УДК 004.056

Н.Н. Баранова, Ю.В. Орлов

НАДЕЖНОСТЬ МОДУЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИБОРОСТРОИТЕЛЬНЫХ ПРЕДПРИЯТИЙ

Баранова Наталья Николаевна, *окончила механико-математический факультет Ульяновского государственного университета. Ведущий инженер по защите информации АО «УКБП», г. Ульяновск. Имеет статьи по защите информации. [e-mail: natasha_bn@mail.ru].*

Орлов Юрий Владимирович, *окончил математико-механический факультет Уральского государственного университета. Старший преподаватель кафедры физико-математических дисциплин Новоуральского технологического института национального исследовательского ядерного университета Московского инженерно-физического университета. Имеет статьи по моделированию и анализу случайных процессов. [e-mail: orlove79@yandex.ru].*

Аннотация

В статье представлен модульный подход к проектированию системы защиты информации приборостроительного предприятия. Оценку надежности спроектированной системы защиты предлагается осуществлять в три этапа. Рассмотрен способ оценки надежности модульной системы защиты информации при заданном количестве выполняемых предприятием работ, а также способ оценки поведения данной системы при увеличении количества работ. Изучены методы оценки вероятности проявления угроз безопасности информации, вероятности нанесения ущерба при обнаружении и необнаружении проявившейся угрозы, вычисления надежности системы. Представлен способ расчета надежности модульной системы защиты информации при выполнении нескольких однотипных работ. Показаны значимость фрагментации модулей защиты при воздействии угроз безопасности и влияние данного подхода на общую надежность системы защиты информации приборостроительного предприятия.

Ключевые слова: модульная система защиты информации, надежность системы защиты информации, информационная безопасность, угрозы безопасности информации.

THE RELIABILITY OF A MODULAR INFORMATION SECURITY SYSTEM IN INSTRUMENT-MAKING ENTERPRISES

Natalia Nikolaevna Baranova, *graduated from the Faculty of Mechanics and Mathematics of Ulyanovsk State University; Leading Information Security Engineer at Ulyanovsk Instrument Manufacturing Design Bureau, JSC; an author of articles in the field of information security. e-mail: natasha_bn@mail.ru.*

Iurii Vladimirovich Orlov, *graduated from the Faculty of Mechanics and Mathematics of Ural State University; Senior Lecturer of the Department of Physics and Mathematics of Novouralsk National Research Nuclear University of MEPhI; an author of articles in the field of simulation and analyzing of random processes. e-mail: orlove79@yandex.ru.*

Abstract

The article presents a modular approach to the design of information security system in an instrument-making enterprise. It is proposed to assess the reliability of the designed information security system in three stages. The method for evaluating the reliability of a modular information security system at a given amount of work performed in an instrument-making enterprise as well as a method for the system behavior evaluation when increasing the amount of work are described. Methods for assessment of the information security threat performance probability, the damage probability upon detection and non-detection of the performed threats as well as for the calculation of the system reliability are considered. The method for calculating the reliability of the modular information security system when performing of several similar tasks is presented. The importance of fragmentation of modules under the influence of security threats and the impact of this approach on the overall reliability of the system in an instrument-making enterprise are shown.

Key words: modular information security system, reliability of information security system, information security, information security threats.

Введение

Разработка авиационных изделий представляет собой процесс, состоящий из последовательно выполняемых этапов (разработка эскизного проекта, разработка технического проекта, разработка рабочей конструкторской документации для изготовления опытного образца изделия и т. д.). Этапы производства и выпуска изделий также утверждены соответствующими нормативными документами.

На сегодняшний день каждое предприятие для защиты своих проектных решений использует подход, при котором специалистам по информационной безопасности (ИБ) предлагается составить классификацию видов обрабатываемой на предприятии информации по степени важности, выделить ресурсы, обрабатывающие данную информацию, и коммутационные средства, используемые для ее транслирования, а также определить виды прав доступа к информации. После проведенного обследования предприятия и сбора необходимой информации специалисты по ИБ предлагают механизмы защиты ценной информации, содержащие организационные и технические решения [1–4]. Такая последовательность при проектировании системы защиты информации (СЗИ) является хорошим решением для организаций с замкнутым производственным циклом, где информационная среда подвергается изменениям с малой периодичностью. Для крупных приборостроительных предприятий, где каждая опытно-конструкторская работа (ОКР) – это новые кооперационные связи (привлечение к работе соисполнителей, закупка дисплеев и других элементов у иностранных производителей и т. д.), новые нестандартные решения в разработке и производстве (собственное производство оснасток и т. д.). Для них данный устоявшийся механизм приводит к частому пересмотру СЗИ в части включения в ее состав новых компонентов защиты (коммутационного оборудования, совместного процесса обработки информации как на стороне предприятия, так и на стороне привлекаемого к работе соисполнителя) для того, чтобы подстроиться под новые требования разработки.

Актуальной задачей для специалистов по ИБ в данной ситуации является оценка надежности СЗИ приборостроительного предприятия.

В данной статье рассмотрим метод оценки поведения системы при заданном количестве выполняемых работ, а также оценки системы при увеличении количества работ.

Постановка задачи

Специалистам по ИБ на этапе сбора данных необходимо проводить исследование не всего предприятия в целом и его информационной системы, как это предлагалось ранее, а его отдельных элементов, используемых в конкретной рассматриваемой ОКР, конкретного этапа проектирования. Представим систему защиты в виде ***модулей защиты*** для каждого этапа проектирования и покажем способ расчета надежности СЗИ (устойчивости противодействия угрозам безопасности информации), зависящей от надежности каждого этапа. При этом предусмотрим возможность фрагментации модуля защиты, в случае его повреждения (в результате воздействия атаки) для сохранения заданного уровня надежности системы и ее устойчивого функционирования.

