на транспорте: тез. докл. на международ. науч.-практ. конф. – Гомель : БелГУТ, 2002. – С. 98–100.

7 Рациональные режимы вождения поездов и испытания локомотивов / под ред. С. И. Осипова. – М. : Транспорт, 1984. – 280 с.

8 **Френкель, С. Я.** Влияние некоторых эксплуатационных факторов на расход топлива магистральными тепловозами / С. Я. Френкель // Совершенствование конструкции, ремонта и обслуживания подвижного состава железных дорог: сб. науч. ст. – Гомель : БелГУТ, 1998. – С. 98–102.

Получено 12.10.2006

S. J. Frenkel, A. P. Dedinkin, E. I. Shubin, S. F. Fedorushchenko. The quality improvement of the power resources expanse rate setting by the main-line locomotives.

The objective rating of the locomotive crew work and the heat engineering condition of a locomotive requires scientifically grounded rate setting of fuel power expenses of the resources on train traction. Quality and objectivity of the setting depend to a considerable degree on the experience and qualification of the heat engineering instructor driver (operator). More widely adopted are statistic prognostication methods of the fuel expenses on train traction, which allow to estimate quantitatively the influence of each fortuity factor, influencing the fuel expense. To differentiate the separate factors action and estimate their influence on the fuel expense they use the methods of regress analysis. One can use the regress equation for the rate setting of fuel expense on a trip. A certain average trip is assumed as a standard. To realize the offered approach to the rate setting the staff of the chair "Diesel locomotives and diesel locomotives engines" of the Belarussian State University of Transport and MOAS CTC of the Belarussian railways have developed and put into operation the automatic system software of the rate setting of the power resources expense on a trip – ASS. The ASS operation control on the data array of the running schedule of some locomotive depots of the Belarussian railways and the experimental system exploitation have shown the expediency and the technical potentiality of the ASS introduction.

Вестник Белорусского государственного университета транспорта: Наука и транспорт. 2007. № 1–2(14–15)

УДК 621.391(075.8)

П. М. БУЙ, аспирант, М. Н. БОБОВ, доктор технических наук, Белорусский государственный университет информатики и радиоэлектроники, г. Минск

ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ БЕЛОРУССКОЙ ЖЕЛЕЗНОЙ ДОРОГИ

Рассматривается необходимость построения математической модели средств аутентификации для формирования системы реальных оценок их эффективности. Приводится математическое описание функций системы защиты от несанкционированного доступа. Делается утверждение о том, что средства аутентификации относятся к классу средств защиты каналов доступа. Приводится доказательство данного утверждения на основании аналитического сопоставления функций, выполняемых средствами защиты каналов доступа и средствами аутентификации.

Защита информации и информационная безопасность играют одну из ключевых ролей в управлении железнодорожным транспортом, в решении проблем безопасности движения, пассажирских и грузовых перевозок. Особенно актуальными эти вопросы стали в последнее время, в рамках динамично нарастающей информатизации отрасли.

Информатизация Белорусской железной дороги на данном этапе заключается в массовой компьютеризации, объединении персональных ЭВМ (ПЭВМ) с телекоммуникационными средствами и их организация в локальные и корпоративные сети, широкое внедрение информационно-управляющих автоматизированных систем. Эти факторы приводят к увеличению потенциальных угроз информационной и экономической сферам Белорусской железной дороги.

Внедряемые на железнодорожном транспорте современные телекоммуникационные и компьютерные технологии и создаваемые корпоративные сети отрасли являются основой для ее дальнейшего развития [1]. Вместе с тем они обусловливают появление возможностей несанкционированного доступа (НСД) к информации, нарушения ее конфиденциальности, несанкционированного искажения и уничтожения.

1 Основные функции системы защиты от несанкционированного доступа. Защита информации в корпоративных сетях (КС) от перечисленных выше угроз обеспечивается использованием технических средств и организационных мер, объединённых в единую систему защиты. Определим основные функции, которые должна выполнять система защиты от НСД.

КС в задаче защиты от несанкционированного доступа будем рассматривать как множество взаимодействий множества субъектов (S) системы и множества объектов (A) системы. В качестве субъектов в данном случае рассматривается пер-

сонал КС, а объектами являются ресурсы системы (программное обеспечение, аппаратура, данные).

