УДК 621.391.18

АВРАМЕНКО В.С., КОЗЛЕНКО А.В.

МОДЕЛЬ ДЛЯ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПО КОМПЛЕКСНОМУ ПОКАЗАТЕЛЮ

Авраменко В.С., Козленко А.В. **Модель для количественной оценки защищенности информации от НСД в АС по комплексному показателю.**
Аннотация. В работе показана актуальность проблемы оценки защищенности информации от несанкционированного доступа (НСД) в автоматизированных системах (АС). Целью работы является разработка модели количественной оценки защищенности информации от НСД, обеспечивающей повышение эффективности управления защитой информации в организациях. Для решения задачи количественной оценки защищенности информации предложен комплексный показатель — коэффициент защищенности АС. На основе данного показателя проведен сравнительный анализ типовых АС предприятий, приведены рекомендации по повышению их уровня защищенности.
Ключевые слова: информация, оценка защищенности, несанкционированный доступ, автоматизированная система, коэффициент защищенности.

Avramenko V.S., Kozlenko A.V. **Model for a quantitative estimation of information security from unauthorized access in the automation system on a complex metric.**
The summary. In this article the urgency of information security estimation problem from unauthorized access in the automation system is shown. The purpose of the article is working out a model for a quantitative estimation of information security from unauthorized access, which provide increasing efficiency management of information security in the organizations. For solution of the information security quantitative estimation task the complex metric is offered — security coefficient of the automation system. On the basis of the given metric the comparative analysis for the standard automation systems of firms is carried out, guidelines on rise of their level of security are resulted.
Keywords: information, security estimation, unauthorized access, automation system, security coefficient.

1. Введение. Оценка уровня защищенности должна производиться на всех этапах жизненного цикла автоматизированной системы (АС), при различной степени полноты и достоверности имеющейся информации. Исследование вопросов оценки защищенности информации от несанкционированного доступа (НСД) в АС является основой для разработки количественных требований к создаваемым системам защиты информации и их подсистемам. Целью работы является разработка модели для количественной оценки защищенности информации от НСД, обеспечивающей повышение эффективности управления защитой информации в организациях за счет комплексного показателя,

учитывающего как характеристики процесса нарушений безопасности, так и характеристики процесса защиты.

2. Основная часть. В настоящее время становление научного направления, связанного с исследованием и оцениванием защищенности данных от НСД в АС, сдерживается отсутствием единого понятийного аппарата в области защиты информации от НСД, преобладанием в руководящих документах качественных подходов к оценке защищенности от НСД в АС, ориентацией на статические условия функционирования систем защиты. Для аттестации АС и сертификации средств вычислительной техники согласно требованиям действующих в РФ нормативных документов (руководящих документов Федеральной службы по техническому и экспортному контролю РФ ГОСТ Р ИСО/МЭК 15408—2002, ГОСТ Р ИСО/МЭК 17799—2005) необходимы высокая квалификация персонала, обработка больших объемов данных и значительные затраты времени. У известных отечественных и зарубежных методик количественного оценивания защищенности информации (подход на базе анализа информационных рисков [1], подход на основе модели системы обеспечения безопасности Клементса [2, 3]) есть ряд недостатков, не позволяющих напрямую использовать их для оценки защищенности, а именно:

— не учитывается реальная структура АС;

— оценивается стоимость потерь от НСД к информации в денежных единицах, что приемлемо не для всех АС;

— не полностью учитываются вариативность сценариев реализации НСД и динамические характеристики процесса защиты информации.

Защищенность информации в АС от НСД определяется защищенностью ее ресурсов. Для оценки защищенности целесообразно использовать ее комплексные показатели, учитывающие и процессы нарушения безопасности ресурсов в АС, и процессы контроля и восстановления их защищенного состояния. В качестве такого показателя предлагается использовать коэффициент защищенности информации АС от НСД, аналогичный используемому в теории надежности коэффициенту готовности.

