ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

DOI: 10.12737/article_5926a05a06de99.61503162

Еременко В.Т., д-р техн. наук, проф.,
Шпичак С.А., ст. препод.
Брянский государственный технический университет

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ДОСТУПОМ К РЕСУРСАМ АСУ ТП ПРЕДПРИЯТИЙ СТРОИТЕЛЬНОЙ ИНДУСТРИИ И ЖКХ

frb113@lenta.ru

В статье представлены: модель процесса обеспечения доступа к ресурсам автоматизированных систем управления технологическими процессами (АСУТП) предприятий строительной индустрии и жилищно-коммунального хозяйства (ЖКХ), базовая структура автоматизированной подсистемы управления доступом и метод оперативного управления доступом на основе комбинирования политики доступа, схемы предварительного распределения аутентификаторов и полного разделения секрета. Рассмотрены алгоритмы штатного предоставления доступа и оперативного предоставления временного доступа в случае внештатных и чрезвычайных ситуаций с использованием эволюции аутентификаторов. Приведен состав программных и аппаратных компонентов автоматизированной подсистемы управления доступом к ресурсам АСУ ТП предприятий водоснабжения ЖКХ.

Ключевые слова: *автоматизированные системы управления, управление доступом, аутентификация, технологические ресурсы.*

Введение. Предприятия строительной индустрии и ЖКХ относятся к критическим объектам народного хозяйства и характеризуются наличием большого количества технологических и информационных ресурсов. Данные ресурсы на практике объединены под управлением автоматизированной системы, включающей в себя такие компоненты как ERP-системы, СУБД, САУ технологическим оборудованием, системы связи с мобильными и стационарными объектами и их позиционирования и пр.

Управление объектами в таких системах директивное, централизованное. Для АСУ характерно наличие большого количества различных каналов связи: ЛВС, полудуплексная радиосвязь в сочетании с радиомодемами, связь посредством каналов GSM и аналоговая телефонная связь.

В таких системах возникают периодические и систематические отказы в обслуживании в каналах связи. На предприятиях происходит сокращение кадров и возникает систематическая нехватка рабочих смен. В результате актуальной становится необходимость обеспечения оперативного перекрестного доступа к технологическим и информационным ресурсам в случае сложных и чрезвычайных ситуаций.

Среда управления определена как доверенная. Циркулирующая в системе технологическая информация не является конфиденциальной, но существует необходимость обеспечения ее доступности, достоверности (аутентичности) и разграничения доступа внутри доверенной среды.

На основе сравнительного анализа моделей разграничения доступа: дискреционной, мандатной, ролевой – выявлено следующее. Модели управления доступом [1] не учитывают дискретный характер доступности ресурсов и абонентов, а также надежность коммуникационных каналов. Существующие модели [2] не учитывают необходимость наличия набора аутентификаторов технологических ресурсов, требующихся для обеспечения достоверности доступа через двухстороннюю аутентификацию пользователя и ресурса.

Основная часть. На основе анализа существующих моделей управления доступом предложена формализованная модель управления доступом к ресурсам АСУ ТП ПСИ ЖКХ (таблица.1).

Данная модель учитывает наличие различных каналов связи с информационными системами и технологическим оборудованием. Кроме того, с целью повышения гибкости управления модель допускает внесение дополнительных ограничений на комбинации компонентов, например ограничения прав доступа субъекта по количеству сеансов или по времени и пр.

На основе формализованной модели управления доступом предложена базовая структура автоматизированной подсистемы оперативного

обеспечения достоверного доступа к информационно-технологическим ресурсам (рис. 1).

Структура подсистемы включает в качестве компонентов, помимо серверов доступа, пользователей и ресурсов, также коммуникационные каналы. В структурной схеме учтена возможность оперативного назначения временного аутентификатора доступа по открытому каналу связи с администратором в случае отказа в штатном канале обслуживания или перекрестного запроса из другой рабочей группы g.

