МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЕРОЯТНОСТНОЙ НАДЕЖНОСТИ КОМПЛЕКСА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Журиленко

Национальный авиационный университет

ЖУРИЛЕНКО Борис Евгеньевич, к.ф.-м.н., доцент, с.н.с.

Год и место рождения: 1946 год, г. Чугуев Харьковской области, Украина.
Образование: Киевский государственный университет им. Т.Г.Шевченко, 1974 год.
Должность: доцент кафедры методов защиты информации с 2003 года.
Научный интерес: методы съема и методы технической защиты информации.
Публикации: около 80 научных статей и патентов на изобретения.
E-mail: zhurilenko@mail. ru

Аннотация. *В данной работе предложена математическая модель вероятностной надежности комплекса технической защиты информации (КТЗИ). Построение модели базируется на основных исходных данных присущих защите. Модель надежности КТЗИ ориентирована на вероятности взломов каждой защиты во времени или всего комплекса и в дальнейшем позволит сравнить расчетные результаты с реальными данными взломов и защищенности.*

Ключевые слова: *защита информации, надежность, вероятность взлома, комплекс технической защиты информации.*

Введение

Современный этап создания комплекса технической защиты информации (КТЗИ) основывается, в основном, на статистических данных не связанных с динамикой непосредственного их развития во времени. В реальных условиях больший интерес представляет защита информации не столько в статике, сколько в динамике, то есть во времени. В этом случае будет возможность предсказать, когда уровень защиты уже не достаточен и КТЗИ требует модернизации или замены. Такой подход позволит сэкономить финансовые ресурсы, провести исследования КТЗИ, выработать рекомендации для его модернизации или новые требования для его разработки. В связи с этим методология создания и исследования защиты требует математической вероятностной модели КТЗИ во времени.

Анализ существующих исследований

В настоящий момент существует хорошо разработанная методика расчета надежности радиоэлектронных устройств и оборудования [1-4], которая реально обеспечивает необходимый уровень надежности на отказ. Необходимый уровень надежности на отказ радиоэлектронных устройств и оборудования обеспечивается проведением серии экспериментальных исследований и определением вероятности на отказ. Аналогично для определения надежности КТЗИ проводятся сертификационные исследования, но они не всегда определяют вероятностные параметры защиты.

В настоящей работе предлагается ввести такое свойство для защиты информации, как надежность технической защиты информации (НТЗИ). Интуитивно эта характеристика качества ничем не будет отличаться от определения надежности технических объектов в [5]. В [5], надежность определяется как комплексное свойство технического объекта (прибора, устройства, машины), заключающееся в его способности выполнять заданные функции, сохраняя свои основные характеристики (при определенных условиях эксплуатации) в установленных пределах. Надежность охватывает безотказность, долговечность, ремонтоспособность и сохраняемость объекта. Теория надежности изучает работоспособность и отказ объекта. Показателями надежности являются вероятность безотказной работы, наработка на отказ, технический ресурс, срок службы и тому подобное.

Таким образом, приведенное определение полностью подходит для определения надежности комплекса технической защиты информации, но не как объекта, а как технической системы, обеспечивающей техническую защиту объекта. В такой интерпретации надежность КТЗИ может определять некоторые важные свойства технической защиты информации (ТЗИ), такие как: количественный уровень надежности ТЗИ; временной срок, обеспечивающий этот уровень надежности; необходимые затраты, обеспечивающие

этот срок и уровень защиты, и другие. Кроме того, надежность КТЗИ может включать в себя не только технические системы, но и программный продукт.

Естественно, если создать такую методологию, которая позволяла бы использовать теоретический материал и практический опыт при расчете вероятностей взлома или устойчивости защиты в результате воздействия различных атак на отдельные защиты или на всю защиту, то можно было бы проектировать КТЗИ, ориентируясь только на исходные данные. Кроме того, если бы такая методология имела возможность количественного измерения надежности, то она позволила бы проектировать ТЗИ с необходимыми требованиями к защищенности информации, позволяла бы создавать оптимальную защиту и при эксплуатации позволяла бы вовремя проводить модернизацию КТЗИ для обеспечения необходимого уровня защищенности без вложения излишних дополнительных финансовых расходов.

В настоящее время существуют публикации [6-8], в которых сделана начальная попытка связать исходные и расчетные параметры КТЗИ с реальными экспериментальными вероятностными данными, полученными в результате взлома КТЗИ.