При наличии возможности восстановления защищенности только одного ресурса для расчета коэффициента защищенности информации от НСД в АС может использоваться следующая формула:

$$K_{\text{зщ АС}} = \frac{1}{\sum_{i=0}^{N_{\text{зр}}} A_{N_{\text{зр}}}^{i} \left(\frac{\lambda_{\text{нб}i}}{\mu_{\text{вз}i}} \right)^{i}}, \qquad (1)$$

где $N_{\text{зр}}$ — число защищаемых ресурсов, $A_{N_{\text{зр}}}^{i} = \frac{N_{\text{зр}}!}{(N_{\text{зр}} - i)!}$ — число размещений из $N_{\text{зр}}$ по i, $\lambda_{\text{нб}}$ — интенсивность нарушений безопасности ресурсов, $\mu_{\text{вз}}$ — интенсивность восстановления защищенности ресурсов.

При условно неограниченных возможностях по восстановлению защищенности ресурсов используемая формула будет иметь вид:

$$K_{\text{зщ АС}} = \prod_{i=1}^{N_{\text{зр}}} \frac{\mu_{\text{вз}}}{\lambda_{\text{нб}} + \mu_{\text{вз}}}. \qquad (2)$$

Проведем сравнительный анализ защищенности информации от НСД на примере трех АС, построенных на основе локальных вычислительных сетей и отличающихся масштабом и возможностями системы защиты. Каждый сотрудник организации имеет рабочую станцию, функционирующую под управлением операционной системы Microsoft Windows 7, на которой находятся его пользовательские данные. Рабочие станции объединены в вычислительную сеть с несколькими серверами на базе операционной системы Microsoft Windows 2008 Server, на которых функционируют почтовый сервер, СУБД, Web-сервер предприятия, мгновенная система обмена сообщений для сотрудников и т. д. Пусть АС первого предприятия имеет 50 критически важных защищаемых ресурсов (5 общих ресурсов, расположенных на серверах, 45 ресурсов — пользовательские данные на их рабочих станциях), АС второго предприятия имеет 100 критически важных защищаемых ресурсов (10 общих ресурсов, 90 ресурсов — пользовательские данные), АС третьего предприятия имеет 150 критически важных защищаемых ресурсов (15 общих ресурсов, 135 ресурсов — пользовательские данные).

В расчете на наихудший случай предположим, что нарушитель «идеален» (имеет высокую квалификацию, постоянно отслеживает появление новых уязвимостей, а также имеет возможность мгновенно использовать их для осуществления НСД к информации, обрабатываемой в АС рассматриваемых организаций). При использовании такой модели нарушителя интенсивность нарушений безопасности информации АС соответствует интенсивности появления уязвимостей в программном

обеспечении АС. Анализ общедоступной статистики по обнаружению уязвимостей в АС на основе ОС Windows показал, что интенсивность в среднем составляет девять нарушений безопасности в месяц, т.е. $\lambda_{\text{нб}} = 0{,}013/\text{час}$. Обычно администратор безопасности АС организации может в каждый момент времени восстанавливать защищенность лишь одного ресурса. Тогда, используя формулу (1), можно получить зависимость коэффициента защищенности информации в АС от интенсивности восстановления ее защищенности в данных условиях (рис. 1).

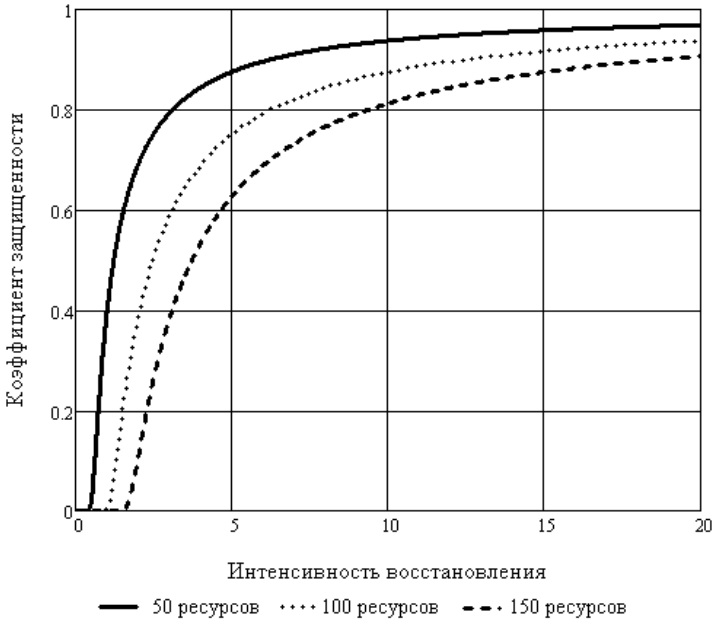

Рис. 1. Зависимость коэффициента защищенности информации в АС от интенсивности восстановления защищенности ресурсов при ограниченных ресурсах на восстановление.