Решение поставленной задачи будем производить в три этапа. На первом этапе мы определим вероятность проявления угроз безопасности информации для выбранного этапа или проектной процедуры. На втором этапе произведем оценку ущерба при проявлении угрозы. На третьем этапе оценим надежность системы без резервных вариантов и с ними.

Этап 1. Оценка вероятности проявления угроз безопасности

За временной промежуток, обозначенный условиями договора на выполнение работы, процесс проектирования изделия подвергается воздействию различных угроз безопасности. Поэтому одной из первых и приоритетных задач, которую необходимо выполнить, будет выявление и формирование множества актуальных угроз безопасности для исследуемого процесса (этапа) разработки.

В настоящее время известно большое количество методов для расчета вероятности проявления угрозы безопасности: к ним относятся вероятностные методы, экспертные методы оценки и т. д. Рассмотрим их более подробно с точки зрения применимости в решении нашей задачи, а именно расчета вероятности проявления угрозы безопасности при проектировании изделий.

Учитывая, что спектр угроз, которым подвергается процесс (этап) проектирования и проектное решение, является достаточно широким, для удобства расчета разобьём их на небольшое число типов (случайные внутренние, случайные внешние и т. д.). Для каждого из них оценим вероятность проявления угрозы этого типа. Широкое распространение при решении данной задачи получили экспертные оценки, которые позволяют оценить вероятность проявления угрозы за время выполнения всего процесса и последствия риска [2, 5].

Использование статистических данных о проявлении угроз безопасности проектных решений за аналогичный период позволяет получить более точные оценки. Предположим, что условия процесса проектирования мало отличаются от тех, при которых была собрана статистика. Например, угрозы безопасности, которым подвергаются проектные решения при разработке датчика аварийного освещения на различные борта воздушных судов гражданского назначения, схожи между собой. Это обусловлено тем, что в процессе разработки задействованы специалисты и аналогичное количество ресурсов, качественные характеристики которых также схожи.

Будем считать, что угрозы безопасности независимы друг от друга и от хода выполнения работ, вероятность одновременного наступления угроз не отличается от произведений их вероятностей.

Еще одним методом оценки вероятности появления угроз является метод, который заключается в использовании статистической информации о проявлении данного вида угрозы за определенный временной период и нахождении среднего значения до первого проявления. После проведения данного расчета можно оценить вероятность проявления угроз за минимально учитываемый промежуток времени (день, час, минута и т. д.).

Для оценки вероятности числа угроз считают, что такая случайная величина имеет распределение Пуассона. Тогда по среднему количеству проявлений угроз λ за базовый промежуток времени процесса можно найти вероятность k проявлений угроз по формуле Пуассона: $P(k)=\frac{\lambda^k}{k!}\cdot e^{-\lambda}$ [6–8]. При необходимости анализа угроз на выбранном (рассматриваемом) промежутке времени найдём t стандартных промежутков и применим формулу Пуассона при $\lambda_1=\lambda\cdot t$.

Пример 1: Если в среднем за год фиксируется три угрозы данного типа, то каковы вероятности хотя бы одной такой угрозы:

а) за один день;

б) за 130 дней.

Решение: Пусть в году 365 дней и известно среднее значение числа угроз за этот промежуток, равное 3, тогда получим за один день ожидаемое количество угроз: $\lambda=3/365\approx 0{,}0082$.

а) Сначала найдём вероятность количества 0 (отсутствия угроз) за один день. Эту вероятность вычтем из 1 и получим вероятность хотя бы одной угрозы за этот день. В данном случае $P(0)=\frac{\lambda^0}{0!}\cdot e^{-\lambda}=\frac{1}{1}\cdot e^{-\frac{3}{365}}\approx$ 0,9918 и вероятность за день хотя бы одной такой угрозы равна 0,0082 или 0,82%;

б) Если в качестве рассматриваемого периода выберем 130 дней, то при тех же условиях ожидаемое число проявлений угрозы станет равным $\lambda=3\cdot 130/365\approx 1{,}068$. Тогда вероятность отсутствия угроз за это время $P(0)=\frac{\lambda^0}{0!}\cdot e^{-\lambda}=\frac{1}{1}\cdot e^{-\frac{390}{365}}\approx 0{,}3435$. Это даёт вероятность проявления хотя бы одной такой угрозы за этот период 0,6565 или 65,65%.

Учтём, что распределение Пуассона, кроме случаев со средним количеством λ появлений события на временном промежутке, применимо и при проведении большого числа независимых испытаний n с одинаково малой вероятностью появления некоторого события p (обычно менее 1%) в каждом случае ($\lambda=n\cdot p\le 5$). Тогда по той же формуле Пуассона можно оценить вероятность реального числа таких событий в серии из n испытаний.

С увеличением объёма статистической информации об угрозах безопасности проектных решений для условий (среды), в которых предполагается осуществлять проектирование, а также для самого процесса проектирования точность вычисления вероятности проявления каждой угрозы повышается. Это позволит для каждой угрозы рассчитать вероятность обнаружения и полную её нейтрализацию без последствий. Для этого можно применять либо экспертные оценки, либо обработку статистических данных.

Этап 2. Оценка вероятности нанесения ущерба

Этап 2.1. Оценка вероятности нанесения ущерба при обнаружении проявившейся угрозы

После проведения работы по оценке вероятности проявления угрозы необходимо оценить ущерб от ее воздействия. Под *ущербом* будем понимать реализацию негативного воздействия от проявившейся, но не локализованной угрозы, без приведения его количественной составляющей.

Пусть имеется N типов угроз, каждая из которых может либо *проявиться* с вероятностью $p1$, либо не проявиться с вероятностью $q1=1-p1$ за выбранное время. Тогда количество возможных комбинаций их проявлений и непроявлений равно 2^N. Для удобства расчета применим вспомогательную матрицу из такого же количества 2^N столбцов. В них по возрастанию записаны N-разрядные двоичные числа. Например, при $N=5$ получим 32 столбца, где 0 – угроза с номером строки не проявилась, 1 – угроза проявилась.