Для продолжения исследований в данном направлении необходимо создание математической модели вероятностной надежности комплекса технической защиты информации.

Целью данной работы является создание математической модели вероятностной надежности комплекса технической защиты информации, которая давала бы количественную оценку надежности того или иного КТЗИ во времени и обеспечивала бы возможность сравнения теоретических результатов с реальными практическими данными.

Основная часть исследований

Из [1], известно, что в основу расчетов вероятности безотказного состояния устройства P, состоящего из N элементов, обладающих вероятностью безотказности p_i, принимаются два следующих соотношения:

1. В случае, если устройство работоспособно только при работоспособном состоянии всех его элементов

$$P = \prod_{i}^{N} p_i . \qquad (1)$$

2. В случае, если отказ устройства наступает только тогда, когда отказывают все его элементы

$$P = 1 - \prod_{i}^{N} (1 - p_i) . \qquad (2)$$

Основываясь на соотношениях (1), (2) построим модель вероятностной надежности КТЗИ. Для этого воспользуемся выражениями вероятности взлома от вложенного финансирования на его защиту [7]

$$P_i(X_i) = [\frac{X_i^{X_i}}{(1+X_i)^{1+X_{ii}}}]^{\beta_s}, \qquad (3)$$

где $X_i = x_i / H_i$ – приведенные вложения финансов на защиту; x_i – финансовые затраты на создание данного ТЗИ; H_i – первоначальные финансовые потери при отсутствии защиты; β_i – определяет эффективность защиты от вложенного финансирования на ее построение.

Для многоуровневой защиты получим вероятность взлома

$$P(X_1, X_2, \ldots, X_n) = \prod_{s=1}^{n} P_i(X_i) . \qquad (4)$$

В отличие от работы [7] в данном выражении опущен множитель $\frac{1}{n!}$, который был введен ошибочно. Однако, отсутствие данного множителя абсолютно не влияет на результаты исследований и выводы работы [7]. Он только несколько изменил числовые значения в таблицах и численных расчетах, где n=2.

Из работы [8] возьмем вероятность взлома во времени

$$P_i(t) = [(\frac{t_{0i}}{t_{0i}+t})^{\frac{t_{0i}}{t}} (\frac{t}{t_{0i}+t})]^{\gamma_s}, \qquad (5)$$

где t_{0i} – временной параметр, присущий данной системе защиты, и который может быть определен только из реальных результатов взлома защиты; t – текущая координата времени; γ_i – определяет эффективность защиты во времени.

Параметр a в работе [8] строго математически не определен, поэтому по ходу вывода уравнения он должен быть равен единице. В результате было получено выражение (5).

Как и в (3), можно воспользоваться приведенным временем $T_i = \frac{t}{t_{0i}}$. Тогда (5) можно представить в виде

$$P_i(T_i) = [(\frac{1}{1+T_i})^{\frac{1}{T_i}} (\frac{T_i}{1+T_i})]^{\gamma_i} . \qquad (6)$$

Следует заметить, что в приведенных координатах X и T все графики будут нормированы и появится возможность сравнения различных применяемых защит.

Определим вероятность защищенности системы, состоящей из вероятности взлома от вложенного финансирования на защиту и вероятности взлома во времени. В обоих случаях принимаем эффективность защиты достаточную, то есть $\beta_i = 1$ и $\gamma_i = 1$.

Получим

$$P_{защ}(X_i) = 1 - P_i(X_i) ,$$
$$P_{защ}(T_i) = 1 - P_i(T_i) . \qquad (7)$$

Поскольку X_i и T_i независимы друг от друга и определяют одну и ту же ТЗИ, то согласно (1), когда работоспособность системы зависит от работоспособности всех его элементов, получим выражение вероятности для защищенности ТЗИ

$$P_{защТЗИ}(X_i,T_i)=[1-P_i(X_i)][1-P_i(T_i)]. \quad (8)$$

Очевидно, вероятность взлома ТЗИ будет

$$P_{взлТЗИ}(X_i,T_i)=\{1-[1-P_i(X_i)]\times \times[1-P_i(T_i)]\}^{\alpha_i} \quad (9)$$

В выражении (9) вводим параметр эффективности используемой ТЗИ a_i, так же как это было получено для выражений (3) и (5) в работах [7,8]. Введение этого параметра справедливо, так как $P_{взлТЗИ}$ определяет один и тот же комплекс защиты, и, следовательно, a_i будет определять эффективность защищенности от взлома одной и той же системы, как обобщение параметров β_i и γ_i.

