Моделирование системы комплексной защиты конфиденциальной информации от кибернетических атак с внедрением блока адаптивного мониторинга

Д.В. Леонов

Краснодарское высшее военное училище им. генерала армии С.М. Штеменко

Аннотация: Данная работа исходит из невозможности достаточного противопоставления средств и методов защиты перед постоянно обновляющимися и модернизирующимися кибернетическими атаками нарушителя. Актуальность данной проблемы заключается в том, что существующие на данный момент системы защиты конфиденциальной информации не обеспечивают всестороннего и глобального контроля. Барьеры защиты и методы защиты остаются однонаправленными и не достаточно надежными, современные системы не обладают элементами подсистемы поддержки и принятия решения, а также элементами адаптации, что приводит к потере важной конфиденциальной информации. В статье приведен разбор предполагаемой системы защиты конфиденциальной информации. Сделан вывод о необходимости всесторонней защиты, так как отсутствие комплексного контроля системы, приводит к досрочным отказам и потере важной конфиденциальной информации. Целью данной статьи является создание комплексной, с внедрением блока адаптивного мониторинга, системы защиты конфиденциальной информации, способной обеспечить всесторонний контроль, наблюдение, своевременный интеллектуальный анализ и принятие решений, а также отражение кибернетических атак нарушителя.
Ключевые слова: система защиты конфиденциальной информации, блок адаптивного мониторинга, подсистемы защиты, комплексная систем защиты конфиденциальной информации, вероятностная оценка.

В настоящее время одним из самых распространенных видов атак на защищаемые информационные ресурсы, являются кибернетические атаки. Поэтому решение вопроса комплексной защиты от данного вида атак является весьма актуальным. Предложено решение по интеллектуальному действию системы защиты за счет внедрения блока адаптивного мониторинга, который поможет решить проблему непрерывного контроля и принятия решения при воздействии кибернетических атак на систему защиты. В данной статье рассматривается новая модель защиты за счет комплексного контроля процесса защиты конфиденциальной информации. Данная модель позволяет за счет распределения канальной защиты системы обработки конфиденциальной информации, добиться снижения отказов в

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

работе и подключения различных подсистем защиты, а также методов защиты.

Комплексная система защиты конфиденциальной информации должна полностью контролировать не только внутренние процессы и методы защиты, но внешние, связанные с процессами обработки и передачи конфиденциальной информации. Смысл заложен не только в защите канала передачи данных, а в комплексной защите всего процесса обработки конфиденциальной информации.

Можно предположить, что при обработке конфиденциальной информации, подсистема защиты информации будет направлена на криптографическую защиту от внешних и внутренних процессов воздействия на обрабатываемую информацию, но вопрос резервных криптографически стойких каналов и методов защиты системы обработки конфиденциальной информации остается открытым и будет изучен в данной работе.

Рассмотрим комплексную систему защиты конфиденциальной информации (далее - КСЗИ) от кибернетических атак, которая обладает основным защищенным каналом передачи информации и двумя запасными.

Применение трех независимых каналов понижает риск компрометации обрабатываемой информации, повышает криптографическую стойкость и безотказность ее функционирования. Оценку надежности функционирования будем вычислять через показатели отказа функционирования системы обработки конфиденциальной информации (далее - СОКИ) после осуществления кибернетических атак. СОКИ – объект адаптивного мониторинга.

Пусть $F_{\text{AM}}(r)$ – конечная функция адаптивного мониторинга с шагом r + 1, являющаяся конечным требуемым результатом блока адаптации.

Пусть имеется подсистема защиты СОКИ, состоящая из внешнего процесса обеспечивающего информационную защиту от кибернетических

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

атак и внутреннего, обеспечивающего безопасную обработку и хранение данных в СОКИ. Будем считать, что безотказность работы в СОКИ на внутреннем уровне всегда обеспечивается. Основное внимание уделим обеспечению безотказной работы в СОКИ на уровне внешнего процесса описываемого в следующем виде:

$$\Pi_{\text{внешн}} = \langle \text{B}, \text{A}_n, \rangle;\ n = 1,2,3,$$

где: *B* – подсистема защиты от кибернетических атак в СОКИ;

A_1 – основной канал с пропускной способностью μ_0;

A_2, A_3 - резервные каналы с интенсивностями защиты μ_1 и μ_2, соответственно;

Введем допущение: каналы выбираются последовательно, в прямом порядке, в зависимости от количества кибернетических атак в СОКИ, по принципу, какой канал, наиболее защищенный в данный момент времени, тот и в приоритете.