Столбец $\begin{pmatrix}0\\1\\1\\0\\1\end{pmatrix}$ с номером 13 говорит об одновременном проявлении угроз с номерами 2, 3 ,5 и непроявлении угроз с номерами 1 и 4 (на местах которых стоят нули). Вероятности всех таких комбинаций найдём как произведение вероятностей независимых событий, считая возникновение угроз независимыми друг от друга.

Вероятность наступления хотя бы одной угрозы можно вычислить двумя способами:

а) Первый способ – через вероятность противоположного события. Для события C – «хотя бы одна из проявившихся угроз не обнаружена» – вводится противоположное событие B – «все проявившиеся угрозы обнаружены и нейтрализованы». Тогда вероятность события C равна $P(C)=1-P(B)=1-\prod_{i=1}^{N}(1-p1_i)$.

Рассмотренный способ вычисления вероятности ущерба несложен, однако конечный результат не даёт ответа, какой ущерб более вероятен, и позднее не позволит оценить математическое ожидание ущерба (риск);

б) Второй способ с записью события «проявилось ровно k угроз» через все возможные комбинации

наступления – ненаступления этих угроз и нахождение вероятностей этих комбинаций.

Для этого введём новые числовые величины:

$$b_{i,j} = \begin{cases} p1_i, & если\ a_{i,j} = 1, \\ 1 - p1_i, & если\ a_{i,j} = 0, \end{cases} \quad (1)$$

$$c_{i,j} = \begin{cases} 1, & если\ a_{i,j} = 0, \\ p2_i, & если\ a_{i,j} = 1, \end{cases} \quad (2)$$

где $a_{i,j} \in \{0, 1\}$ – соответствующий элемент построенной матрицы $A_{N \times 2^N}$.

Тогда при каждом номере j (от 1 до 2^N) столбца матрицы A вероятность появления и обнаружения только угроз с номерами i, для которых $a_{i,j} = 1$, равна произведению N множителей $b_{i,j}$ и N множителей $c_{i,j}$ при фиксированном номере j и изменении i от 1 до N, $\prod_{i=1}^{N}\left(b_{i,j} \cdot c_{i,j}\right)$. Итоговая вероятность события D-«обнаружение и полная нейтрализация всех проявившихся угроз» является суммой всех таких вероятностей по числу столбцов для A,

$$P(B) = \sum_{j=1}^{2^N}\left(\prod_{i=1}^{N}\left(b_{i,j} \cdot c_{i,j}\right)\right), \quad (3)$$

что даёт полную вероятность $P(E) = 1 - P(D)$ ущерба хотя бы от одной угрозы.

Рассмотрим упрощённый случай, когда имеется N угроз с одинаковой вероятностью $p1$ их наступления и одинаковой вероятностью $p2$ их обнаружения с полной нейтрализацией. Тогда при вычислении вероятности отсутствия ущерба среди 2^N слагаемых окажутся отличающиеся только порядком следования множителей, формула упростится и будет аналогична формуле Бернулли. При наступлении k угроз вероятность будет равна

$$\prod_{i=1}^{N}\left(b_{i,j} \cdot c_{i,j}\right) = p1^k \cdot (1 - p1)^{N-k} \quad (4)$$

и их количество равно $C_N^k = \frac{N!}{k!(N-k)!}$. (5)

Для подсчёта вероятности отсутствия ущерба домножим результат на произведение вероятностей обнаружения в количестве k и полученные значения просуммируем при всех значениях k от 0 до N:

$$P = \sum_{k=0}^{N}\left(C_N^k \cdot p1^k \cdot (1 - p1)^{N-k} \cdot p2^k\right). \quad (6)$$

Вычислим в пакете MathCAD такие вероятности (надёжность за один промежуток времени) при $N = 5$ и различных вероятностях $p1$ проявления угроз безопасности информации (по строкам от 0,04 до 0,4) и вероятностях $p2$ обнаружения проявленных угроз безопасности информации (по столбцам от 0,98 до 0,6 по убыванию) и запишем их в таблице 1.

Таблица 1

Надёжность процесса при пяти равновероятных угрозах в зависимости от вероятностей $p1$ их проявления и одинаковых вероятностях $p2$ обнаружения проявленных угроз