Очевидно, вероятность взлома КТЗИ будет

$$P_{взлКТЗИ}(X_{in},T_{in})=\prod_i^n\{1-[1-P_i(X_i)]\times \times[1-P_i(T_i)]\}^{\alpha_i} \quad (10)$$

И окончательно получим формулу математической модели вероятностной надежности КТЗИ.

$$P_{защКТЗИ}(X_{in},T_{in})=1-\prod_i^n\{1- -[1-P_i(X_i)][1-P_i(T_i)]\}^{\alpha_i} \quad (11)$$

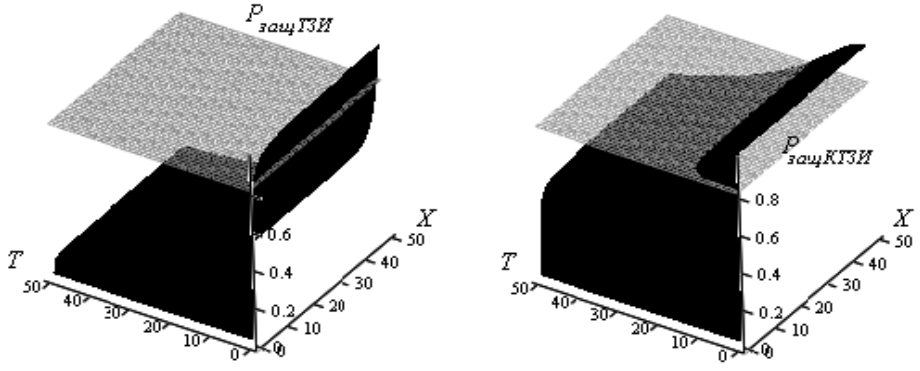
Расчеты и анализ многоуровневой системы защиты выполнялись с помощью выражения (11) в предположении, что системы защиты равноценны.

В этом случае (11) будет иметь вид

$$P_{защКТЗИ}(X_{in},T_{in})=1-\{1- -[1-P_i(X_i)][1-P_i(T_i)]\}^{\alpha_i\cdot n} \quad (12)$$

Исследуем выражение (11), для чего построим вероятность надежности защищенности ТЗИ $P_{защКТЗИ}(X_{in},T_{in})$ в координатах X и T при $a_i=1$, $t_{0i}=1$, $n=1$, то есть фактически рассмотрим поведение одной ТЗИ от вложенного финансирования на защиту во времени.

На рис.1а представлена поверхность вероятности надежности защищенности ТЗИ, а в таблице 1 числовые значения расчета этой же поверхности в начальной области.



а) *б)*

Рис.1. Результаты расчета вероятностей надежности защищенности: ТЗИ - (а) при $a_i=1$, $t_{0i}=1$, $n=1$; и КТЗИ - (б) при $a_i=2$, $t_{0i}=2$, $n=2$; плоскости отсекают требуемый уровень 0,8 вероятности надежности защищенности ТЗИ и КТЗИ

Таблица 1

X \ T	0	1	2	3	4
0	0	0	0	0	0
1	0.75	0.562	0.461	0.396	0.349
2	0.852	0.639	0.524	0.449	0.396
3	0.894	0.671	0.55	0.472	0.416
4	0.918	0.689	0.565	0.484	0.427
5	0.933	0.7	0.574	0.492	0.434
6	0.943	0.707	0.58	0.498	0.439
7	0.951	0.713	0.585	0.502	0.442
8	0.957	0.718	0.588	0.505	0.445
9	0.961	0.721	0.591	0.507	0.447

Таблица 2

X \ T	0	1	2	3	4
0	0	0	0	0	0
1	0.996	0.983	0.963	0.94	0.916
2	1	0.994	0.983	0.967	0.949
3	1	0.997	0.988	0.975	0.959
4	1	0.998	0.991	0.979	0.964
5	1	0.998	0.992	0.981	0.967
6	1	0.999	0.993	0.982	0.969
7	1	0.999	0.993	0.983	0.97
8	1	0.999	0.994	0.984	0.971
9	1	0.999	0.994	0.985	0.972

Анализируя полученную поверхность вероятности защищенности, можно сделать следующие заключение. Если в защиту не было вложено финансирование ($X=0$), то вероятность надежности защищенности во времени полностью отсутствует $P_{защТЗИ}(X_i,T_i)=0$. При вкладывании

финансирования в защиту вероятность надежности защищенности быстро растет, достигает определенного уровня при $X=2\text{-}3$ и затем вложение больших затрат не приводит к заметному росту вероятности надежности защищенности.

