Алгоритм адаптивного управления удаленной аутентификацией в корпоративных сетях связи

Algorithm of Adaptive Control by Remote Authentification in Corporate Communication Networks

УДК 004
Получено: 02.09.2021 Одобрено: 21.09.2021 Опубликовано: 25.09.2021

Белов А.С.
д-р техн. наук, доцент, сотрудник Академии ФСО России
e-mail: andrej2442016@yandex.ru

Belov A.S.
Doctor of Technical Sciences, Associate Professor, Employee of the Academy of the FSO of Russia
e-mail: andrej2442016@yandex.ru

Добрышин М.М.
канд. техн. наук, сотрудник Академии ФСО России
e-mail: dobrithin@yandex.ru

Dobryshin M.M.
Canidate of Technical Sciences., Employee of the Academy of FSO of Russia
e-mail: dobrithin@yandex.ru

Шугуров Д.Е.
канд. техн. наук, сотрудник Академии ФСО России
e-mail: shdevg@mail.ru

Shugurov D.E.
Candidate of Technical Sciences, Employee of the Academy of FSO of Russia
e-mail: shdevg@mail.ru

Аннотация
В работе предложен алгоритм адаптивного управления удаленной аутентификацией в корпоративных сетях связи в различных условиях состояния сети. Рассматриваемый алгоритм позволяет решить задачу управления процедурами аутентификации и обеспечения гарантированности того, что взаимодействующие субъекты и объекты остаются теми же, что и в начальной фазе соединения. При этом аутентификация осуществляется с оптимальной периодичностью, заданной вероятностью правильной аутентификацией и своевременностью и с учетом ограничения по пропускной способности и выполнения конечной цели обеспечения оперативного обмена данными в корпоративных сетях связи.
Ключевые слова: алгоритм адаптивного управления, удаленная аутентификация, достоверность, оперативный обмен данными, оптимальная периодичность.

Abstract
In operation the algorithm of adaptive control by remote authentification in corporate communication networks in various conditions of network condition is offered. Considered algorithm allow to solve the task of control of procedures of authentification and support гарантированности that interacting subjects and objects remain the same, as in an initial phase of connection. Thus authentification is carried out with optimal periodicity, the given probability the correct authentification and timeliness and taking into account restriction on transmission capacity and performance of an ultimate goal of support of an operative data interchange in corporate communication networks.
Keywords: algorithm of adaptive control, remote authentification, reliability, an operative data interchange, optimal periodicity.

Перевод в 2020 г. во время карантинных мероприятий основных финансовых потоков в цифровое пространство способствовал значительному росту финансового ущерба [1−6]. Одним из действенных методов хищения личных данных или денежных средств является компьютерная атака типа «человек посередине», направленная на подмену доверенного пользователя. Успех данной атаки обусловлен тем, что злоумышленники способны определить и воспользоваться уязвимостями алгоритмами аутентификации [7−13]. Для устранения указанной угрозы и повышении защищенности корпоративной сети связи (КСС) разработан алгоритм, предназначенный для адаптивного управления удаленной аутентификацией субъектов и объектов при удаленном доступе пользователей к информационным ресурсам ограниченного доступа, а также установления оперативного и служебного обмена данными и позволяет обеспечить выполнение требований к процедурам аутентификации в различных условиях функционирования КСС [14−20].

Целью алгоритма является:

1. Выбор метода аутентификации – $1..N$ под различные ситуации X_i, Y_j.

2. Выбор периодичности проведения аутентификации от $0…k$ для сложившейся ситуации X_i, Y_j.

3. Обоснование выбора параметров аутентификации (V – объем аутентифицирующей информации, $P_{\text{аут}}$ – вероятность правильной аутентификации, $P_{\text{ош}1,2}$ ошибки 1 и 2 рода) под различные ситуации X_i, Y_j.

4. Управление порядком взаимодействия с осуществлением третьей доверенной стороны (ТДС) и без нее под ситуации X_i, Y_j.