Получение разрешения на работу в том или ином канале будем рассматривать как простейший поток событий со следующими параметрами [1, 2]:

λ - криптографическая стойкость (среднее число методов шифрования, приходящееся в единицу времени);

$F(t) = 1 - e^{-\lambda t}$ – закон, распределения вероятности появления одного метода шифрования за время t;

$P_0(t) = e^{-\lambda t}$ – вероятность того, что за время t не появится ни одна кибернетическая атака (далее - кибератак).

В каналах происходит обработка возникших кибератак, причем обработка кибератак ($m_{i\text{обр}}$) распределена по показательному закону [1-3]:

$$g(t) = \mu_i . e^{\mu_i \cdot t},\ (i=0,\ 1,\ 2),$$

$$\mu_i = {}^{1}/_{m_{i\text{обр}}},\ (i=0,\ 1,\ 2).$$

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

Итак, будем рассматривать комплексную систему защиты СОКИ как трехканальную подсистему защиты, причем отражение кибератак на каждом канале происходит с разной интенсивностью μ_i: (i=*0, 1, 2*).

Найдем значение криптографической стойкости от потока кибератак, при которой необходимо подключать запасные каналы обработки информации [4,5] и вероятность безотказной работы рассматриваемой подсистемы защиты. Но перед этим введем систему целевых функций адаптивного мониторинга СОКИ в общем виде, как комплексную функцию совместной последовательной адаптации системы оцениваемых параметров, процедуры наблюдения, системы параметров качества, метода оценивания, процедуры прогнозирования в рамках мониторинга СОКИ:

$$F_{\text{АМ}}(r)=\{F_{\text{соп}}(r)\}\cup\{F_{\text{ПН}}(r)\}\cup\{F_{\text{СПК}}(r)\}\cup\{F_{\text{МО}}(r)\}\cup\{F_{\text{ПП}}(r)\}$$

В данном случае, комплексная целевая функция адаптивного мониторинга СОКИ, может представлять собой объединение целевых функций адаптации к конкретным условиям свойствам комплексной системы защиты СОКИ и зависеть от условий воздействия и интенсивности кибернетических атак.

Далее рассмотрим данную трехканальную подсистему защиты при работе только одного основного канала.

Тогда мы можем рассмотреть данную подсистему как одноканальную систему комплексной защиты с отказами. Тогда вероятность отказа считается по формуле:

$$P_{\text{отк}}=\frac{\frac{\lambda}{\mu_1}}{1+\frac{\lambda}{\mu_1}}=\frac{\lambda}{\mu_1+\lambda} \quad (1)$$

Так как для системы обработки конфиденциальной информации допустимой вероятностью отказа является значение, не превышающее 0,05, то мы можем найти максимальное допустимое значение криптографической

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

стойкости от кибератак, при котором обеспечивается надежное бесконтактное состояние основного канала:

$$P_{\text{отк}} \leq 0{,}05 \quad (2)$$

$$\frac{\lambda}{\mu_1+\lambda} \leq 0{,}05 \quad (3)$$

$$\frac{0{,}95\lambda-0{,}05\mu_1}{\mu_1+\lambda} \leq 0 \quad (4)$$

Так как $\lambda \succ 0$ и $\mu_1 \succ 0$, то получаем:

$$0{,}95\lambda - 0{,}05\mu_1 \leq 0 \quad (5)$$

$$\lambda \leq \frac{\mu_1}{19} \quad (6)$$

Таким образом при значениях криптографической стойкости от кибератак не удовлетворяющим условию (37), подсистема защиты не может обеспечить безотказную работу СОКИ и необходимо подключать запасной канал защиты информации A_2.

Найдем вероятность отказа данной подсистемы при включении запасного канала A_2 «рис 2».