$p1$ \ $p2$	1	0,95	0,90	0,85	0,80	0,75	0,70	0,65	0,60	0,55	0,50	0,45	0,40	0,35	0,30	0,25	0,20	0,15	0,10	0,05
0,001	1	1	1	0,999	0,999	0,999	0,999	0,998	0,998	0,998	0,998	0,997	0,997	0,997	0,997	0,996	0,996	0,996	0,996	0,995
0,051	1	0,987	0,975	0,962	0,950	0,938	0,926	0,914	0,902	0,890	0,879	0,867	0,856	0,845	0,834	0,823	0,812	0,801	0,791	,780
0,101	1	0,975	0,951	0,927	0,903	0,880	0,857	0,835	0,814	0,792	0,772	0,751	0,732	0,712	0,693	0,674	0,656	0,638	0,621	0,604
0,151	1	0,963	0,927	0,892	0,858	0,825	0,793	0,762	0,732	0,703	0,675	0,648	0,622	0,597	0,572	0,548	0,525	0,503	0,482	0,461
0,201	1	0,951	0,903	0,858	0,815	0,773	0,733	0,694	0,658	0,622	0,589	0,557	0,526	0,497	0,469	0,442	0,416	0,392	0,369	0,347
0,251	1	0,939	0,881	0,825	0,773	0,723	0,676	0,631	0,589	0,549	0,511	0,476	0,442	0,410	0,381	0,352	0,326	0,301	0,278	0,256
0,301	1	0,927	0,858	0,794	0,733	0,676	0,623	0,573	0,527	0,483	0,442	0,405	0,369	0,337	0,306	0,278	0,252	0,228	0,206	0,186
0,351	1	0,915	0,836	0,763	0,695	0,632	0,573	0,519	0,469	0,423	0,381	0,342	0,307	0,274	0,244	0,217	0,192	0,170	0,150	0,132
0,401	1	0,904	0,815	0,733	0,658	0,590	0,527	0,469	0,417	0,370	0,327	0,288	0,253	0,221	0,193	0,167	0,145	0,124	0,107	0,091
0,451	1	0,892	0,794	0,705	0,623	0,550	0,483	0,424	0,370	0,322	0,279	0,240	0,206	0,176	0,150	0,127	0,107	0,089	0,074	0,061
0,501	1	0,881	0,773	0,677	0,590	0,512	0,443	0,381	0,327	0,279	0,237	0,200	0,167	0,139	0,115	0,095	0,077	0,062	0,050	0,040
0,551	1	0,870	0,753	0,650	0,558	0,477	0,405	0,343	0,288	0,241	0,200	0,164	0,134	0,109	0,087	0,070	0,055	0,042	0,033	0,025
0,601	1	0,859	0,734	0,624	0,527	0,443	0,370	0,307	0,253	0,207	0,167	0,134	0,107	0,084	0,065	0,050	0,038	0,028	0,020	0,015
0,651	1	0,848	0,714	0,598	0,498	0,411	0,337	0,274	0,221	0,177	0,140	0,109	0,084	0,064	0,048	0,035	0,025	0,018	0,012	0,008
0,701	1	0,837	0,695	0,574	0,470	0,382	0,307	0,245	0,193	0,150	0,116	0,088	0,065	0,048	0,034	0,024	0,016	0,011	0,007	0,004
0,751	1	0,826	0,677	0,550	0,443	0,354	0,279	0,218	0,168	0,127	0,095	0,070	0,050	0,035	0,024	0,016	0,010	0,006	0,004	0,002
0,801	1	0,815	0,659	0,527	0,418	0,327	0,253	0,193	0,145	0,107	0,077	0,055	0,038	0,025	0,016	0,010	0,006	0,003	0,002	0,001
0,851	1	0,805	0,641	0,505	0,393	0,302	0,229	0,171	0,125	0,089	0,063	0,043	0,028	0,018	0,011	0,006	0,003	0,002	0,001	0
0,901	1	0,794	0,624	0,484	0,370	0,279	0,207	0,150	0,107	0,074	0,050	0,033	0,020	0,012	0,007	0,004	0,002	0,001	0	0

Например, если в ходе процесса может проявиться пять различных типов угроз с одинаковой вероятностью (вторая строка таблицы). Для каждой проявившейся угрозы система безопасности её обнаруживает и нейтрализует с вероятностью 90% (третий столбец таблицы). Тогда надёжность такого процесса (вероятность отсутствия последствий от всех этих угроз) равна 0,975, т. е. риск составляет 2,5%.

Вероятности из таблицы 1 графически представлены на рисунке 1 двумя типами линий:

а) Первый вид линий на рисунке 1а составлен *по строкам* таблицы с постоянным значением $p1$ – возрастающие линии, для каждой из которых увеличение $p2$ приводит к возрастанию общей надёжности. Каждая пятая из линий выделена толщиной и типом линии. С увеличением значения $p1$ линия оказывается ниже с увеличением выпуклости вниз. По оси абсцисс для них изменяются вероятности $p2$ обнаружения проявившейся угрозы, по оси ординат – соответствующая общая надёжность. По совокупности этих линий видно, что при фиксированной вероятности $p1$ проявления угроз общая надёжность системы с увеличением вероятности обнаружения угроз повышается;

б) Второй вид линий на рисунке 1б составлен *по столбцам* таблицы с постоянными значениями $p2$ – убывающие линии, которые с увеличением вероятности $p1$ приводят к снижению общей надёжности. Каждая пятая из них выделена толщиной и типом линии. С увеличением значения $p1$ линия оказывается ниже с увеличением выпуклости вниз. По оси абсцисс для них – вероятности по возрастанию, и по оси ординат им соответствует общая надёжность.

По обеим частям рисунка 1 видно, что влияния $p1$ и $p2$ на общую надёжность симметричные, но взаимообратные: при фиксированной вероятности $p1$ с ростом вероятности $p2$ надёжность возрастает; при фиксированной вероятности $p2$ с ростом вероятности $p1$ надёжность снижается. Одновременные их изменения можно проследить по таблице 1.