В настоящее время для КСС используются протоколы *NTLM, RADIUS, IPSec* и др., которые реализуют процедуры аутентификации, но при этом не позволяют реализовать адаптацию с учетом различных ситуаций и условий функционирования сети. На рис. 1 представлена удаленная аутентификация с использованием каналов ЕСЭ РФ и хранением аутентификационной информации (эталонов) непосредственно на сервере с информационным ресурсом. В данной ситуации воздействовать на процедуры аутентификации за пределами контролируемой зоны может внешний нарушитель типа Н1, Н5.

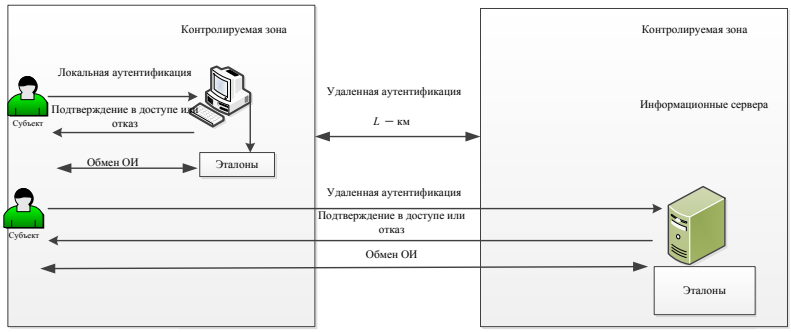

Рис. 1. Удаленная аутентификация через открытые (недоверенные) сети с аутентификацией на информационном сервере (ситуация Y_1)

На рис. 2 представлена удаленная аутентификация с использованием каналов ЕСЭ РФ с привлечением ТДС. Особенностью использования ТДС наряду с тем, что аутентификация субъектов и объектов осуществляется на ней, также имеет место при проведении подлинности самой третьей доверенной стороны.

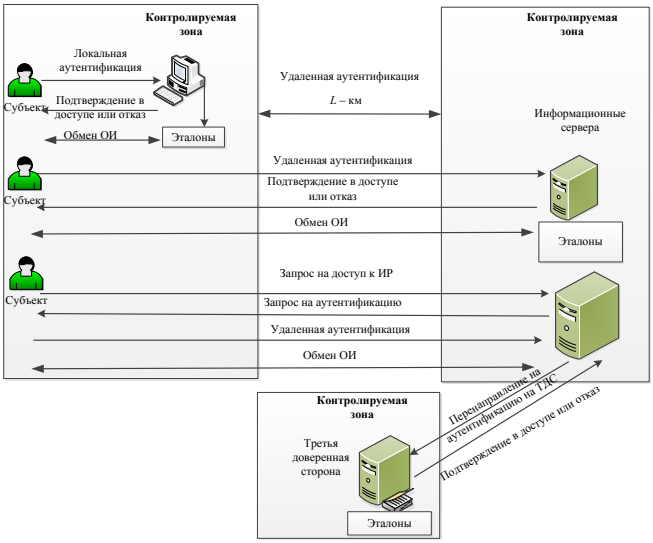

Рис. 2. Удаленная аутентификация с привлечением ТДС (ситуация Y_2)

Таким образом, учитывая ситуации Y_1, Y_2, возникает задача по выбору применения методов (способов) аутентификации (табл. 1) [21].

Таблица 1

Существующие методы и процедуры аутентификации и их характеристики

Название метода	Вид процедуры	Значение объема эталона	Вероятность правильной аутентификации	Ошибка 1 рода	Ошибка 2 рода
Биомет-рические методы	Отпечаток пальца	234 421 байт (228 бит (нейросеть))	0,998	0,01	0,3
	Голос	от 2 до 20 Кбайт	0,982	0,35	0,1
	Радужная оболочка	11 921 байт	0,99925	0,1	0,05
	Сетчатка глаза	от 40 до 160 байт	0,997995	0,001	0,4
	Геометрия	419 430 байт	0,987	0,1	0,25