Предположим, что в организации имеются практически неограниченные возможности по восстановлению защищенности информации. Тогда, используя формулу (2), можно получить зависимость коэффициента защищенности информации в АС от интенсивности восстановления защищенности ресурсов (рис. 2).

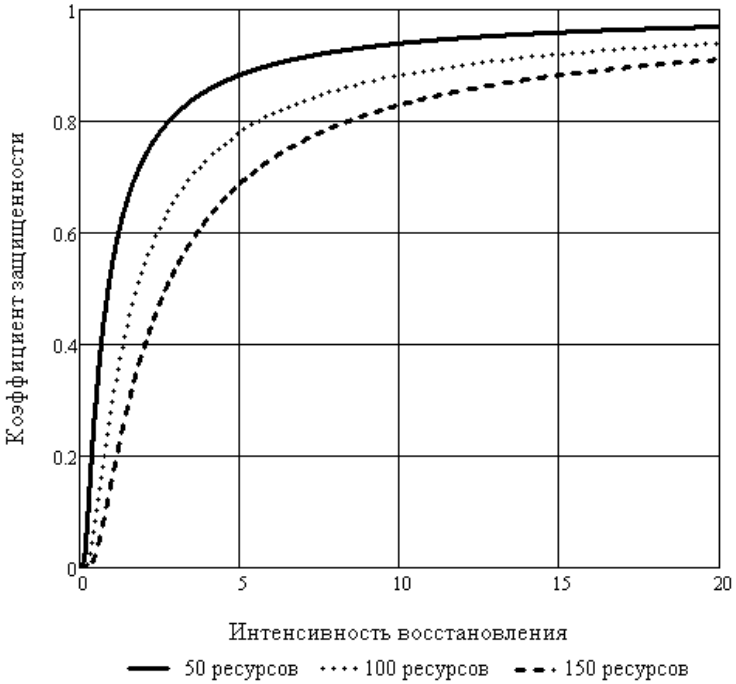

Рис. 2. Зависимость коэффициента защищенности информации в АС от интенсивности восстановления защищенности ресурсов при условно неограниченных ресурсах на восстановление.

Выясним, какая должна быть интенсивность восстановления защищенности ресурсов в АС администратором безопасности среднего предприятия (100 защищаемых ресурсов) при следующих требуемых значениях коэффициента защищенности информации от НСД в АС: $K_{\text{зщ}_1\text{АС}} = 0.9$, $K_{\text{зщ}_2\text{АС}} = 0.95$, $K_{\text{зщ}_3\text{АС}} = 0.99$. Предположим, что администратор безопасности АС предприятия имеет ограниченные ресурсы на восстановление защищенности информации, тогда для расчетов будет использоваться формула (1). Результаты расчетов приведены на рис. 3.