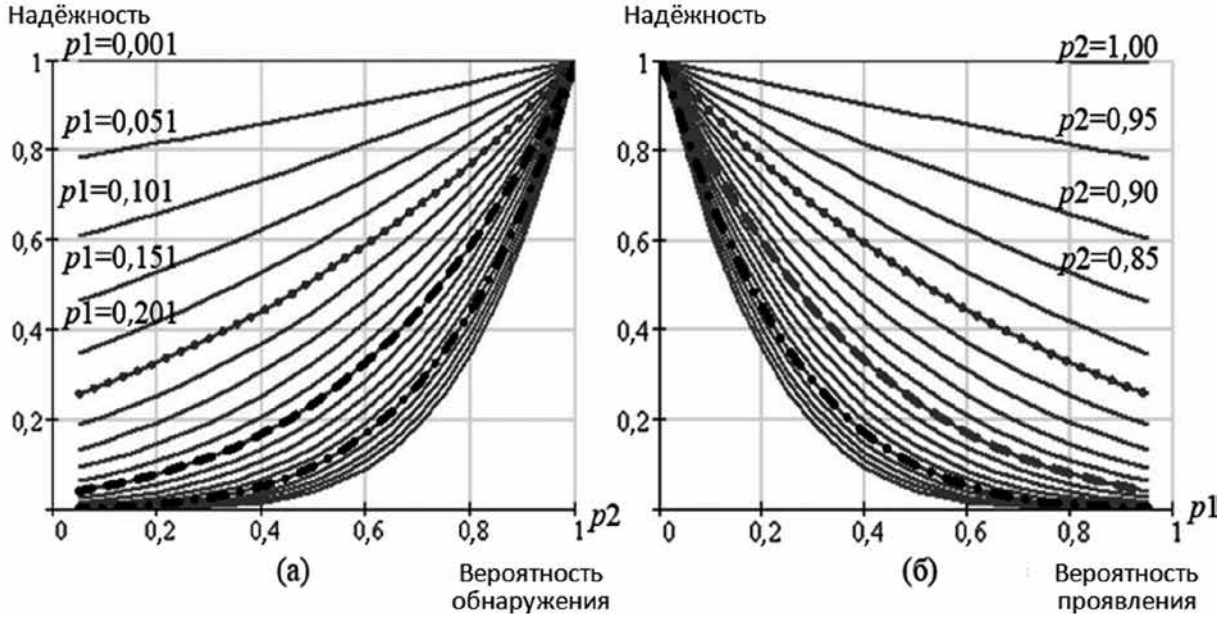
После анализа общего вида зависимости надёжности от двух переменных $p1$ и $p2$ для прикладных задач найдём надёжность при наиболее применимых значениях этих переменных, составив из них таблицу 2. В ней возьмём малые значения вероятностей $p1$ с шагом 0,001 по возрастанию, а для вероятности обнаружения $p2$ – убывающие от 1,000 с шагом 0,002.

Например, пусть в ходе процесса проектирования может наступить только 5 видов угроз и их наступление имеет одинаковую вероятность 0,4%. Если система безопасности отслеживает и обезвреживает эти угрозы с одинаковой вероятностью 99,2%, то вероятность ущерба составляет 1 – 0,99984 или 0,016%.

Для другого числа угроз с одинаковыми вероятностями проявления и одинаковыми вероятностями обнаружения общая надёжность вычисляется аналогично по формуле (6). Вычисления усложняются при различных вероятностях $p1$ и (или) $p2$, когда следует применять общую формулу (3).

Этап 2.2. Оценка вероятности нанесения ущерба при необнаружении проявившейся угрозы

В предыдущем пункте рассмотрена оценка вероятности ущерба, как обратного события. То есть сначала предполагали, что за рассмотренный промежуток вре-



1. Рис. 1. Надежность системы защиты от пяти угроз:

а) при постоянных вероятностях $p1$ проявления угроз;

б) при постоянных вероятностях $p2$ обнаружения угроз

Таблица 2

Надёжность при пяти угрозах с малыми вероятностями $p1$ их проявления и большими вероятностями $p2$ их обнаружения и нейтрализации

$p1$ \ $p2$	0,998	0,996	0,994	0,992	0,990	0,988	0,986	0,984	0,982	0,980	0,978	0,976	0,974	0,972	0,970
0,001	0,99999	0,99998	0,99997	0,99996	0,99995	0,99994	0,99993	0,99992	0,99991	0,99990	0,99989	0,99988	0,99987	0,99986	0,99985
0,002	0,99998	0,99996	0,99994	0,99992	0,99990	0,99988	0,99986	0,99984	0,99982	0,99980	0,99978	0,99976	0,99974	0,99972	0,99970
0,003	0,99997	0,99994	0,99991	0,99988	0,99985	0,99982	0,99979	0,99976	0,99973	0,99970	0,99967	0,99964	0,99961	0,99958	0,99955
0,004	0,99996	0,99992	0,99988	0,99984	0,99980	0,99976	0,99972	0,99968	0,99964	0,99960	0,99956	0,99952	0,99948	0,99944	0,99940
0,005	0,99995	0,99990	0,99985	0,99980	0,99975	0,99970	0,99965	0,99960	0,99955	0,99950	0,99945	0,99940	0,99935	0,99930	0,99925
0,006	0,99994	0,99988	0,99982	0,99976	0,99970	0,99964	0,99958	0,99952	0,99946	0,99940	0,99934	0,99928	0,99922	0,99916	0,99910
0,007	0,99993	0,99986	0,99979	0,99972	0,99965	0,99958	0,99951	0,99944	0,99937	0,99930	0,99923	0,99916	0,99909	0,99902	0,99895
0,008	0,99992	0,99984	0,99976	0,99968	0,99960	0,99952	0,99944	0,99936	0,99928	0,99920	0,99912	0,99904	0,99896	0,99888	0,99880
0,009	0,99991	0,99982	0,99973	0,99964	0,99955	0,99946	0,99937	0,99928	0,99919	0,99910	0,99901	0,99892	0,99883	0,99874	0,99865
0,010	0,99990	0,99980	0,99970	0,99960	0,99950	0,99940	0,99930	0,99920	0,99910	0,99900	0,99890	0,99880	0,99870	0,99860	0,99850
0,011	0,99989	0,99978	0,99967	0,99956	0,99945	0,99934	0,99923	0,99912	0,99901	0,99890	0,99879	0,99868	0,99857	0,99846	0,99835
0,012	0,99988	0,99976	0,99964	0,99952	0,99940	0,99928	0,99916	0,99904	0,99892	0,99880	0,99868	0,99856	0,99844	0,99832	0,99820
0,013	0,99987	0,99974	0,99961	0,99948	0,99935	0,99922	0,99909	0,99896	0,99883	0,99870	0,99857	0,99844	0,99831	0,99818	0,99805
0,014	0,99986	0,99972	0,99958	0,99944	0,99930	0,99916	0,99902	0,99888	0,99874	0,99860	0,99846	0,99832	0,99818	0,99804	0,99790
0,015	0,99985	0,99970	0,99955	0,99940	0,99925	0,99910	0,99895	0,99880	0,99865	0,99850	0,99835	0,99820	0,99805	0,99790	0,99775
0,016	0,99984	0,99968	0,99952	0,99936	0,99920	0,99904	0,99888	0,99872	0,99856	0,99840	0,99824	0,99808	0,99792	0,99776	0,99760
0,017	0,99983	0,99966	0,99949	0,99932	0,99915	0,99898	0,99881	0,99864	0,99847	0,99830	0,99813	0,99796	0,99779	0,99762	0,99745
0,018	0,99982	0,99964	0,99946	0,99928	0,99910	0,99892	0,99874	0,99856	0,99838	0,99820	0,99802	0,99784	0,99766	0,99748	0,99730
0,019	0,99981	0,99962	0,99943	0,99924	0,99905	0,99886	0,99867	0,99848	0,99829	0,99810	0,99791	0,99772	0,99753	0,99734	0,99715