Введем следующие обозначения:

– s – субъект доступа, $s \in S$;

– a – объект доступа, $a \in A$.

Взаимодействие субъектов с объектами обозначим как

$$(s,a) \in S \times A = D \qquad (1)$$

и назовем доступом субъекта s к объекту a. Зададим правила разграничения доступа $П$, по которым каждому объекту и субъекту ставится в соответствие определенный доступ. Задать правила $П$, по существу, означает определить подмножество

$$П \subset S \times A \qquad (2)$$

разрешенных доступов.

Определим множество $T = \{t\}$ моментов времени, в которые рассматривается функционирование системы. Множество T будем считать конечным подмножеством множества действительных чисел. Моменты времени t располагаются в изолированных точках числовой оси, т.е. система функционирует в дискретном времени.

Определим на множестве T множество R доступов, которые имели место в момент времени $t \in T$:

$$R \subset S \times A . \qquad (3)$$

На основе функционирования объекта защиты и в соответствии с правилами $П$ можно предположить сложившимися следующие связи:

$Y \subset S \times K$ – отношение, задающее для каждого субъекта множество каналов доступа K, которыми в соответствии с правилами пользуется субъект;

$Z \subset K \times A$ – отношение, задающее физические возможности каналов доступа в рамках правил $П$ [2].

С учётом (1) имеем

$$П \subset S \times A = Y \cap Z = S \times K \cap K \times A .$$

Непротиворечивость этих условий обеспечивает условие

$$\left[(s,a) \in П\right] \rightarrow \left[k((s,k) \in Y \;\&\; (k,a) \in Z)\right]. \qquad (4)$$

Итак, для любого времени $t \in T$ пусть заданы: $Y_t : S \rightarrow K$ – отображение, описывающее соответствие между субъектами и каналами доступа; $Y_t(s) = k$ означает, что субъект s использует в момент времени t канал k; $Y_t : K \rightarrow A$ – отображение, описывающее возможности канала в части доступа к объектам; $Y_t(k) = a$ означает, что в момент времени t субъект s имеет доступ к объекту a.

Из условия (4) следует, что

$$\left[R_t(s) = a\right] \rightarrow \left[\exists k(k \in K, Y_t(s) = k \;\&\; Z_t(k) = a)\right]. \qquad (5)$$

Доступ R_t возможен лишь в том случае, если существует канал k, который в момент времени t использует субъект s, и доступ R_t входит в возможности этого канала.

Из условия (5) следует, что для каждого s такого, что $(s,k,t) \in Y_П$, и для любого a такого, что $(k,a,t) \in Z_П$, выполнимо $(s,a,t) \in R_П$, где $Y_П$, $Z_П$, $R_П$ множества состояний КС, удовлетворяющих правилам $П$.

Тогда для обеспечения защиты от НСД достаточно наложить ограничения:

– на связь субъекта с каналом доступа в соответствии с $Y_П$,

– на действия субъекта в канале доступа в соответствии с $Z_П$.

Следовательно, функции системы защиты от НСД заключаются в ограничении доступа субъектов к каналам доступа, а также ограничении действий субъектов в канале доступа.

2 Средства аутентификации как средства защиты штатных каналов доступа. Средство защиты каналов доступа [2] в процессе своей работы выполняет четыре функции:

– обнаружение (f_1);

– опознание (f_2);

– управление (f_3);

– контроль (f_4).

К функции обнаружения относится та часть алгоритма работы средства защиты, которая обеспечивает выявление подлежащего анализу воздействия и его перевод на «язык» средства защиты.

К функции опознания относится та часть алгоритма работы средства защиты, которая обеспечивает установление соответствия между образом воздействия на входе устройства защиты определенным множествам образов допустимых воздействий, а также проверку условий установления данного соответствия.

Проверка условий установления соответствия может осуществляться в зависимости от значения других независимых параметров, которыми описывается рассматриваемое воздействие.

К функции управления относится та часть алгоритма работы средства защиты, которая обеспечивает формирование выходного воздействия на объект защиты.