	лица 2D				
	Геометрия лица 3D	838 860 байт	0,9994615	0,0047	0,103
	Геометрия руки	от 9 до 1000 байт	0,999	0,1	0,1
	Ручная подпись	40 бит (5 букв)	0,999865	0,015	0,012
Пароль	Символы	от 4 байт	≈ 1	н/о	$< 8 \cdot 10^{-8}$
	Цифры	от 4 байт	≈ 1	н/о	$< 10^{-4}$
	Символы + Цифры	от 4 байт	≈ 1	н/о	$< 4 \cdot 10^{-8}$
	С+Ц+Спец знаки	от 4 байт	≈ 1	н/о	$< 10^{-8}$
Хэш	Цифровой код	128 - 2048 бит	≈ 1	н/о	н/о
Токен	Цифровой код	32 бит + 256 бит	Зависит от реализации устройства	н/о	н/о
Смарт карта	Цифровой код	4 байта + 256 бит	Зависит от реализации устройства	н/о	н/о
Электронная подпись	Цифровой код	512 - 1024 бит	≈ 1	н/о	н/о
Сертификат	Сертификат X.509	920 байт – 1,5 Кбайт (ЭП 512 - 1024 бит)	Зависит от вероятности ошибки в канале связи	н/о	н/о

Рассматривая удаленную аутентификацию и процедуры, которые могут использоваться в зависимости от условий, необходимо учесть не только выполнение требований по правильной аутентификации $P_{\text{аут}}^{\text{тек}} \geq P_{\text{аут}}^{\text{треб}}$, но и своевременность выполнения сеанса связи $\overline{T}_{\text{сеанса}} = \overline{T}_{\text{аут}} + \overline{T}_{\text{инф.обм}}$, а также учесть возможности сети по пропускной способности информационного направления и реализовать оптимальную периодичность проведения аутентификации. При допущении на выполнение процедур аутентификации может быть выделено не более 3−5% от информационного обмена $\overline{T}_{\text{аут}} \leq (0{,}03 \div 0{,}05) \cdot \overline{T}_{\text{инф.обм}}$ [22−26]. Данное допущение обусловлено периодической аутентификацией на уровне объект – объект, которым является протокол *IPSec*, где на аутентификацию от общего размера *IP*-пакета выделяется от 3–5% $(0{,}03 \div 0{,}05)$ от общего объема оперативных и служебных данных в зависимости от режима работы протокола (транспортный или туннельный). На рис. 3 представлен обобщенный алгоритм адаптивного управления удаленной аутентификацией.

В блоке 1 вводятся исходные данные по существующей ситуации, условиям и характеристикам сети.

В блоке 2 производится формирование требований к процедурам удаленной аутентификации по своевременности и вероятности правильной аутентификации $\overline{T}_{\text{аут}}^{\text{тек}} \leq T_{\text{аут}}^{\text{треб}}$, $P_{\text{аутУА}}^{\text{тек}} \leq P_{\text{аутУА}}^{\text{треб}}$.

В блоке 3 производится комплексирование процедур аутентификации (табл. 1) для протоколов удаленной аутентификации.

В блоке 4 производится сравнение конечного количества возможных вариантов. В случае, если перебор всех вариантов не окончен, то происходит дальнейшее комплексирование и переход к блоку 3. Если перебор всех вариантов окончен, то осуществляется их оценка по своевременности выполнения в протоколах удаленного взаимодействия.

В блоке 5 производится расчет времени выполнения процедур аутентификации и оптимальной периодичности.

В блоке 6 производится сравнение выполненного протокола со всеми процедурами аутентификации по критерию своевременности $\overline{T}_{\text{аут}}^{\text{тек}} \le T_{\text{аут}}^{\text{треб}}$. Если выполненный протокол удовлетворяет критерию, то осуществляется переход к блоку 8. Если нет, то осуществляется переход к блоку 7. Кроме того, необходимо увеличить пропускную способность и перейти к блоку 1.