мени либо угроз не наступило, либо при их проявлении каждая угроза обнаружена и полностью нейтрализована.

Найдём такую вероятность с учётом проявления угроз и их необнаружения (второй метод вычисления надёжности). Это позволит оценить не только вероятность, но и ожидаемый размер ущерба.

Как и в рассмотренном ранее методе, составим таблицу из 2^N столбцов, состоящих из 0 и 1. В каждом из этих вариантов вероятность наступлений – ненаступлений угроз даёт число $d_j = \prod_{i=1}^{N} b_{i,j}$. В этом произведении количество единиц в столбце с номером j для матрицы A даёт число множителей вида $p1_i$, остальные имеют вид $1-p1_i$. Если при этом наступила одна угроза, то умножение на вероятность её необнаружения даёт вероятность одного этого варианта ущерба. Если угроз 2, то есть 2 × 2 комбинаций их обнаружений – необнаружений. Для наступивших трёх угроз таких вариантов 2 × 2 × 2 и т. д. Одна из таких комбинаций с обнаружением всех проявившихся угроз может не рассматриваться, т. к. при этом ущерб нулевой. В остальных случаях при количестве k проявившихся угроз получим 2^k-1 слагаемых. В каждом слагаемом по k множителей с разными комбинациями вероятностей обнаружения $p2_{i*}$ либо необнаружения $1-p2_{i*}$ угрозы с номером $i*$ среди выбранных (проявившимся угрозам, которым в выбранном столбце матрицы A соответствуют единицы). Когда все выбранные угрозы обнаружены, результат домножаем на 0. Полученная сумма g_j таких 2^k слагаемых умножается на ранее полученное число d_j. В итоге получим вероятность $p4_j$ *ущерба*. Сумма таких вероятностей даёт вероятность ущерба за отведённый промежуток времени (на рассматриваемом временном промежутке).

В общем случае при N возможных угрозах для вычисления общей вероятности ущерба можно выполнить вычисления на компьютере. Тогда каждый из 2^N столбцов матрицы A, имеющий k_j единиц, превращается в 2^{k_j} дополнительных столбцов. При этом в добавленных столбцах перебираются все комбинации нулей и единиц на местах, где в исходном столбце j стояли единицы. При этом для всех столбцов, порожденных одним столбцом с номером j матрицы A, будет одинаковая вероятность проявлений – непроявлений учтённых угроз, как произведение вероятностей вида (1), т. е. $\prod_{i=1}^{N}\left(b_{i,j}\right)$. Каждая из таких вероятностей умножается на вероятности $q2_i$ угроз с номерами i, на месте которых в рассмотренном (дополнительном) столбце стоят единицы, т. е. на числа $c_{i,j}$ вида (2). Тогда вероятность ущерба в комбинации с номером j угроз равна сумме таких вероятностей. Итоговая вероятность ущерба будет равна сумме таких вероятностей при изменении

номеров j от 1 до 2^N. Вычитание такой вероятности из 1 даёт найденную ранее надёжность.

Пример 2. Пусть при некотором процессе возможно только три вида угроз. По статистическим данным были получены результаты, представленные в таблице 3. Необходимо вычислить надёжность этого процесса.

Таблица 3

Заданные вероятности проявления и обнаружения трёх угроз

Номер угрозы	i	1	2	3
Вероятность появления	$p1_i$	0,003	0,002	0,001
Вероятность нейтрализации	$p2_i$	0,99	0,98	0,97

Решение: Каждая угроза может давать два исхода – её проявление либо непроявление. Тогда в каждый момент времени общее число возможных комбинаций для этих трёх угроз равно 2 × 2 × 2 = 8. В каждом таком случае его вероятность является результатом перемножения трёх множителей либо $p1_i$, либо $1-p1_i$. Если угроза с номером i проявилась, полученную вероятность домножим на вероятность $p2_i$ её нейтрализации либо на $q2_i=1-p2_i$ необнаружения. Сумма этих результатов даёт общую вероятность ущерба:

$$p4=(q1_1\cdot q1_2\cdot q1_3)\cdot 0++(p1_1\cdot q1_2\cdot q1_3)\cdot q2_1+$$
$$+(q1_1+\cdot p1_2\cdot q1_3)\cdot q2_2+(q1_1\cdot q1_2\cdot p1_3)\cdot q2_3+$$
$$+(p1_1\cdot p1_2\cdot q1_3)\cdot(q2_1\cdot q2_2+p2_1\cdot q2_2+q2_1\cdot p2_2+0)+$$
$$+(p1_1\cdot q1_2\cdot p1_3)\cdot(q2_1\cdot q2_3+p2_1\cdot q2_3+q2_1\cdot p2_3+0)+$$
$$+(q1_1\cdot p1_2\cdot p1_3)\cdot(q2_2\cdot q2_3+p2_2\cdot q2_3+q2_2\cdot p2_3+0)+$$
$$+(p1_1\cdot p1_2\cdot p1_3)\cdot q2_1\cdot q2_2\cdot q2_3=$$
$$= 2{,}991006\cdot 10^{-5}+3{,}984012\cdot 10^{-5}+2{,}985018\cdot 10^{-5}+$$
$$+1{,}786212\cdot 10^{-7}+1{,}188618\cdot 10^{-7}+9{,}85036\cdot 10^{-8}+$$
$$+3{,}6\cdot 10^{-14}=9{,}999634660\cdot 10^{-5},$$

$p4\approx 0{,}0001$, т. е. вероятность *ущерба* составляет 0,01%.