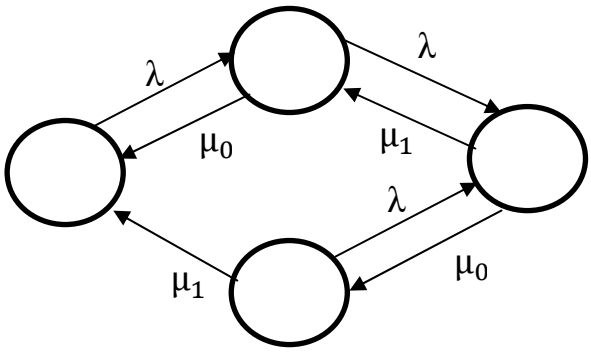

Рис. 2 - Вероятность отказа данной подсистемы при включении запасного канала A_2.

Для этого рассмотрим следующие состояния подсистемы:

x_0 – свободны все каналы;

x_1 – занят первый канал;

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

x_2 – занят второй канал.

x_3 – заняты 2 канала.

Определим вероятности состояния подсистемы в каждый из моментов времени *t*

$$P_0(t),\ P_1(t),\ P_2(t),\ P_3(t), \quad (7)$$

при условии

$$\sum_{k=0}^{3} P_k(t) = 1 \quad (8)$$

Составим дифференциальные уравнения для состояний подсистемы (7).

1. Зафиксируем момент времени *t* и найдем вероятность того, что в момент времени $t+\Delta t$ подсистема будет находиться в состоянии x_0. Это возможно при:

A – в момент *t под*система находилась в состоянии x_0 и за промежуток времени Δt не переходит в другое состояние;

B – в момент *t* подсистема находилась в состоянии x_1 и за промежуток времени Δt переходит в состояние x_0.

C – в момент *t* подсистема находилась в состоянии x_2 и за промежуток времени Δt переходит в состояние *0*.

$$P_0(t) + P_0(t+\Delta t) = P(A) + P(B) + P(C) \quad (9)$$

Вероятность события *A* равна:

$$P(A) = P_0(t) \cdot e^{-\lambda \cdot \Delta t} \approx P_0(t) \cdot (1 - \lambda \cdot \Delta t) \quad (10)$$

Вероятность события B равна:

$$P(B) = P_1(t) \cdot \mu_0 \cdot \Delta t \quad (11)$$

Вероятность события C равна:

$$P(C) = P_2(t) \cdot \mu_1 \cdot \Delta t \quad (12)$$

Подставим в формулу вероятности нахождения подсистемы в состоянии x_0 значения из формул (10-12) [1]:

$$P_0(t+\Delta t) = P_0(t) \cdot (1 - \lambda \cdot \Delta t) + P_1(t) \cdot \mu_0 \cdot \Delta t + P_2(t) \cdot \mu_1 \cdot \Delta t \quad (13)$$

$$P_0(t+\Delta t) + P_0(t) = -P_0(t) \cdot \lambda \cdot \Delta t + P_1(t) \cdot \mu_0 \cdot \Delta t + P_2(t) \cdot \mu_1 \cdot \Delta t \quad (14)$$

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

Разделим обе части на Δt, и при t→0 перейдем к дифференциальному уравнению:

$$\frac{\partial P_0(t)}{\partial t} = -P_0(t) \cdot \lambda + P_1(t) \cdot \mu_0 + P_2(t) \cdot \mu_1 \quad (15)$$

2. Далее зафиксируем момент времени *t* и найдем вероятность того, что в момент времени *t*+Δ*t* подсистема будет находиться в состоянии x_1. Это возможно при:

A – в момент *t* подсистема находилась в состоянии x_1 и за промежуток времени Δt не перешла в другое состояние.

B – в момент *t* подсистема находилась в состоянии x_3 и за промежуток времени Δ*t* перешла в состояние x_1.

C – в момент t подсистема находилась в состоянии x_0 и за промежуток времени Δ*t* перешла в состояние x_1.

$$P_1(t+\Delta t) = P(A) + P(B) + P(C) \quad (16)$$

$$P(A) = P_1(t) \cdot e^{-(\lambda+\mu_0)\cdot\Delta t} \approx P_1(t) \cdot (1 - (\lambda + \mu_0) \cdot \Delta t) \quad (17)$$

$$P(B) = P_3(t) \cdot (1 - e^{-\mu_1 \cdot \Delta t}) \approx P_3(t) \cdot \mu_1 \cdot \Delta t \quad (18)$$

$$P(C) = P_0(t) \cdot e^{-\lambda \cdot \Delta t} \approx P_0(t) \cdot \lambda \cdot \Delta t \quad (19)$$