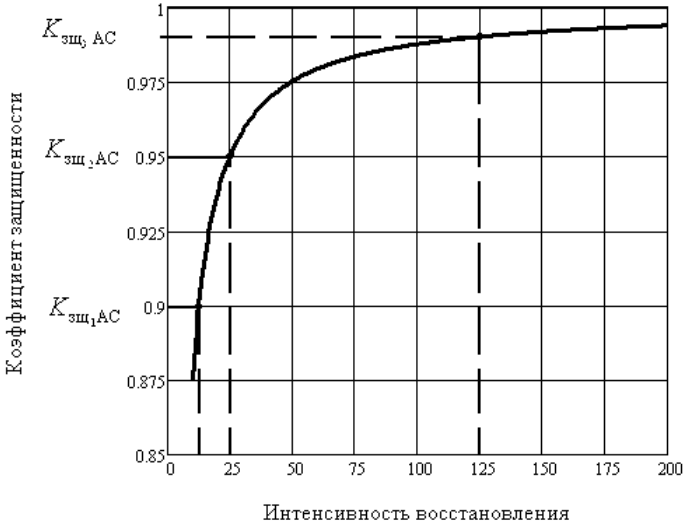

Рис. 3. Интенсивность восстановления защищенности ресурсов при $K_{зщ\ 1АС} = 0.9$, $K_{зщ\ 2АС} = 0.95$, $K_{зщ_3\ АС} = 0.99$.

Результаты расчета времени на восстановление защищенности ресурсов администратором безопасности АС представлены в таблице.

Время на восстановление защищенности при требуемых значениях коэффициента защищенности

$K_{зщАС}$	$\mu_{вз}$, раз / час	Время на восстановление защищенности ресурсов
0,9	12,5	4,8 мин
0,95	25	2,4 мин
0,99	125	28,8 с

3. Выводы. Контроль защищенности информации в АС по критерию пригодности $K_{зщ\,АС} \geq 0.99$ позволяет сделать следующие выводы:

1. Зависимость уровня защищенности информации от НСД в АС от ресурсов, выделяемых на восстановление защищенности, носит ярко выраженный нелинейный характер. Для каждой АС существует пороговое значение выделяемых ресурсов, превышение которого практически не приводит к повышению уровня защищенности.

2. Для обеспечения требуемого уровня защищенности необходимо использовать дополнительные и альтернативные средства защиты.

3. Без использования автоматических средств обнаружения нарушений безопасности ресурсов и восстановления защищенности ресурсов АС, способных функционировать в масштабе времени, близком к реальному, в условиях эксплуатации высокий уровень защищенности труднодостижим.

По мнению авторов, цель работы достигнута. Данный подход может представлять интерес как для разработчиков систем защиты информации, так и для должностных лиц, ответственных за защиту информации от НСД в организациях.

Литература

1. *Шумский А.А., Шелупанов А.А.* Системный анализ в защите информации: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. Безопасности. М. : Гелиос-АРВ, 2005. 224 с.
2. *Хоффман Л.Дж.* Современные методы защиты информации. М.: Советское радио, 1980. 264 с.
3. *Астахов А.* Анализ защищенности корпоративных автоматизированных систем // [электронный ресурс *http://www.cobit.ru/security/Pubs/Pub1_AAM_SecEval.htm/*].

Авраменко Владимир Семенович — канд. техн. наук, доцент; начальник кафедры Военной академии связи. Область научных интересов: построение автоматизированных систем управления на основе современных информационных технологий, оценивание и контроль защищенности информации в условиях различного рода неопределенности информации о состоянии защиты, автоматическое обнаружение ранее неизвестных нарушений безопасности информации на основе информационных образов, методы биометрической аутентификации. Число научных публикаций — 95. vsavr@yandex.ru; Военная академия связи, Тихорецкий проспект, д. 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9342.

Avramenko Vladimir Semenovich — PhD in Technical, associate professor; chief of chair, Military academy of signal communication. Research interests: Construction of the automated control systems on the basis of modern information technologies, the information security estimation and control in the various sort of uncertainty information security conditions, automatic detection unknown information security violations on the basis of information images, biometric authentication methods. The number of publications — 94. vsavr@ vsavr@yandex.ru; Military academy of signal communication, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9342.

Козленко Андрей Владимирович — адъюнкт Военной академии связи. Область научных интересов: оценивание и контроль защищенности информации в условиях различного рода неопределенности информации о состоянии защиты, программирование, разработка комплексов программ. Число научных публикаций — 11. et-ak@yandex.ru; Военная академия связи, Тихорецкий проспект, д. 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842. Научный руководитель — канд. техн. наук, доцент В.С. Авраменко.