К функции контроля относится та часть алгоритма работы средства защиты, которая произво-

дит контроль правильности выработанного управляющего воздействия, т. е. его соответствие анализируемому воздействию.

Рассмотрим подробнее содержание понятия «канал доступа». С позиций защиты информации, имеющиеся в КС каналы доступа можно подразделить на каналы доступа, предусмотренные эксплуатационной документацией на систему (штатные каналы доступа), и несанкционированные каналы доступа. Несанкционированные каналы доступа выявляются и устраняются на этапе разработки КС, а штатные каналы доступа защищаются соответствующими средствами защиты. Примерами штатных каналов доступа являются клавиатура автоматизированного рабочего места, служащая для взаимодействия оператора с ПЭВМ, или средство коммуникаций, посредством которого удаленное автоматизированное рабочее место (АРМ), взаимодействует с базой данных.

Как известно из научно-технической литературы по защите информации [1], доступ в защищаемую систему может предоставляться только после проведения процедуры подтверждения подлинности пользователя, которая определяется также, как процедура аутентификации. Анализ алгоритмов работы реальных средств аутентификации показал, что типовая структура средства аутентификации содержит модули обработки входных воздействий и преобразования их в необходимый вид, модули идентификации и аутентификации, модуль принятия решения о разрешении доступа к защищаемой системе или его запрете, модуль контроля правильности управляющего воздействия [3]. Поэтому вполне естественно предположить, что средства аутентификации являются средствами защиты штатных каналов доступа. В связи с этим можно сформулировать следующее утверждение: *«Средства аутентификации относятся к классу средств защиты каналов доступа»*.

Докажем это утверждение.

Как было показано выше, процесс функционирования средства защиты каналов доступа заключается в последовательном выполнении четырех функций: f_1, f_2, f_3, f_4.

$$(f_1, f_2, f_3, f_4) \in F_{\text{кд}}, \qquad (6)$$

где $F_{\text{кд}} = (f_1, f_2, f_3, f_4)$ – конечное множество функций, выполняемых средствами защиты каналов доступа.

Процесс функционирования средства аутентификации заключается в последовательной работе его модулей. Согласно [3] процесс работы модулей типовой структуры средства аутентификации можно объединить в функции: f_1', f_2', f_3', f_4'.

$$(f_1', f_2', f_3', f_4') \in F_{\text{a}}, \qquad (7)$$

где $F_{\text{a}} = (f_1', f_2', f_3', f_4')$ – конечное множество функций, выполняемых средствами аутентификации.

Достаточным для доказательства того, что средства аутентификации относятся к классу средств защиты каналов доступа, будет, соответствие друг другу определенных параметров этих средств. Целесообразно, в качестве параметров выбрать функции, которые средства защиты каналов доступа и средства аутентификации выполняют в процессе своей работы. Проведем сравнительный анализ процессов функционирования средств защиты каналов доступа и средств аутентификации.

Функция f_1 (обнаружения), выполняемая средством защиты каналов доступа, и функция f_1', выполняемая средством аутентификации, включают в себя этапы выявления подлежащих анализу внешних воздействий и их преобразование в необходимую форму. В связи с этим можно считать, что обе эти функции соответствуют друг другу: $f_1' \sim f_1$.

Функция f_2', выполняемая средством аутентификации, производит проверку законности объекта аутентификации и устанавливает, является ли он тем, за кого себя выдает. Законность объекта аутентификации устанавливается на основании одного или нескольких параметров, которые он предоставляет. Это может быть что-то, что объект аутентификации знает (пароль, ответы на ключевые вопросы), что он имеет (смарт-карта, USB-ключ), или то, что ему присуще (отпечаток пальца, рисунок радужной оболочки). После обработки этих параметров функцией f_2' они преобразуются в понятный средству аутентификации вид, становясь, тем самым, образом входного воздействия. Образы разрешенных входных воздействий объекта аутентификации внесены в базу данных средства аутентификации. На основании соответствия образа входного воздействия одному из образов базы данных средства аутентификации осуществляется проверка законности объекта аутентификации и устанавливается, является ли он тем, за кого себя выдает.