Таблица 1

Формализованная модель управления доступом

<table>
<tr><td colspan="5">$M = \langle U, T, S, P, R, Z, G, F \rangle$.</td></tr>
<tr><td colspan="2">Множества</td><td colspan="2">Наборы, отношения</td><td>Базовые функции F</td></tr>
<tr><td>$U = \{u_1, u_2, ..., u_{uc}\}$</td><td>субъекты доступа</td><td>$I = \{i_1, i_2, ..., i_{ik}\}$
$A = \{a_1, a_2, ..., a_{ak}\}$</td><td>идентификаторы
аутентификаторы</td><td>$user : I \to U$,
$id : A \to I$</td></tr>
<tr><td>$T = \{t_1, t_2, ..., t_{tc}\}$</td><td>ресурсы</td><td>$C = \{c_1, c_2, ..., c_{ck}\}$
$K = \{k_1, k_2, ..., k_{kc}\}$</td><td>коммуникационные каналы
протоколы</td><td>-</td></tr>
<tr><td>$S = \{s_1, s_2, ..., s_{sc}\}$</td><td>идентификаторы сеанса</td><td colspan="2">$sid : S \to I$, $suser : S \to U$, $sauth : S \to A$.</td><td></td></tr>
<tr><td rowspan="2">$P = \{p_1, p_2, ..., p_{pc}\}$</td><td rowspan="2">права</td><td>$UP = U \times P$
$PH = P \times P$</td><td>соответствие прав
иерархия «$\succeq$»</td><td>$permission$:
$U \to 2^P$</td></tr>
<tr><td colspan="3">$permission : (u_i) \subseteq \{p \mid (\exists p_0 \succeq p) \wedge ((u_i, p_0) \in UP)\}$</td></tr>
<tr><td>$R = \{r_1, r_2, r_3, r_4, r_5\}$</td><td>роли</td><td>$UR = U \times R$
$RP = R \times P$
$RH \in R \times R$</td><td>субъект-роль
субъект-права
иерархия «$\succeq$»</td><td>$role : S \to R$</td></tr>
<tr><td>$Z = \{z_1, z_2, ..., z_{zc}\}$</td><td>серверы доступа</td><td colspan="2">$z_i = \langle u_i, t_j, g_k \in G \rangle$</td><td>-</td></tr>
<tr><td rowspan="2">$G = \{g_1, g_2, ..., g_{gc}\}$</td><td rowspan="2">пользовательские группы</td><td colspan="2">$u_i \subset g_i$ для $j \in \{1, ..., uc\}$ и $i \in \{1, ..., gc\}$</td><td>$serv : Z \to G$,</td></tr>
<tr><td colspan="3">$autorization$:
$t_i \times \{permission(u_k) \mid u_k \in U\} \times U \to \{ok, access\ denied\}$</td></tr>
<tr><td colspan="5">Правило взаимодействия пользователей и информационных ресурсов</td></tr>
<tr><td colspan="5">$\exists \langle g, privacy \rangle \in D_r(t) : g \in D_p(u) \wedge privacy \geq access(u)$</td></tr>
<tr><td colspan="5">Правило предоставления оперативного перекрёстного доступа</td></tr>
<tr><td colspan="5">$\exists \langle a, c \rangle \in D_c(t) : a \in A, c \in C : a \in sauth(s) \wedge resourses(t, k, a, c)$</td></tr>
</table>