Если число угроз увеличить, то количество вычислений существенно возрастет. Вместо этого можно оценить вероятность ущерба по первому способу: в данной задаче из трёх значений $p1_i$ их среднее арифметическое равно 0,002; для трёх значений $p2_i$ их среднее арифметическое – 0,98. В таблице 2 по этой паре получим надёжность 0,99980, т. е. 99,98%. Тогда вероятность ущерба равна 0,02%, что имеет порядок малости, как и найденная вторым методом вероятность.

В итоге для этого процесса на рассмотренном промежутке времени получили надёжность, равную 99,99%, и вероятность ущерба, равную 0,01%.

Рассмотренный второй способ нахождения вероятности ущерба более универсален. Если в каждом из слагаемых полученную вероятность комбинации проявления угроз и отсутствия их обнаружения добавить умножение на ожидаемый размер ущерба при этом, то можно найти не только вероятность, но и ожидаемый размер ущерба при учёте всех возможных угроз.

Этап 2.3. Оценка вероятности ущерба при нескольких одновременно выполняемых работах

Пусть разработка изделия состоит из n этапов. В общем случае для каждого этапа проектирования необходимо по рассмотренному выше алгоритму найти вероятности двух видов для каждого типа работ и по ним вычислить общую вероятность ущерба для данного этапа.

Поскольку проектное предприятие представляет собой совокупность независимых процессов, осуществляемых в одно время, надёжность выполнения этой серии процессов состоит в их одновременной работе без ущерба от всех угроз. Вероятность такого события можно описать как вероятность одновременного отсутствия ущерба для каждой из них. В силу независимости этих процессов получаем вероятность в виде произведения их надёжностей, $P_n=\prod_{i=1}^{n} p3_i$. ([6, 7]). Каждая из надёжностей является числом менее единицы (не бывает абсолютно защищенного процесса разработки, вероятность ущерба даже в самых защищенных случаях не может быть равна 0). Тогда с увеличением числа одновременно выполняемых работ общая надёжность системы защиты снижается, и она всегда меньше самой низкой из надёжностей.

Исходя из этого, можно определить предельно допустимое количество одновременно выполняемых работ по изготовлению изделий, при котором общая надёжность не ниже допустимой, $Pn\geq\varepsilon$. При известной общей надёжности таким образом можно проверить, не снизит ли добавление дополнительной работы с известной надёжностью $p3_{n+1}$ общую надёжность ниже порогового значения $\varepsilon_{\text{крит}}$.

Для удобства и наглядности будем считать, что выполняемые предприятием работы *однотипные* и все они подвергаются одинаковым угрозам (типы которых рассматривались выше, и вероятности таких угроз, как и вероятности их нейтрализации), их надёжности, соответственно, одинаковые и $p3_i=p$. Тогда общая надёжность всей системы защиты одновременно выполняемых работ равна p^n и условие примет вид $p^n\geq\varepsilon$. Это позволит по значениям p и ε найти $n_{max}=\left[log_p(\varepsilon)\right]=\left[\frac{lg(\varepsilon)}{\lg(p)}\right]$.

Пример 3. Во время одной работы возможно наступление пяти видов угроз. При известных вероятностях их проявлений и вероятностях их обнаружения рассмотренными выше методами вычислена надёжность 0,9997131 и вероятность ущерба 0,0002869 в ходе этой работы.

Пусть процесс состоит в выполнении нескольких таких работ. Тогда в силу независимости проявления угроз на разных работах можно считать инадёжности тоже независимыми. Для процесса из двух таких работ надёжность будет равна произведению их надёжностей, 0,9997131 × 0,9997131 ≈ 0,999426. Для трёх таких

работ надёжность будет равна $0{,}9997131^3 \approx 0{,}9991395$. График изменения надёжности процесса из N таких работ по закону p^N показан на рисунке 2.

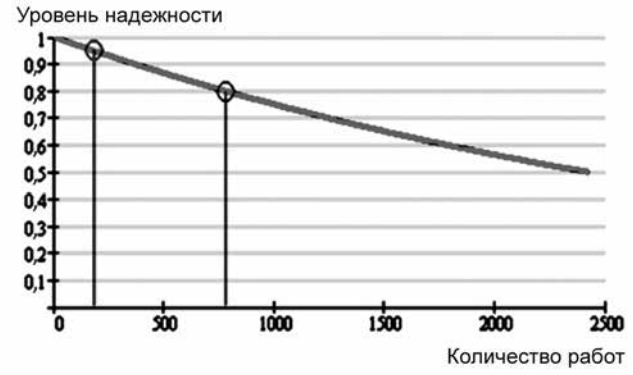


Рис. 2. Изменение надёжности процесса из N работ с одинаковой надёжностью и изменением количества N

Для предельной надёжности 95% (левый столбик на рисунке 2) допустимо использовать однотипных работ в количестве не более

$$n_{max} = \left[log_p(0{,}95)\right] = \left[\frac{lg(0{,}95)}{\lg(0{,}9997131)}\right] = 179.$$

Тогда для процесса с количеством работ $N \geq 180$ его надёжность будет менее 95%.