Kozlenko Andrei Vladimirovich — post-graduate student, Military academy of signal communication. Research interests: the information security estimation and control in the various sort of uncertainty information security conditions, programming, complex software development. The number of publications — 11. et-ak@yandex.ru; Military academy of signal communication, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific adviser — V.S. Avramenko.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией д-р техн.наук, проф. И.В. Котенко.
Статья поступила в редакцию 22.11.2010.

РЕФЕРАТ

Авраменко В.С., Козленко А.В. **Модель для количественной оценки защищенности информации от НСД в АС по комплексному показателю.**

Оценка уровня защищенности должна производиться на всех этапах жизненного цикла АС при различной степени полноты и достоверности имеющейся информации. Исследование вопросов оценки защищенности информации от НСД в АС является основой для разработки количественных требований к создаваемым системам защиты информации и их подсистемам. Целью работы является разработка модели для количественной оценки защищенности информации от НСД, обеспечивающей повышение эффективности управления защитой информации в организациях.

Защищенность информации в АС от НСД определяется защищенностью ее ресурсов. Для решения задачи оценки защищенности целесообразно использовать комплексные показатели защищенности, учитывающие процессы нарушения безопасности ресурсов в АС, а также процессы контроля и восстановления их защищенного состояния. В качестве такого показателя предлагается использовать коэффициент защищенности информации АС от НСД. Показана зависимость коэффициента защищенности информации АС от числа защищаемых ресурсов, интенсивности нарушений безопасности ресурсов и интенсивности восстановления защищенности ресурсов при ограниченных и условно неограниченных ресурсах на восстановление защищенности. На основе данного показателя проведен сравнительный анализ типовых АС предприятий, который позволил сделать следующие выводы.

1. Зависимость уровня защищенности информации от НСД в АС от ресурсов, выделяемых на восстановление защищенности, носит ярко выраженный нелинейный характер. Для каждой АС существует пороговое значение выделяемых ресурсов, превышение которого практически не приводит к повышению уровня защищенности.

2. Для обеспечения требуемого уровня защищенности необходимо использовать дополнительные и альтернативные средства защиты.

3. Без использования автоматических средств обнаружения нарушений безопасности ресурсов и восстановления защищенности ресурсов АС, способных функционировать в близком к реальному масштабу времени, в реальных условиях эксплуатации высокий уровень защищенности труднодостижим.

По мнению авторов, цель работы достигнута. Данный подход может представлять интерес как для разработчиков систем защиты информации, так и для должностных лиц, ответственных за защиту информации от НСД в организациях.

SUMMARY

Avramenko V.S., Kozlenko A.V. **Model for quantitative estimation of information security from unauthorized access in the automation system on a complex metric.**

The security level estimation should be made at all stages of automation systems life cycle at various degree of completeness and reliability of the available information. Research the questions of an estimation of information security from unauthorized access in the automation system is a basis for working out of quantitative requirements to create information security systems their subsystems. The purpose of the article is working out a model for a quantitative estimation of information security from unauthorized access, which provide increasing efficiency management of information security in the organizations.

Information security from unauthorized access in the automation systems is defined by security of its resources. For solution of the security estimation task it is expedient to use the complex security coefficient considering both processes of resources security violation in the automation systems, and processes of the control and restoring of their defended status. As such metric it is offered to use security coefficient of information security from unauthorized access in the automation systems. Dependence of security coefficient of information from unauthorized access in the automation systems from quantity of defended resources, intensity of security violations of resources and intensity of resources security restoring is shown for limited and is conditional non-limiting resources on security restoring. On the basis of the given metric the comparative analysis of the standard automation systems of firms which has allowed to draw following outputs is carried out:

1. Dependence of information security from unauthorized access in the automation systems level from the resources selected for security restoring, has pronounced strongly nonlinear character. For every automation system exists a threshold value of the allocated resources which excess practically does not lead to increase the security level.

2. For ensuring of demanded security level it is necessary to use additional and it is desirable alternative protection frames.

3. Without using automatic sensors of resources security violation and resources security restoration in the automation system, capable to function in close to a real time scale, in real conditions of operation it is hard to mount the high security level.

According to authors, the work purpose is reached. The given approach can be of interest both for developers of information security systems, and for the officials responsible for information security from unauthorized access in the organizations.