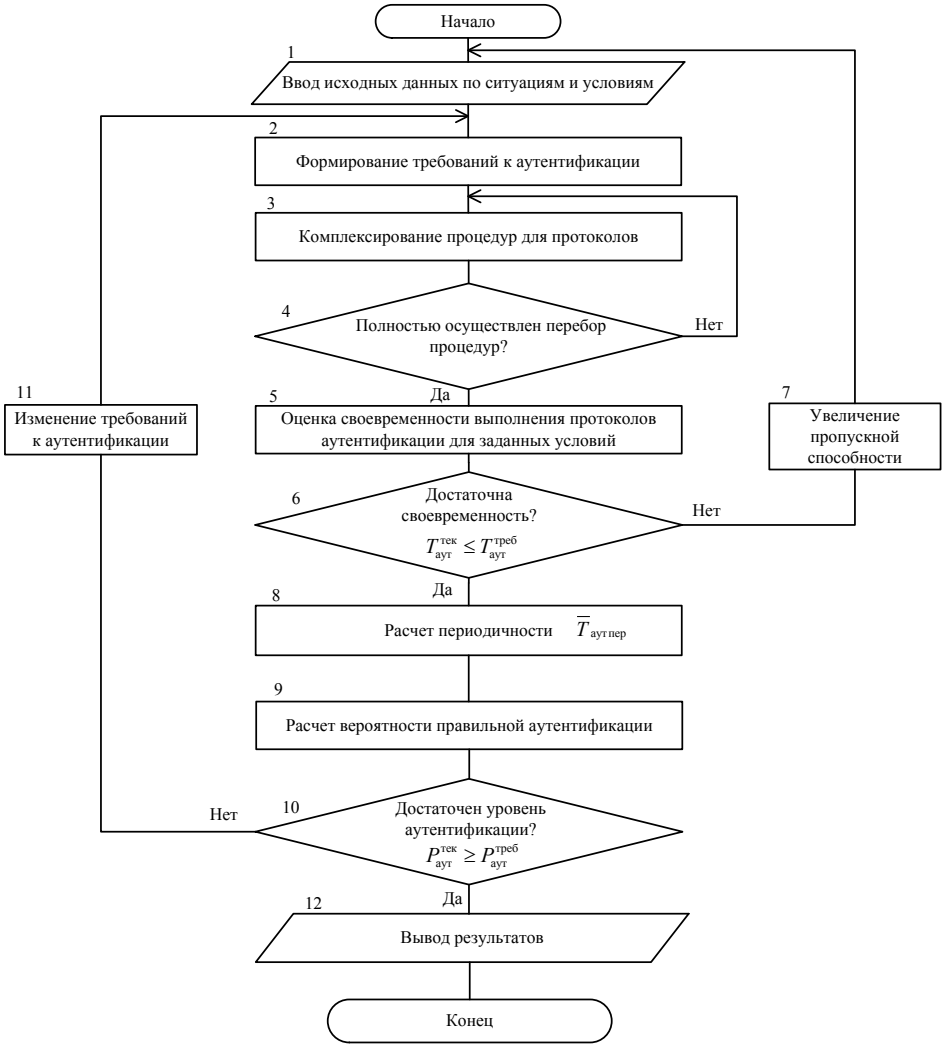

Рис. 3. Обобщенный алгоритм адаптивного управления удаленной аутентификацией

В блоке 8 решается задача определения оптимальной периодичности применения процедур аутентификации. Задача решается следующим образом.

Дано: $V_{\text{с}}$ $V_{\text{о}}$ – оперативная нагрузка; $V_{\text{аут}}$ $v_{\text{кан}}$ –

скорость канала (пропускная способность канала); $T_{\text{аут}}^{\text{треб}}$ – требуемая своевременность (канал без задержек) выполнения аутентификации; $P_{\text{аут}}^{\text{треб}}$ – требуемая вероятность правильной аутентификации.

Требуется найти среднюю оптимальную периодичность проведения аутентификации – $\overline{T}_{\text{аут}}^{\text{тек}}$.