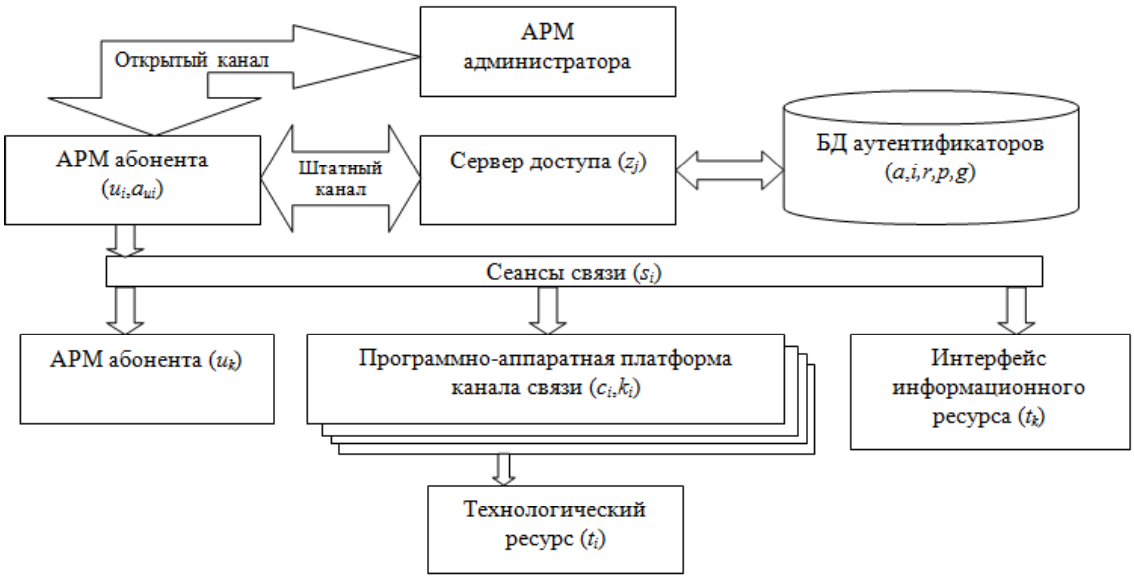

Рис. 1. Структурная схема автоматизированной подсистемы оперативного обеспечения достоверного доступа к информационно-технологическим ресурсам

На базе формализованной модели и структурной схемы предложен метод обеспечения доступа к информационно-технологическим ресурсам на основе предварительного распределения депонированных аутентификаторов [3].

Предложенный метод предусматривает комбинированное совместное применение политики управления доступом, схемы предварительного распределения ключей, схемы разделения секрета для выработки временного аутентификатора доступа и алгоритма эволюции аутентификаторов.

В доверенной коммуникационной среде рекомендовано использование уникального ключа для связи между каждой парой абонентов, что влечет за собой для сети из n абонентов необходимость генерации и хранения $n(n-1)/2$ ключей. Причем каждый из n абонентов должен хранить $n-1$ аутентификатор. Сократить количество аутентификаторов, генерируемых и хранимых в среде автоматизированной системы управления позволяет применение схем предварительного распределения ключей (Блома, KDP и пр.).

Рассмотрим в качестве базовой схемы предварительного распределения аутентификаторов схему Блома [4]. В данной схеме над конечным полем F фиксируется n различных нетривиальных элементов $r_1, \ldots, r_n \in F$, которые приписываются в качестве идентификаторов абонентам сети. Далее выбирается многочлен над полем F степени $2m$, $1 \le m < n$, вида

$$f(x,y)=\sum_{i=0}^{m}\sum_{j=0}^{m}a_{ij}x^i y^j, \qquad (1)$$

коэффициенты a_{ij} которого образуют симметричную относительно главной диагонали обратимую квадратную матрицу аутентификаторов $\Lambda=(a_{ij})_{m\times m}$ над конечным полем F. Матрица Λ секретна и депонируется на сервере аутентификации. Каждый абонент A получает в качестве универсального аутентификатора набор $(a_0^{(A)}, a_1^{(A)}, \ldots, a_m^{(A)})$, состоящий из коэффициентов многочлена

$$g_A(x)=f(x,r_A)=a_0^{(A)}+a_1^{(A)}x+\ldots+a_m^{(A)}x^m. \qquad (2)$$

Далее для связи между каждой парой абонентов A и B используется уникальный аутентификатор k_{AB}:

$$k_{AB}=k_{BA}=f(r_A,r_B)=g_A(r_B)=g_B(r_A), \qquad (3)$$

что в конечном итоге позволяет вместо $n-1$ хранить m аутентификаторов.