Подставим в формулу вероятности (10) значения из формул (17-19) [1]:

$$P_1(t+\Delta t) = P_1(t) \cdot (1 - (\lambda + \mu_0) \cdot \Delta t) + P_3(t) \cdot \mu_1 \cdot \Delta t + P_0(t) \cdot \lambda \cdot \Delta t \quad (20)$$

Переходя к дифференциальному уравнению, получим:

$$P_1(t+\Delta t) = P_1(t) \cdot (1 - (\lambda + \mu_0) \cdot \Delta t) + P_3(t) \cdot \mu_1 \cdot \Delta t + P_0(t) \cdot \lambda \cdot \Delta t \quad (21)$$

$$\frac{\partial P_1(t)}{\partial t} = -P_1(t) \cdot (\lambda + \mu_0) + P_3(t) \cdot \mu_1 + P_0(t) \cdot \lambda \quad (22)$$

3. Теперь зафиксируем момент времени t и найдем вероятность того, что в момент времени *t*+Δ*t* подсистема будет находиться в состоянии x_2. Опуская промежуточные вычисления, аналогично получим дифференциальное уравнение:

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

Отсюда аналогично переходим к дифференциальному уравнению:

$$\frac{\partial P_2(t)}{\partial t} = -P_2(t) \cdot (\lambda + \mu_1) + P_3(t) \cdot \mu_0 \quad (23)$$

4. Наконец, по аналогии получим дифференциальное уравнение для состояния x_3:

$$\frac{\partial P_3(t)}{\partial t} = -P_3(t) \cdot (\mu_1 + \mu_0) + P_2(t) \cdot \lambda + P_1(t) \cdot \lambda \quad (24)$$

Таким образом, получаем систему дифференциальных уравнений (8, 15, 22, 23, 24) [6,7]:

$$\begin{cases} \frac{\partial P_0(t)}{\partial t} = -P_0(t) \cdot \lambda + P_1(t) \cdot \mu_0 + P_2(t) \cdot \mu_1 \\ \frac{\partial P_1(t)}{\partial t} = -P_1(t) \cdot (\lambda + \mu_0) + P_3(t) \cdot \mu_1 + P_0(t) \cdot \lambda \\ \frac{\partial P_2(t)}{\partial t} = -P_2(t) \cdot (\lambda + \mu_1) + P_3(t) \cdot \mu_0 \\ \frac{\partial P_3(t)}{\partial t} = -P_3(t) \cdot (\mu_1 + \mu_0) + P_2(t) \cdot \lambda + P_1(t) \cdot \lambda \\ P_0(t) + P_1(t) + P_2(t) + P_3(t) = 1 \end{cases} \quad (25)$$

Из (25) найдем предельные вероятности состояний подсистемы в установившемся режиме [8-12]:

$$P_0 = \frac{\mu_0\mu_1(\mu_0+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (26)$$

$$P_1 = \frac{\lambda\mu_1(\lambda+\mu_0+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (27)$$

$$P_2 = \frac{\lambda^2\mu_0}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (28)$$

$$P_3 = \frac{\lambda^2(\lambda+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (29)$$

Найдем максимальное допустимое значение криптографической стойкости от кибератак, при котором обеспечивается надежное безотказное состояние основного и одного запасного каналов:

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

$$P_{\text{отк}} \leq 0{,}05 \tag{30}$$

$$\frac{\lambda^2(\lambda+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \leq 0{,}05 \tag{31}$$

Так как знаменатель больше нуля, получаем:

$$0{,}95\lambda^3 + (0{,}9\mu_1 - 0{,}05\mu_0)\lambda^2 - 0{,}05(\mu_0+\mu_1)\mu_1\,\lambda -$$

$$-0{,}05\mu_0\mu_1(\mu_0+\mu_1) \leq 0 \tag{32}$$

Так, при известных μ_0 и μ_1, мы можем найти значение уровня защиты, при которой два канала не могут обеспечить безотказную работу СОКИ, и необходимо подключать второй запасной канал защиты информации A_3.