В начальный момент времени $t=0$ вероятность взлома обеспечивается только вложенным финансированием в защиту. Эта вероятность защищенности определяется с помощью расчетов работы [7]. Определим некоторый уровень вероятности защищенности величиной 0,8 и на рисунках представим его горизонтальной плоскостью. Эта величина определяет, например, требуемый уровень защищенности.

На рис. 1б, табл. 2 представлены результаты расчета вероятности надежности КТЗИ при $a_i=2$, $t_{0i}=2$, $n=2$. Расчет выполнялся по формуле (12).

При использовании двухуровневой защиты на горизонтальной плоскости хорошо видно, что вероятность защищенности во времени от вложенного финансирования на защиту имеет максимально оптимальный вклад при $X=2\text{-}3$. Неограниченное вложение финансирования не приводит к существенному повышению вероятности надежности КТЗИ и ТЗИ во времени.С другой стороны использование двух эффективных систем защиты с одинаковым финансированием на каждую из них приводит к существенному росту вероятности надежности защищенности при общем одинаковом финансировании (сравнить строку 2 табл. 1 и строку 1 табл. 2).

Эти результаты подтверждают и совпадают с расчетами и выводами работы [7]. В обоих случаях представленных на рис.1а, рис.1б, таблица 1 и таблица 2 вероятность надежности защищенности во времени спадает со временем, и крутизна спада зависит от t_{0i}. Чем больше t_{0i}, тем больше во времени обеспечивается надежность защищенности ТЗИ.

На рис.1б приведена поверхность вероятности надежности защищенности при $t_{0i}=2$. Отсюда видно, что t_{0i}, существенно влияет на временную крутизну спада вероятности надежности защищенности.

В работе [7], было сделано заключение, что одна система защиты не сможет обеспечить должный уровень защищенности ТЗИ. Из поверхности вероятности защищенности рис.1 видно, что вероятность надежности ограничена приблизительно вероятностью 0,75 при $X=1$. Только дополнительные вложения финансирования в одну защиту несколько повышают вероятность защищенности, но ее может оказаться недостаточно. Дальнейшая зависимость вероятности защищенности от времени только падает. Следовательно, чтобы обеспечить необходимый уровень защищенности во времени может потребоваться несколько одиночных защит.

Выводы

В результате проделанной работы можно сделать следующие выводы. Полученное выражение показывает, что если нет финансовых вложений на защиту или модернизацию защиты, то есть нет защиты, то вероятность надежности защищенности равна нулю независимо от времени. В начальный момент $t=0$ ТЗИ соответствует вероятности защищенности только за счет вложенного финансирования на защиту или модернизацию.

Если рассматривать вероятность защищенности от максимально эффективного вложения финансирования, то она определяется приведенной защищенностью в пределах $X\leq 3$, то есть при финансовых вложениях на защиту менее или равно трем, общие финансовые потери будут менее или равны трем финансовым потерям без защиты. Получено общее выражение, позволяющее определять вероятности любых событий во времени. Для этого в общем выражении (11) вероятность финансовых затрат на КТЗИ заменяется вероятностью рассматриваемого события в начальный момент времени $t=0$.

Временная вероятность остается в том же виде, но из экспериментальных исследований или реальных событий взлома или защищенности определяется время t_0. Если в защищенности участвуют различные вероятностные процессы, то в этом случае общая вероятность защищенности будет определяться как для комплекса технической защиты информации с помощью выражения (11).

Литература

[1] Голинкевич Т.А. Оценка надежности радиоэлектронной аппаратуры. М.: Из-во «Советское радио». 1969. -176с.

[2] Базовский И. Надежность. Теория и практика. Перевод с английского под ред Б.Р.Левина.-изд-во «Мир», 1965.

[3] Смирнов Н.В., Дунин-Барковский И.В. Курс теории вероятностей и математической статистики для технических приложений, изд-во «Наука», 1965.