Получим формулу для расчета среднего времени аутентификации в общем потоке данных со служебной и оперативной информацией:

$$\overline{T}_{\text{ауд}} = \frac{\overline{V}_{\text{с}} + \overline{V}_{\text{о}} + \overline{V}_{\text{аут}}}{v_{\text{кан}}} \quad (1).$$

Выдвигаем условие $\overline{T}_{\text{ауд}} \le \overline{T}_{\text{аут}}^{\text{треб}}$, что соответствует полученной своевременности аутентификации при передаче в общем трафике не менее значения требуемой.

Предположим, что $\overline{V}_{\text{с}} = 2$ Мбит, $\overline{V}_{\text{о}} = 30$ Мбит, $\overline{V}_{\text{аут}} = 5$ Мбит, $\overline{T}_{\text{аут}}^{\text{треб}} = 1$ с, $v_{\text{кан}} = 50$ Мбит/с. Тогда: $\overline{T}_{\text{ауд}} = 0{,}74$ с.

Таким образом, для заданного объема аутентификационной информации с учетом характеристик сети обеспечивается своевременность передачи аутентификации. При этом, выполняется условие $\overline{T}_{\text{аут}}^{\text{тек}} \le T_{\text{аут}}^{\text{треб}}$.

Для определения $\overline{V}_{\text{аут}}$ среднего объема аутентифицируемой информации при заданных характеристиках сети $T_{\text{аут}}^{\text{треб}}$, $v_{\text{кан}} = 50$ Мбит/с и с заданным объемом оперативной и служебной информации $\overline{V}_{\text{с}} = 2$ Мбит, $\overline{V}_{\text{о}} = 30$ Мбит.

$$V^* = T_{\text{аут}}^{\text{треб}} \cdot v_{\text{кан}} \quad (2),$$

где V^* – величина общей нагрузки V^*=50 Мбит, при которой будет обеспечена заданная своевременность $T_{\text{аут}}^{\text{треб}} = 1$, определим оставшийся ресурс, который можно предоставить под процедуры аутентификации.

Результатом расчетов является зависимость значения аутентифицирующей нагрузки в канале связи от значения периодичности проведения процедуры аутентификации при фиксированном значении пропускной способности канала связи и своевременности проведения, при этом изменяется объем оперативной и служебной нагрузки (рис. 4). Зададимся условием, при котором выполняется следующее неравенство: $V_{0_1} < V_{0_2} < V_{0_3}$.

На рис. 4 видно, что при увеличении объема оперативного трафика $V_{\text{о}}$ значения аутентифицирующей нагрузки $V_{\text{аут}}$ уменьшаются при $v_{\text{кан}} = 50$ Мбит/с. Таким образом, при фиксированном значении периодичности процедуры аутентификации $T_{\text{аут опт}} = 1$ с, при $V_{0_1} = 20$ Мбит – $V_{\text{аут1}} \le 16$ Мбит, при $V_{0_2} = 30$ Мбит – $V_{\text{аут1}} \le 10$ Мбит. Данный график зависимости позволяет определить необходимый объем аутентифицирующей информации (нагрузку) при заданной оптимальной периодичности ее проведения.

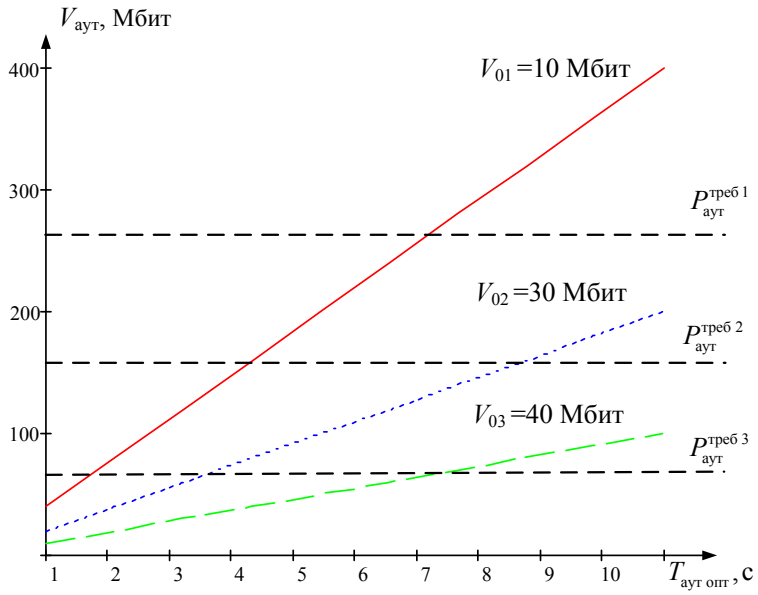

Рис. 4. Зависимость значения аутентифицирующей нагрузки от значения периодичности процедуры аутентификации