В классической схеме Блома идентификаторы находятся в открытом доступе. При использовании же комбинированной (матрично-ролевой) политики доступа используется алгоритм, реализующий правило взаимодействия пользователей и информационных ресурсов (см. табл. 1.). Устанавливается соответствие в матрице доступа между правами абонента, запрашивающего доступ и идентификатором r_B запрашиваемого информационного ресурса или абонента.

Технологические ресурсы зачастую имеют фиксированный аутентификатор доступа. Кроме того, при организации перекрестного доступа полномочия абонента могут быть ограничены по времени или количеству сеансов. Также возможен отказ в обслуживании по аутентичному (защищенному) каналу связи. Для экстренного предоставления доступа предлагается использовать комбинацию схемы предварительного распределения ключей и схемы полного разделения секрета (СРС).

Предположим необходимо предоставить доступ к технологическому ресурсу U, имеющему фиксированный аутентификатор k_U. Сервером аутентификации в данном случае генерируется случайный битовый вектор b длины m:

$$b=(b_0, b_1, \ldots, b_m)_2, \qquad (4)$$

и вычисляется временный аутентификатор r' как:

$$r'=k_U+\sum_{i=0}^{m}b_i a_i^{(A)} \text{ над полем } GF_2. \qquad (5)$$

Вычисленный таким образом временный аутентификатор r' и случайный вектор b передаются абоненту по открытому резервному каналу. Получив их, абонент восстанавливает аутентификатор k_U как:

$$k_U=r'+\sum_{i=0}^{m}b_i a_i^{(A)} \text{ над полем } GF_2. \qquad (6)$$

Для увеличения стойкости можно дополнительно применить к результату суммирования аутентификаторов функцию хэширования $H(x)$:

$$r'=k_U+H\left(\sum_{i=0}^{m}b_i a_i^{(A)}\right) \qquad (7)$$

Проведение аналогичного комбинирования возможно также на основе схемы KDP[5], основанной на пересечении множеств. Для $n>2$ абонентов и множества аутентификаторов A, $|A| = q$ вводится прямая нумерация аутентификаторов 1, 2, .. q. Выбирается некоторое семейство $\{S_1, \ldots, S_n\}$ подмножеств множества $\{1, 2, .. q\}$, являющееся семейством Шпернера в котором ни одно из подмножеств не содержится в другом. В

оригинальной схеме KDP семейство $\{S_1, \ldots, S_n\}$ представляет собой несекретную таблицу с номерами аутентификаторов из набора a_{ik}, $k \in S_i$, переданного предварительно каждому абоненту по защищенному каналу. При использовании комбинированной (матрично-ролевой) политики доступа устанавливается соответствие в матрице доступа между правами абонента, запрашивающего доступ и элементом S_i запрашиваемого информационного ресурса или абонента.

Для выработки общего аутентификатора связи между абонентами A и B используют пересечение $S_A \cap S_B$. Например:

$$k_{AB} = k_{BA} = \sum_{i=1}^{|S_A \cap S_B|} a_i \text{ над полем } GF_2. \quad (7)$$

При возникновении необходимости предоставить доступ к технологическому ресурсу U, имеющему фиксированный аутентификатор k_U, сервером аутентификации как и в предыдущем случае генерируется случайный битовый вектор b длины $m = |S_A|$:

$$b = (b_0, b_1, \ldots, b_m)_2, \quad (8)$$

и вычисляется временный аутентификатор r' как:

$$r' = k_U + H\left(\sum_{i=0}^{m} b_i a_i\right) \text{над полем } GF_2. \quad (9)$$

Вычисленный таким образом временный аутентификатор r' и случайный вектор b передаются абоненту по открытому резервному каналу. Получив их, абонент может восстановить аутентификатор k_U аналогично рассмотренному выше случаю.

Недостатком приведенных выше методов является то, что полученный абонентом A аутентификатор k_U является постоянным. Для прекращения временных экстренных прав доступа абонента A к ресурсу U предлагается использовать эволюцию аутентификаторов технологических ресурсов.

