарушения правовых норм.

7. Ущерб при чрезвычайных ситуациях.

Обсуждение результатов. На основании вышеизложенного в работе предложена методика анализа рисков ущерба в ИТС ОВД с учетом эффективности финансовых затрат на ОТМЗИ. Методика состоит из реализации следующих этапов:

1. Получение функции плотности вероятности параметра, характеризующего состояние атакованной системы.

2. Оценка тяжести ущерба группой экспертов путем применения метода анализа иерархий для случая DDoS-атаки. С целью уточнения тяжести ущерба оценка производится по семи категориям ущерба.

3. Получение значения интегрального показателя риска до проведения ОТМЗИ.

4. Разработка возможных наборов ОТМЗИ.

5. Получение значений интегрального показателя риска после проведения ОТМЗИ для каждого набора.

6. Расчет интегрального показателя риска после проведения ОТМЗИ. Применение коэффициента с учетом затрат на наборы ОТМЗИ.

7. Определение оптимального набора ОТМЗИ на основе сравнения коэффициентов риска и нахождения искомых значений в полуинтервале [0;1].

Применим методику для модели ИТС ОВД на примере Воронежского института МВД России в связи с высокой важностью доступности образовательных ресурсов в период дистанционного обучения.

Актуальными угрозами будем считать УБИ.140 и УБИ.164, которые возможны для удаленной реализации и высокодоступны. Получим 20 значений плотности вероятности наступления ущерба $\mathrm{P}(t)$, используя модель при заданных начальных параметрах.

При этом $\mathrm{P}(t_{max}) \rightarrow \min$. Экспертным методом произведем оценку ущерба за сутки по приведенным выше категориям в условных единицах до проведения ОТМЗИ (табл. 1).

Оценку будем производить при помощи программного комплекса, реализованного на языке программирования PHP.

Применение данного программного комплекса позволяет упростить и автоматизировать процесс оценки рисков (ущербов) от реализации угроз информационной безопасности в ИТС ОВД.

Таблица 1. Значения риска до организационно-технических мероприятий по защите информации

Table 1. Risk values before organizational and technical measures to protect information

№ п/п	Интервалы сгруппированных данных, t_i Grouped data intervals		Количество утерянных пакетов, n_i Number of packages lost	Значения функции плотности вероятности наступления ущерба, p_i Values of the loss probability density function	Значения риска Risk values $R_{i_{\text{до отмзи}}}$
1.	4,0000	4,2445	0,0001	0,000000061	0,00251
2.	4,2445	4,4890	0,001	0,00000061	0,02509
3.	4,4890	4,7335	0,02	0,0000123	0,50186
4.	4,7335	4,978	0,381	0,000236	9,56041
5.	5,2225	5,467	3,191	0,001977	80,07156
6.	5,467	5,7115	14,731	0,00912	369,6441
7.	5,7115	5,956	43,592	0,027	1093,851
8.	5,956	6,2005	91,945	0,0569674	2307,17
9.	6,2005	6,445	149,155	0,092413	3742,737
10.	6,445	6,6895	196,796	0,12193	4938,19
11.	6,6895	6,934	220,228	0,136	5526,167
12.	6,934	7,1785	215,823	0,1337	5415,633
13.	7,1785	7,423	189,865	0,1176	4764,27
14.	7,423	7,6675	152,883	0,0947	3836,283
15.	7,6675	7,912	114,432	0,07089942	2871,435
16.	7,912	8,1565	80,611	0,04994	2022,767
17.	8,1565	8,401	53,985	0,033448	1354,642
18.	8,401	8,6455	34,655	0,02147	869,5957
19.	8,6455	8,89	21,468	0,0133	538,6952
20.	8,89	9,1345	12,9	0,007997	323,6989

Программно-методический комплекс представляет собой программу для расчёта величины показателей наступления ущерба по семи категориям (рис. 2).