Зная объем аутентификационной информации, которую можно вводить в трафик, можно определить оптимальный период выполнения аутентификации. Исходя из заданного объема аутентификационной информации, можно определить количество процедур, что позволяет повысить вероятность правильной аутентификации. Зная характеристики оперативного трафика с заданной вероятностью правильной аутентификации, возможно определить пропускную способность канала.

В блоке 9 производится расчет вероятности правильности аутентификации процедур для различных ситуаций Y_1, Y_2.

В блоке 10 производится сравнение полученных данных по вероятности правильной аутентификации с требуемой $P_{аутУА}^{реал} \geq P_{аутУА}^{треб}$.

На рис. 4 представлен возможный максимальный порог для различных условий. Если требование не выполняется, происходит переход к блоку 11 (уточнение требований к аутентификации), в случае выполнения требования – переход к блоку 12.

В блоке 12 происходит использование процедур аутентификации на заданном информационном направлении с оптимальной периодичностью. На рис. 4 представлен условный порог по вероятности правильной аутентификации для различных условий и фиксированных параметров трафика.

Представленный алгоритм управления аутентификацией в корпоративных сетях связи позволит оптимально выбрать необходимые процедуры аутентификации для различных ситуаций и условий с требуемой вероятностью правильной аутентификации, своевременностью и возможностью оптимальной периодичности, что снижает угрозу подмены субъектов и объектов аутентификации при их взаимодействии [27−29].

Литература

1. *Сауренко Т.Н.* Прогнозирование инцидентов информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2019. − № 3. − С. 24-28.

2. *Анисимов В.Г.* Моделирование возможных последствий внешних информационных воздействий на распределенную сеть связи / *В.Г. Анисимов* [*и др*.] // Телекоммуникации. – 2020. – № 12. – С. 32–38.
3. *Анисимов В.Г.* Проблема инновационного развития систем обеспечения информационной безопасности в сфере транспорта // Проблемы информационной безопасности. Компьютерные системы. − 2017. − № 4. − С. 27-32.
4. *Анисимов Е.Г., Анисимов В.Г., Солохов И.В.* Проблемы научно-методического обеспечения межведомственного информационного взаимодействия // Военная мысль. − 2017. − № 12. − С. 45-51.
5. *Анисимов В.Г., Анисимов Е.Г., Белов А.С., Скубьев А.В.* Эффективность обеспечения живучести подсистемы управления сложной организационно-технической системы // Телекоммуникации. − 2020. − № 11. − С. 41-47.
6. *Anisimov V.G., Anisimov E.G., Saurenko T.N., Zotova E.A.* Models of forecasting destructive influence risks for information processes in management systems // Информационно-управляющие системы. − 2019. − № 5 (102). − С. 18-23.
7. *Добрышин М.М.* Моделирование процессов деструктивных воздействий на компьютерную сеть связи с применением компьютерной атаки типа «человек посередине» // Телекоммуникации. − 2019. − № 11. − С. 32-36.
8. *Anisimov V.G., Zegzhda P.D., Anisimov E.G., Bazhin D.A.* A risk-oriented approach to the control arrangement of security protection subsystems of information systems // Automatic Control and Computer Sciences. 2016. Т. 50. № 8. С. 717-721.
9. *Anisimov V.G., Anisimov E.G., Saurenko T.N.* Efficiency of ensuring the survivability of logistics information and control systems // E3S Web of Conferences: Сер. "International Scientific and Practical Conference "Environmental Risks and Safety in Mechanical Engineering", ERSME 2020" 2020. С. 07025. https://doi.org/10.1051/e3sconf/202021707025.
10. *Зегжда П.Д.* Методический подход к построению моделей прогнозирования показателей свойств систем информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2019. − № 4. − С. 45-49.
11. *Анисимов А.В., Анисимов А.Е., Анисимов В.Г., Анисимов Е.Г., Барабанов В.В.* Проблема сравнения и выбора варианта построения системы безопасности // Актуальные проблемы защиты и безопасности: Труды Четвертой Всероссийской научно-практической конференции. − 2001. − С. 348-351.
12. *Анисимов Е.Г.* Межведомственное информационное взаимодействие в сфере обороны российской федерации. − Москва: Военная академия Генерального штаба Вооруженных Сил Российской Федерации, Военный институт (управления национальной обороной), 2017. − 198 с.
13. *Добрышин М.М., Шугуров Д.Е.* Способ моделирования сетевой атаки типа "человек посередине" / Патент РФ на изобретение № 2645294 от 14.11.2016 бил. № 5. Заявка № 2016144639 от 14.11.2016. Патентообладатель: Академия ФСО России. H04W 16/22 (2009.01), G06N 7/06 (2006.01), G06N 7/04 (2006.01), H04L 12/00 (2006.01).
14. RFC 4301. Security Architecture for the Internet Protocol. S. Kent, K. Seo. December 2005.
15. *Зегжда П.Д.* Модели и метод поддержки принятия решений по обеспечению информационной безопасности информационно-управляющих систем// Проблемы информационной безопасности. Компьютерные системы. − 2018. − № 1. − С. 43-47.
16. *Анисимов В.Г.* Показатели эффективности защиты информации в системе информационного взаимодействия при управлении сложными распределенными