Таким образом, функция f_2 (опознания), выполняемая средством защиты каналов доступа, которая описана выше, включает в свой состав функцию f_2', выполняемую средством аутентификации. Следовательно, можно сделать вывод о том, что функции f_2 и f_2' соответствуют друг другу: $f_2' \sim f_2$.

Основной задачей функции f_3', выполняемой средством аутентификации, является выработка управляющего воздействия. Основной задачей функции f_3 (управления), выполняемой средством защиты каналов доступа, является выработка выходного воздействия, которое фактически является управляющим, т. к. перед подачей на выход устройства подвергается проверке функцией f_4 (контроля). В связи с этим можно утверждать, что функция f_3', выполняемая средством аутентификации, соответствует функции f_3, выполняемой средством защиты каналов доступа: $f_3' \sim f_3$.

Функция f_4 (контроля), выполняемая средством защиты каналов доступа, и функция f_4', выполняемая средством аутентификации, осуществляют контроль управляющих воздействий, выработанных функциями f_3 и f_3' соответственно. Функция f_4 осуществляет контроль за счет сопоставления результатов работы функции f_2 с управляющим воздействием, выработанным в результате работы функции f_3. Функция f_4' осуществляет контроль за счет сопоставления результатов работы функции f_2' с управляющим воздействием, выработанным в результате работы функции f_3'. На основании вышеперечисленного можно сделать вывод о том, что функции f_4 и f_4' соответствуют друг другу: $f_4' \sim f_4$.

На основании приведенного выше сравнительного анализа процессов функционирования средств защиты каналов доступа и средств аутентификации можно составить следующую систему:

$$\begin{cases} F_{\text{кд}} = (f_1, f_2, f_3, f_4), \\ F_{\text{а}} = (f_1', f_2', f_3', f_4'), \\ (f_1' \sim f_1) \,\&\, (f_2' \sim f_2) \,\&\, (f_3' \sim f_3) \,\&\, (f_4' \sim f_4). \end{cases} \quad (8)$$

Система (8) означает, что все функции конечного множества функций, выполняемых средствами аутентификации, попарно соответствуют всем функциям конечного множества функций, выполняемых средствами защиты каналов доступа. Тогда, согласно признаку равенства конечных множеств, который состоит в попарном равенстве всех его элементов [4], можно сделать вывод о том, что множество функций, выполняемых средствами аутентификации, соответствует множеству функций, выполняемых средствами защиты каналов доступа:

$$F_{\text{а}} \sim F_{\text{кд}}. \quad (9)$$

На основании соответствия (9) можно утверждать, что средства аутентификации относятся к классу средств защиты каналов доступа. Утверждение доказано.

Заключение. Доказательство того, что средства аутентификации относятся к классу средств защиты каналов доступа, дает возможность использовать известную в научно-технической литературе по защите информации математическую модель средств защиты каналов доступа для построения математической модели средств аутентификации, которая позволит сформировать систему реальных оценок их эффективности.

Список литературы

1 **Яковлев, В. В.** Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта : учеб. для вузов ж.-д. трансп. / В. В. Яковлев, А. А. Корниенко; под ред. В. В. Яковлева. – М. : УМК МПС России, 2002. – 328 с.

2 **Бобов, М. Н.** Обеспечение безопасности информации в телекоммуникационных системах / М. Н. Бобов, В. К. Коновелько. – Мн. : БГУИР, 2002. – 164 с.

3 **Буй, П. М.** Типовые элементы структуры средства аутентификации / П. М. Буй, М. Н. Бобов // Доклады БГУИР. – 2006. – № 5. – С. 40–47.

4 **Александров, П. С.** Введение в общую теорию множеств и функций / П. С. Александров. – М. – Л., 1948. – 315 с.

Получено 05.10.2006

P. M. Bui, M. N. Bobov. Protection of the information in corporate networks of the belarusian railway.

The necessity of construction of mathematical model of the means of authentification for formation of system of real estimations of their efficiency is considered. The mathematical description of functions of system of protection from the non-authorized access is resulted. The statement is made that the authentification's means concern to a class of means of protection of channels of access. The proof of the given statement is resulted on the basis of analytical comparison of functions which are carried out by means of protection of channels of access and the authentification's means.