[4] Lloyd D., Lipow M., Reliabiliti: Management, Methods, and Mathematics, Prentice-Hall, Inc. Englewood Gliffs, N.J.,1962; Русский перевод: Ллойд Д., Липов М. Надежность: организация, исследования, методы, математический аппарат, изд-во «Советское радио», 1964..

[5] Советский энциклопедический словарь / Научно-редакционный совет: А.М. Прохоров (пред.). – М.: «Советская энциклопедия», 1981. – 1600 с.

[6] Журиленко Б.Є. Оцінювання деградації стійкості комплексної системи захисту інформації в часі / Б.Є.Журиленко // Вісник НАУ: науковий журнал. – Київ, НАУ, 2007. - №1(31). - С.67-69.

[7] Журиленко Б.Є. Оптимальные финансовые затраты и основные критерии построения или модернизации комплекса технической защиты информации / Журиленко Б.Є. Николаева Н.К., Пелих Н.С. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Науково-технічний збірник. – Київ, КПІ НДЦ «Тезіс», 2011. - Випуск 1 (22). - С.33-43.

[8] Журиленко Б.Є. Оценка стойкости технической защиты информации во времени / Журиленко Б.Є., Николаева Н.К., Пелих Н.С. // Захист інформації: науково-технічний журнал. – Київ: НАУ, №1(54), 2012. с.104-108.

УДК 004.056.5(045)

Журиленко Б.Є. Математична модель вірогідної надійності комплексу технічного захисту інформації
Анотація. *В даній роботі запропонована математична модель вірогідної надійності комплексу технічного захисту інформації (КТЗІ). Побудова моделі ґрунтується на основних початкових даних властивих захисту. Модель надійності КТЗІ орієнтована на вірогідності зломів кожного захисту в часі або всього комплексу і надалі дозволить порівняти розрахункові результати з реальними даними зломів і захищеності.*
Ключові слова: *захист інформації, надійність, вірогідність злому, комплекс технічного захисту інформації.*

Zhurilenko B.E. Mathematical model of reliable reliability for complex of technical information security
Abstract. *In the given work the mathematical model of probabilistic reliability of complex of technical information security is offered. Construction of model is based on master initial data of inherent to defence. The model of the complex of technical information security reliability is oriented on probability of breaking of every defence in time or all complex in and will in future allow to compare computation results to the real data of breaking and protected in.*
Keywords: *information security, reliability, probability of breaking in, complex of technical information security.*

Отримано *28 вересня 2012 року* , затверджено редколегією *27 листопада 2012 року*
(рецензент д.т.н., професор Г.Ф. Конахович)

АНАЛІЗ ІСНУЮЧИХ ШАБЛОНІВ СИСТЕМ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Анна Чунарьова, Андрій Чунарьов

Національний авіаційний університет

ЧУНАРЬОВА Анна Вадимівна, к.т.н., доцент

Рік та місце народження: 1987 рік, м. Вентспілс, Латвія.
Освіта: Національний авіаційний університет, 2009 рік.
Посада: доцент кафедри комп'ютеризованих систем захисту інформації кафедри з 2012 року.
Наукові інтереси: інформаційна безпека, телекомунікації.
Публікації: 63 наукові публікації, серед яких наукові статті, патенти на корисні моделі та навчально-методичні роботи.
E-mail: chunariova@gmail.com

ЧУНАРЬОВ Андрій Вадимович

Рік та місце народження: 1992 рік, м. Вентспілс, Латвія.
Освіта: Національний авіаційний університет
Посада: студент 4 курсу кафедри комп'ютеризованих систем захисту інформації кафедри з 2009 року.
Наукові інтереси: інформаційна безпека, телекомунікації.
Публікації: 42 наукові публікації, серед яких наукові статті та патенти на корисні моделі.
E-mail: chunariov@ukr.net

Анотація. *У даній статті проведено аналіз шаблонів автентифікації в сучасних інформаційно-комунікаційних системах та мережах. В результаті проведено аналізу виділені переваги та недоліки застосування існуючих шаблонів для забезпечення надійного захисту. Виділені найбільш ефективні з точки зору розмежування та контролю доступу до інформаційних ресурсів.*

Ключові слова: *захист інформації, автентифікація, верифікатор, інформаційно-комунікаційна система та мережа, система захисту.*

Актуальність. На сьогодні розмежування доступу в інформаційно-комунікаційних системах та мережах (ІКСМ) полягає в розділенні і організації доступу до інформації користувачів відповідно до їх