В качестве методов эволюции аутентификаторов рассмотрены: протокол одноразовой аутентификации Лампорта[6]; динамическое изменения аутентификатора в режиме гаммирования (CTR)[7]; комбинация двух предыдущих методов.

При использовании протокола Лампорта для каждого технологического ресурса U, имеющего фиксированный аутентификатор k_U, устанавливается продолжительность действия L_U базового аутентификатора k_U и предполагаемая периодичность замены L_i временных аутентификаторов k_{Ui}. Вычисляется необходимое количество периодов как

$$t = L_U / L_i. \quad (10)$$

На базовом шаге протокола используется однонаправленная функция хэширования H. Для текущего i-го периода действия временный аутентификатор k_{Ui} определяется как:

$$k_{Ui} = \underbrace{H(H(\ldots(k_U)\ldots))}_{t-i \text{ раз}} = H^{t-i}(k_U). \quad (11)$$

Таким образом для предоставления временных прав доступа абоненту A передаются сервером аутентификации по открытому каналу связи: случайный двоичный вектор b, период действия аутентификатора L_i, номер периода i , количество периодов t и временный аутентификатор r' вычисленный как:

$$r' = \underbrace{H^{t-i}(k_U)}_{k_{Ui}} + H\left(\sum_{i=0}^{m} b_i a_i^{(A)}\right) \text{над полем } GF_2. \quad (12)$$

Получив их абонент может восстановить действующий в течении периода T_i аутентификатор k_{Ui} как:

$$k_{Ui} = r' + H\left(\sum_{i=0}^{m} b_i a_i^{(A)}\right) \text{над полем } GF_2. \quad (13)$$

Недостатками данного метода являются ограниченный период действия аутентификатора k_U, а также возрастание вычислительной нагрузки при высокой интенсивности информационного обмена.

При использовании режима гаммирования, аутентификатор k_U динамически изменяется через некоторый период L_i посредством шифрования в режиме гаммирования.

Аутентификатор k_{Ui} является очередным фрагментом блочной гаммы.

$$k_{Ui} = T_s(e_K(CTR_i)), \quad (14)$$

где $CTR_1 = IV$ – инициирующий вектор (синхропосылка), $CTR_i = inc(CTR_{i-1})$ – значение счетчика, e_K – блочный алгоритм шифрования [8] на секретном ключе K, T_s – процедура взятия старших s бит.

В данном случае аутентификатор k_U может выступать как в роли ключа K так и в роли синхропосылки IV.

Два вышеописанных метода могут быть скомбинированы следующим образом. Временному администратору технологического ресурса с помощью протокола Лампорта выдается аутентификатор, используемый в качестве ключа K, а администратор в свою очередь может передавать пользователям временные аутенти-

фикаторы, сгенерированные в CTR режиме, пользуясь упрощенным способом генерации r':

$$r' = k_{Ui} \oplus H(k_{AB}) \oplus b \qquad (15)$$

где k_{AB} – общий аутентификатор связи между пользователем и администратором.

На основе предложенных метода и алгоритмов управления доступом разработан программно-аппаратный комплекс оперативного обеспечения доступа к информационно-технологическим ресурсам автоматизированных систем управления предприятиями водоснабжения, состоящий из АРМ администратора и конечных пользователей.

Программные компоненты, комплекса реализуют:

– предварительное распределение аутентификаторов (схемы Блома, KDP), в сочетании с политиками доступа;

– эволюцию аутентификаторов на основе протокола Лампорта или режима Counter (CTR);

– генерацию и передачу временных аутентификаторов доступа с использованием комбинации схемы предварительного распределения аутентификаторов и схемы полного разделения секрета.

Программная часть комплекса, разработанная с использованием высокоуровневых библиотек стандарта PKCS#11[9], использует криптопровайдер Rutoken CSP, который реализует основные операции по обеспечению имитозащиты и целостности (выработка имитовставки CMAC [7] и прочие преобразования). Подсистема мультиплатформенная, предъявляет низкие системные требования, что обеспечивает стыкуемость с аппаратным компонентом технологического оборудования.