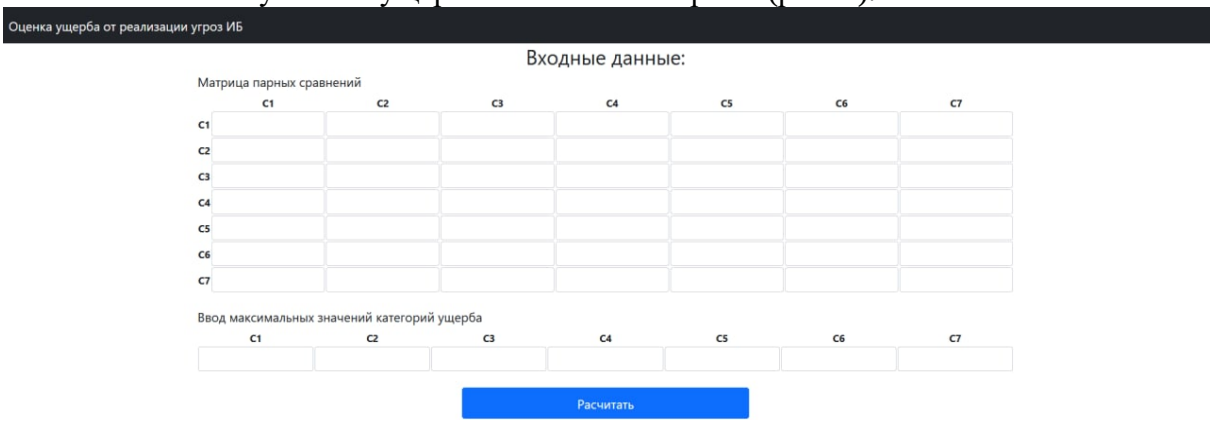

Рис. 2. Интерфейс программы для расчёта матрицы парных сравнений по семи категориям ущерба

Fig. 2. Program interface for calculating the matrix of paired comparisons for seven categories of damage

Поля ввода предназначены для ввода экспертом оценки значимости категории ущерба попарно, допускаются значения от 1 до 10. Буквами $C_1, \dots, C_7$ обозначены рассматриваемые категории ущерба. После ввода необходимых для расчёта данных необходимо ввести максимальные значения по семи категориям ущерба (рис. 3).

При нажатии кнопки «рассчитать», производится расчёт путем перемножения значимости категории ущерба и соответствующего максимального значения. Вычисленное значение: $U_{\sum_{\text{до отмзи}}} = 810980$ у.е.

Рис. 3. Интерфейс программы для ввода максимальных значений ущерба по 7 категориям
Fig. 3. Program interface for entering maximum damage values in seven categories

Получим значения функции плотности вероятности наступления ущерба путем деления значения количества потерянных пакетов во временном интервале на общее количество потерянных пакетов. Результатом является произведение суммы ущерба по семи категориям и значения функции плотности вероятности наступления ущерба на исследуемом интервале:

$$R_{i_{\text{до ОТМЗИ}}} = p_i \times U_{\sum_{\text{до ОТМЗИ}}}. \quad (6)$$

На основании этой функции риска получим интегральный показатель риска:

$$R_{\Sigma_{\text{до ОТМЗИ}}} = \frac{R_1 + \cdots + R_n}{n}. \quad (7)$$

На основе построенного графика функции риска убедимся, что ранее выдвинутая гипотеза подтверждается (рис. 4). Полученная функция риска подчиняется закону распределения Вейбулла.

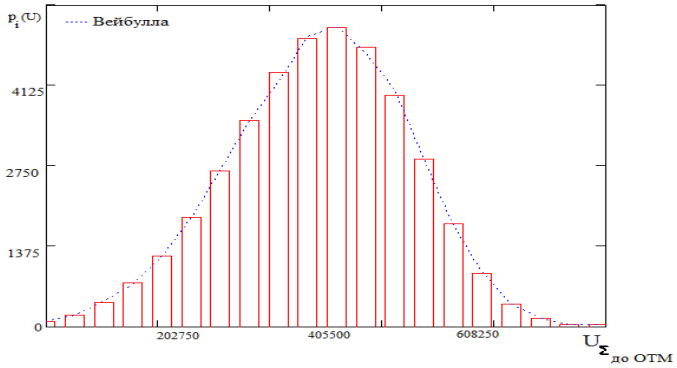

Рис. 4. График распределения функции риска
Fig. 4. Graph of the distribution of the risk function

Применительно к данному случаю предложим два обобщенных набора ОТМЗИ в рамках годового цикла:

1. Улучшение производительности ИТС ОВД силами сотрудников подразделения с целью увеличения пропускной способности серверного и сетевого оборудования.

Оценим стоимость данного набора ОТМЗИ в 110000 у.е. в связи с затратами на модернизацию путем увеличения производительности серверного оборудования, расширения пропускной способности и дублирования канала связи, а также разработки скриптов обработки входящего трафика с целью блокировки ip-адресов злоумышленников и жертв ботнет-сети, направляющих большое количество однотипных запросов.

2. Приобретение специализированных программных решений от организаций, занимающихся подобным на стороне клиента.