Взяв предельную надёжность 80%, получим

$$n_{max} = \left[\frac{lg(0{,}80)}{\lg(0{,}9997131)}\right] = 778.$$

Приведенный эксперимент показал, что при уровне надёжности 80% предприятие может выполнять до 778 работ. Это количество работ кажется весьма значительным, но в данном случае учитывается надёжность системы одновременно выполняемых работ только на одном временном такте (час, сутки, месяц… в зависимости от промежутка, на котором находилось среднее количество проявлений угрозы при вычислении её вероятности).

Если возьмем $n = 10$ однотипным работам, то на одном начальном такте надёжность их системы будет уже меньше, $p^n = 0{,}997135$. Выполняемые последовательно такты в количестве M при оценке общей надёжности тоже дадут формулу $(p^n)^M = 0{,}997135^M$, которая даёт значение менее 0,8 уже при $M = 78$.

Взяв $n = 20$, к этой пороговой надёжности 80% перейдём уже при $M = 39$ и т. д. Снижение надёжности на одном такте существенно уменьшает и эти цифры, после которых общая надёжность окажется ниже 80% (вероятность ущерба достигнет 20%, что на практике является очень большим значением).

Однако стоит учитывать, что реальный процесс проектирования значительно отличается от моделируемого в нашем случае. Понятие «однотипности работ» применимо скорее к предприятиям авиационной отрасли ввиду того, что при разработке изделий они опираются на общепринятые национальные и международные стандарты, регламентирующие их работу. Кроме того, однотипными можно назвать процессы, при которых производится доработка некоторой модификации уже выпускаемого изделия и т. д.

Этап 3. Оценка надёжности системы при наличии резервных вариантов выполнения работ

Пусть для выполняемого процесса кроме применяемого способа имеется резервный, которым при обнаружении или воздействии угрозы можно воспользоваться. Тогда при неблагополучном завершении этой работы должны реализоваться риски по обоим вариантам. Вероятность этого будет равна $P = 1 - (1 - p_1) \times (1 - p_2)$. При увеличении количества k резервных вариантов в общем случае получим надёжность $P = 1 - \prod_{i=1}^{k}(1 - p_i)$, которая возрастает и стремится к 1. Общая надёжность такой работы возрастает и становится выше любой из надёжностей этих взаимозаменяемых способов.

Заключение

Использование предложенного метода позволит оценить поведение СЗИ при изменении объемов работ предприятий и условий проектирования.

Полученные результаты позволят рассчитать предельно допустимое количество выполняемых работ с требуемым уровнем надежности, которое на практике должно стремиться к 1. При изменении объемов работ (поступлении новых заказов) и полученных результатах, свидетельствующих о снижении уровня надежности системы защиты, рекомендуется использовать резервные варианты. Необходимо рассмотреть участок работ (выделенный процесс), влияющий на снижение общего уровня защиты, с позиции фрагментации. Модуль системы защиты для данного участка работы фрагментировать на более мелкие модули, способные предотвращать актуальную номенклатуру угроз безопасности и таким образом повышать общий уровень надежности системы защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб. : БХВ-Петербург, 2003. – 752 с.

2. Астахов А.М. Искусство управления информационными рисками. – М. : ДМК Пресс, 2010. – 312 с.

3. Халяпин Д.Б., Ярочкин В.И. Основы защиты информации: учебное пособие. – М. : ИПКИР, 1994. – 128 с.

4. Анин Б.Ю. Защита компьютерной информации. – СПб. : БХВ-Петербург, 2000. – 384 с.

5. Уродовских В.Н. Управление рисками предприятия : учеб. пособие. – М. : ВЗФЭИ, 2009. – 130 с.

6. Гмурман В.Е. Руководство к решению задач по теории вероятностей и математической статистике. – М. : Высшая школа, 2004. – 407 с.

7. Письменный Д.Т. Конспект лекций по теории вероятностей и математической статистике. – М. : Айрис-пресс, 2004. – 256 с.

8. Правиков Ю.М., Муслина Г.Р. Основы теории надежности технологических процессов в машиностроении : учеб. пособие. – Ульяновск : УлГТУ, 2015. – 122 с.

REFERENCES

1. Koneev I.R., Beliaev A.V. *Informatsionnaia bezopasnost predpriiatiia* [Information Security of an Enterprise]. St.Petersburg, BHV-Peterburg Publ., 2003. 752 p.

2. Astakhov A.M. *Iskusstvo upravleniia informatsionnymi riskami* [Information Security Risk Managing as a Workmanship]. Moscow, DMK Press Publ., 2010. 312 p.

3. Khaliapin D.B., Yarochkin V.I. *Osnovy zashchity informatsii. Uchebnoe posobie* [Fundamentals of Information Security. Textbook]. Moscow, IPKIR Publ., 1994. 128 p.

4. Anin B.Iu. *Zashchita kompiuternoi informatsii* [Computer Information Protection]. St.Petersburg, BHV-Peterburg Publ., 2000. 384 p.

5. Urodovskikh V.N. *Upravlenie riskami predpriiatiia. Ucheb. posobie* [Risk of Management in an Enterprise. Textbook]. Moscow, VZFEI Publ., 2009. 130 p.

6. Gmurman V.E. *Rukovodstvo k resheniiu zadach po teorii veroiatnostei i matematicheskoi statistike* [Guide for Solving the Problems on the Theory of Probability and Mathematical Statistics]. Moscow, Vysshaia Shkola Publ., 2004. 407 p.

7. Pismennyi D.T. *Konspekt lektsii po teorii veroiatnostei i matematicheskoi statistike* [Lecture on the Theory of Probability and Mathematical Statistics]. Moscow, Airis-press Publ., 2004. 256 p.

8. Pravikov Iu.M., Muslina G.R. *Osnovy teorii nadezhnosti tekhnologicheskikh protsessov v mashinostroenii. Ucheb. posobie* [Fundamentals of the Theory of Engineering Processes Reliability in Engineering Industry]. Ulyanovsk, UlSTU Publ., 2015. 122 p.