Аппаратная часть комплекса представлена криптографическими идентификаторами Рутокен ЭЦП/ЭЦП Flash, платформой Raspberry Pi/Orange Pi и контроллерами технологического оборудования.

Результаты анализа эффективности принятых решений приведены на рисунке 1.

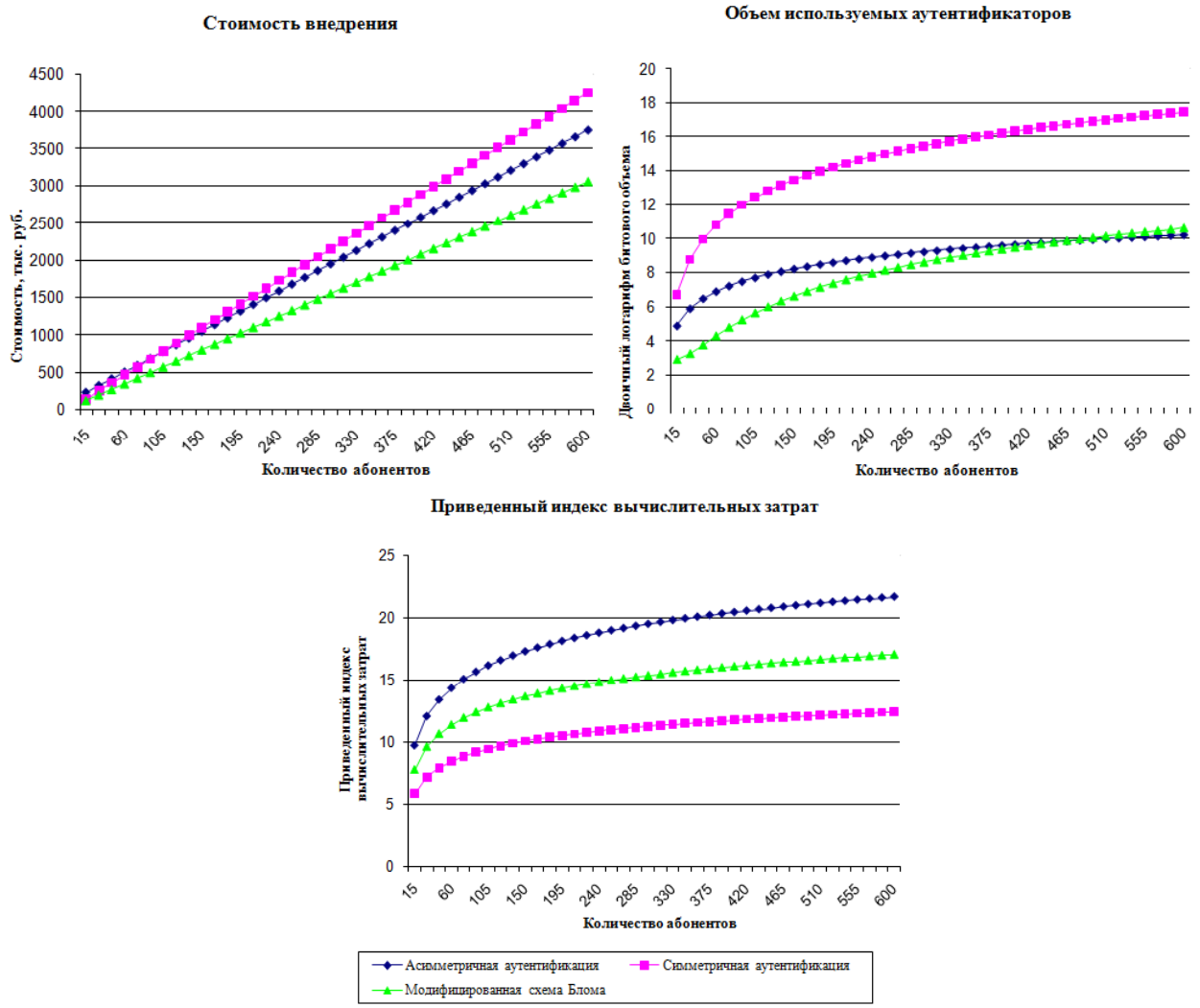

Рис. 2. Анализ эффективности подсистемы управления доступом

Выводы. Использование разработанной автоматизированной подсистемы управления доступом к ресурсам АСУ на основе модифицированной схемы Блома в штатном режиме в сравнении с асимметричной аутентификацией с использованием электронной подписи и удостоверяющего центра дает выигрыш в быстродействии, стоимости и объеме хранимых в системе аутентификаторов, при количестве абонентов до 500. В сравнении же с классическими системами симметричной аутентификации дает уменьшение стоимости и значительное уменьшение объема аутентификаторов, при незначительном снижении быстродействия.

Достоинством подсистемы является возможность предоставления оперативного перекресного доступа к ресурсам АСУ ТП предприятий строительной индустрии и ЖКХ в случае внештатных и чрезвычайных ситуаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Демидов А.В., Офицеров А.И., Афонин С.И. Моделирование процессов информационного обмена с приоритетами в сетях передачи данных промышленных предприятий // Информационные технологии в науке, образовании и производстве. 2010. Т. 5. С. 94–101.

2. Ерёменко В.Т, Мишин Д.С., Парамохина Т.М., Ерёменко А.В., Ерёменко С.В. Направления и проблемы интеграции автоматизированных систем управления для предприятий с непрерывным технологическим циклом // Информационные системы и технологии. 2014. № 3. С. 51–58

3. Рытов М.Ю., Шпичак С.А. Метод управления оперативным доступом на основе комбинирования схем предварительного распределения ключей и разделения секрета // Информация и безопасность. 2016. Т.19. вып.1 С. 118–122

4. Blom R. Nonpublic key distribution // Advances in Cryptology. Proceeding of EUROCRYPT'82 Plenum New York. 1983. Pp. 231–236.