Выведена формула нахождения критических значений уровня защиты, при которых необходимо подключать запасные каналы защиты информации, что позволяет правильно реагировать при возникновении угрозы отказа подсистемы защиты. Так же сформирована комплексная целевая функция адаптивного мониторинга СОКИ, путем объединения функций процессов, методов и систем входящих в блок адаптивного мониторинга.

В дальнейшем планируется найти вероятность отказа всей комплексной системы защиты конфиденциальной информации при обработке всех запасных каналов, описать систему поддержки принятия решений при выборе канала для обработки очередной кибератаки, блока оптимизации защитных функций комплексной системы защиты конфиденциальной информации, а также внедрения блока системы поддержки и принятия решения.

Литература

1. Венцель Е.С. Теория вероятностей. 2010. 628 с.

2. Матвеев В.Ф., Ушаков В.Г. Системы массового обслуживания. МГУ: 1984. 246 с.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

3. Коценяк М.А., Кулешов И.А., Лаута О.С. Устойчивость информационно-телекоммуникационных сетей. СПб.: Политех, 2013. 92 с.

4. Боговик А.В., Игнатов В.В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 183 с.

5. Боговик А.В., Игнатов В.В. Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.

6. Леонов Д.В. Анализ проблем системы защиты информации защищаемой государством // Наука вчера, сегодня, завтра / Сб. ст. по материалам XLIV междунар. науч.-практ. конф. № 3 . Новосибирск: АНС «СибАК», 2017. 85 с.

7. Леонов Д.В. Методика системного анализа системы защиты сведений охраняемых государством // Естественные и математические науки в современном мире / Сб. ст. по материалам LII междунар. науч.-практ. конф. № 3. Новосибирск: АНС «СибАК», 2017. 57 с.

8. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. Криптография: 1999. 123 с.

9. Banks J., Carson J., Nelson B., Nicol D. Discrete-event system simulation. New Jersey: Prentice Hall, 2000. 140 p.

10. Elliott M.R. Buyer’s guide simulation . IEE Solutions, 2000. 165 p.

11. Зотов А.И., Гриценко В.В. Надежностная модель частичного отказа в технической системе // Инженерный вестник Дона, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5759.

12. Андрианов А.В., Зикий А.Н., Давтян А.Д. Генератор частотно-модулированных сигналов // Инженерный вестник Дона, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5722.

References

1. Vencel' E.S. Teorija verojatnostej [Probability theory]. 2010. 628 p.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

2. Matveev V.F., Ushakov V.G. Sistemy massovogo obsluzhivanija [Queuing systems]. MGU: 1984. 246 p.

3. Kocenjak M.A., Kuleshov I.A., Lauta O.S. Ustojchivost' informacionno-telekommunikacionnyh setej [Stability of information and telecommunication network]. SPb.: Politeh, 2013. 92 p.

4. Bogovik A.V., Ignatov V.V. Jeffektivnost' sistem voennoj svjazi i metody ee ocenki [The effectiveness of military communication systems and methods of its evaluation]. SPb.: VAS, 2006. 183 p.

5. Bogovik A.V., Ignatov V.V. Teorija upravlenija v sistemah voennogo naznachenija [Control Theory in Military Systems]. SPb.: VAS, 2008. 460 p.

6. Leonov D.V. Nauka vchera, segodnja, zavtra. Sb. st. po materialam XLIV mezhdunar. nauch.-prakt. konf. № 3. Novosibirsk: ANS «SibAK», 2017. 85 p.

7. Leonov D.V. Estestvennye i matematicheskie nauki v sovremennom mire. Sb. st. po materialam LII mezhdunar. nauch.-prakt. konf. № 3. Novosibirsk: ANS «SibAK», 2017. 57 p.

8. Nechaev V.I. Jelementy kriptografii. Osnovy teorii zashhity informacii [Elements of cryptography. Fundamentals of Information Security Theory]. Kriptografija: 1999. 123 p.

9. Banks J., Carson J., Nelson B., Nicol D. Discrete-event system simulation. New Jersey: Prentice Hall, 2000. 140 p.

10. Elliott M.R. Buyer’s guide simulation. IEE Solutions, 2000. 165 p.

11. Zotov A.I., Gricenko V.V. Inzenernyj vestnik Dona, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5759.

12. Andrianov A.V., Zikij A.N., Davtjan A.D. Inzenernyj vestnik Dona, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5722.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019