Оценку данного набора ОТМЗИ произведем на основе стоимости услуг лаборатории Касперского [10]. Стоимость решения по защите от подобных угроз составит 250000 у.е. В рамках данного вычислительного эксперимента будем считать, что результаты проведенных ОТМЗИ близки. Значение интегрального ущерба на основании экспертной оценки [11, 12] снизится $U_{\sum_{\text{после ОТМЗИ}}} = 14755$ у.е.

Также заметим, что со снижением вероятного ущерба уменьшатся и значения риска наступления ущерба после применения ОТМЗИ (табл. 2). С целью точного определения величины затрат C_1 и C_2 на ОТМЗИ разделим затраты на 365 дней. Произведем расчет интегрального показателя риска до проведения ОТМЗИ и после, соответственно, с учетом затрат на наборы ОТМЗИ.

Таблица 2. Значения риска после организационно-технических мероприятий по защите информации

Table 2. Risk values after organizational and technical measures to protect information

№ п/п	Интервалы сгруппированных данных, t_i Grouped data intervals		Количество утерянных пакетов, n_i Number of packages lost	Значения функции плотности вероятности наступления ущерба, p_i Values of the loss probability density function	Значения риска Risk ues$R_{i_{\text{после ОТМЗИ}}}$
1.	4,0000	4,2445	0,0001	0,00000039	0,0029
2.	4,2445	4,4890	0,001	0,0000039	0,02905
3.	4,4890	4,7335	0,02	0,0000787	0,58091
4.	4,7335	4,978	0,081	0,000319	2,35267
5.	5,2225	5,467	0,191	0,000752	5,54765
6.	5,467	5,7115	1,2	0,004724	34,85433
7.	5,7115	5,956	4,71	0,018543	136,8032
8.	5,956	6,2005	12,945	0,050965	375,9911
9.	6,2005	6,445	26,56	0,104567	771,4425
10.	6,445	6,6895	28,37	0,111693	824,0145
11.	6,6895	6,934	32,341	0,127327	939,3533
12.	6,934	7,1785	33,83	0,133189	982,6017
13.	7,1785	7,423	31,95	0,125787	927,9966
14.	7,423	7,6675	24,83	0,097756	721,1942
15.	7,6675	7,912	20,232	0,079654	587,644
16.	7,912	8,1565	16,99	0,06689	493,4792
17.	8,1565	8,401	10,114	0,039819	293,7639
18.	8,401	8,6455	4,53	0,017835	131,5751
19.	8,6455	8,89	3,8	0,014961	110,372
20.	8,89	9,1345	1,15	0,004528	33,402

Применим коэффициент риска для оценки эффективности примененных наборов ОТМЗИ:

$$R_{\Sigma_{\text{до ОТМЗИ}}} = 2004{,}56;$$

$$R_{\Sigma_{\text{после ОТМЗИ}}} = 737{,}05;$$

$$K_R = \frac{R_{\Sigma_{\text{после ОТМЗИ}}} + C_1}{R_{\Sigma_{\text{до ОТМЗИ}}}} = \frac{737{,}05 + 301{,}36}{2004{,}55} = 0{,}518.$$

$$K_R = \frac{R_{\Sigma_{\text{после ОТМЗИ}}} + C_2}{R_{\Sigma_{\text{до ОТМЗИ}}}} = \frac{737{,}05 + 684{,}931}{2004{,}55} = 0{,}7093$$

Оба значения находятся в полуинтервале [0;1], что свидетельствует об оптимальности [13, 14]. Первый из двух рассматриваемых наборов ОТМЗИ является оптимальным.

Вывод. Разработана и предложена методика анализа рисков нарушения информационной безопасности на основе количественной оценки ущербов ИТС ОВД. Применение данной методики позволит повысить финансовую эффективность затрат на эксплуатацию и информационную безопасность ИТС ОВД. Эффективное использование финансовых ресурсов позволит поддерживать на достаточном уровне показатель допустимого риска.

Библиографический список:

1. Астахов А. М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.
2. Язов Ю. К., Соловьев С. В. Организация защиты информации в информационных системах от несанкционированного доступа. Монография. Воронеж: Кварта, 2018. 588 с.
3. URL:https://news.mail.ru/politics/36045077.
4. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных».
7. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст).
8. URL:https://news2.ru/story/520757/.
9. Голубинский А. Н. О математических моделях ущербов и рисков возникновения угроз в информационно-технических системах / А. Н. Голубинский, И. В. Алехин // Международная научно-практическая конференция «Охрана, безопасность, связь – 2015»: Сборник материалов. Часть 3. Воронеж: Воронежский институт МВД России, 2016. С. 109–115.
10. URL:https://store.softline.ru/kaspersky/kl4646raafs-4300
11. Алехин И. В. К вопросу о вероятности наступления ущерба в результате атаки на информационный ресурс информационно-технических систем органов внутренних дел типа «отказ в обслуживании». Алехин И. В., Бокова О. И., Рогозин Е. А., Коробкин Д. И. Вестник Дагестанского государственного технического университета. Технические науки. 2018. Т. 45. № 4. С. 68-77. DOI:10.21822/2073-6185-2018-45-4-68-77
12. Организационно-экономическое моделирование : учебник : в 3ч. / А. И. Орлов. М.: Изд-во МГТУ им. Н. Э. Баумана. 2009 Ч. 2: Экспертные оценки. 2011. 486 с.
13. Голиусов А. А., Дубровин А. С., Лавлинский В. В., Рогозин Е.А. Методические основы проектирования программных систем защиты информации. Воронеж: ВИРЭ, 2002. 96 с.
14. Expert assessments in an innovative environment of the optimization of the information security process in the digital educational environment Alekhin I. V., Rogozin E. A., Vorobyov E. I., Belyaev R. V. *Journal of Physics: Conference Series.* Krasnoyarsk Science and Technology City Hall. Krasnoyarsk, Russian Federation, 2020; 12060.

References:

1. Astakhov AM Art of information risk management. Moscow: *DMK Press*, 2010;312 (In Russ)
2. Yazov Yu. K., Soloviev SV Organization of information protection in information systems from unauthorized access. Monograph. Voronezh: [Kvarta] *Quarta*, 2018; 588. (In Russ)
3. URL:https://news.mail.ru/politics/36045077.
4. Order of the FSTEC of Russia dated 11.02.2013 No. 17 "On approval of the Requirements for the protection of information that does not constitute a state secret contained in state information systems." (In Russ)
5. Decree of the Government of the Russian Federation of 01.11.2012 No. 1119 "On approval of requirements for the protection of personal data during their processing in personal data information systems." (In Russ)
6. Order of the FSTEC of Russia dated February 18, 2013 N 21 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in the personal data information system." (In Russ)
7. National standard of the Russian Federation GOST R ISO / IEC 27005-2010 "Information technology. Methods and means of ensuring security. Information security risk management" (approved by order of the Federal Agency for Technical Regulation and Metrology of November 30. 2010; 632(In Russ)
8. URL:https://news2.ru/story/520757/.
9. Golubinsky A. N. On mathematical models of damages and risks of threats in information and technical systems / A. N. Golubinsky, I. V. Alekhin // International Scientific and Practical Conference " Security, safety, communications - 2015": Collection materials. Part 3. Voronezh: *Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2016; 109–115. (In Russ)
10. URL:https://store.softline.ru/kaspersky/kl4646raafs-4300
15. Alekhin I. V. To the question of the probability of damage as a result of an attack on an information resource of information and technical systems of internal affairs bodies of the "denial of service" type Alekhin I. V., Bokova O. I., Rogozin E. A., Korobkin D.I. [Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskiye nauki.]*Herald of the Dagestan State Technical University. Technical Science.* 2018; 45(4): 68-77. DOI:10.21822/2073-6185-2018-45-4-68-77 (In Russ)
11. Organizational and economic modeling: textbook: in 3 hours . / AI Orlov. *Publishing house of MSTU im. N.E.Bauman*. 2009 Part 2: Expert assessments. 2011; 486. (In Russ)
12. Goliusov A.A., Dubrovin A.S., Lavlinsky V.V., Rogozin E.A. Methodological foundations for the design of software information security systems. Voronezh: VRE, 2002; 96. (In Russ)
13. Expert assessments in an innovative environment of the optimization of the information security process in the digital educational environment Alekhin I. V., Rogozin E. A., Vorobyov E. I., Belyaev R. V. In the collection: *Journal of Physics*: Conference Series. Krasnoyarsk Science and Technology City Hall. Krasnoyarsk, Russian Federation, 2020; 12060. (In Russ)

Сведения об авторе:

Алехин Игорь Викторович, старший инженер-электроник отдела информационно-технического обеспечения учебного процесса ialekhin2@mvd.ru

Information about the author:

Igor V. Alekhin, Senior Electronics Engineer, Department of Information and Technical Support of the Educational Process ialekhin2@mvd.ru

Конфликт интересов/ Conflict of interest.

Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.

Поступила в редакцию/Received 10.11.2021.

Одобрена после/рецензирования Reviced 30.11.2021.

Принята в печать/ Accepted for publication 01.12.2021.