5. Dyer M., Fenner T., Frieze A., Thomason A. On key storage in secure networks // J. Cryptology. 1995. 8. Pp. 189–200.

6. Lamport L. (July 1978). Time, Clocks and the Ordering of Events in a Distributed System // Communications of the ACM 21 (7). 1979. Pp. 558–565.

7. ГОСТ Р 34.13 – 2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. М. Стандартинформ. 2015. 38 с.

8. ГОСТ Р 34.12 – 2015 Информационная технология. Криптографическая защита информации. Блочные шифры. М. Стандартинформ. – 2015. 21 с.

9. PKCS #11 Base Functionality v2.30: Cryptoki – Draft 4. RSA Laboratories. 10 July 2009

Shpichyack S.A.

AUTOMATION ACCESS CONTROL TO THE RESOURCESOF AUTOMATED CONTROL SYSTEM IN BUILDING INDUSTRY AND UTILITIES

Model of the process of ensuring access to the resources of the process control system of building industry, the basic structure of automated access management subsystem and method of operative access control based on a combination of access policies, schemes preliminary distribution of authenticators and full of secret sharing. The algorithms provide regular access to and timely provision of temporary access in case of contingency and emergency situations using the evolution of authenticators. Given the composition of hardware and software components of the automated subsystem control access to the resources of ACS of water supply utilities.

***Key words**: automated control systems, access control, authentication, technological resources.*

Еременко Владимир Тарасович, профессор кафедры «Системы информационной безопасности».
Брянский государственный технический университет.
Адрес: Россия, 241035, Брянск, бул. 50-лет Октября, д. 7.

Шпичак Сергей Александрович, старший преподаватель кафедры «Системы информационной безопасности».
Брянский государственный технический университет.
Адрес: Россия, 241035, Брянск, бул. 50-лет Октября, д. 7.
E-mail: frb113@lenta.ru