организационными объектами // Проблемы информационной безопасности. Компьютерные системы. − 2016. − № 4. − С. 140-145.
17. RFC 4302. IP Authentication Header. S. Kent. December 2005.
18. *Зегжда П.Д.* Эффективность функционирования компьютерной сети в условиях вредоносных информационных воздействий // Проблемы информационной безопасности. Компьютерные системы. − 2021. − № 1 (45). − С. 96-101.
19. Зегжда П.Д. Подход к оцениванию эффективности защиты информации в управляющих системах // Проблемы информационной безопасности. Компьютерные системы. − 2020. − № 1 (41). − С. 9-16.
20. *Зегжда П.Д., Зегжда Д.П., Анисимов В.Г., Анисимов Е.Г., Сауренко Т.Н.* Модель формирования программы развития системы обеспечения информационной безопасности организации // Проблемы информационной безопасности. Компьютерные системы. − 2021. − № 2 (46). − С. 109-117.
21. *Шугуров Д.Е.* Методы и протоколы аутентификации. – Орёл: Академия ФСО России, 2013. – 219 с.
22. *Ямпольский С.М.* Научно-методические основы информационно-аналитического обеспечения деятельности органов государственного и военного управления в ходе межведомственного информационного взаимодействия / Москва: Военная академия Генерального штаба Вооруженных Сил Российской Федерации, Военный институт (управления национальной обороной). 2019. − 146 с.
23. Анисимов В.Г., Анисимов Е.Г., Бажин Д.А., Барабанов В.В., Филиппов А.А. Модели организации и проведения испытаний элементов системы информационного обеспечения применения высокоточных средств // Труды Военно-космической академии им. А.Ф. Можайского. − 2015. − № 648. − С. 6-12.
24. *Анисимов Е.Г.* Показатели эффективности межведомственного информационного взаимодействия при управлении обороной государства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. − 2016. − № 7-8 (97-98). − С. 12-16.
25. Анисимов В.Г. Обобщенный показатель эффективности взаимодействия федеральных органов исполнительной власти при решении задач обеспечения национальной безопасности государства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. − 2017. − № 5-6 (107-108). − С. 101-106.
26. Зегжда П.Д. Модель оптимального комплексирования мероприятий обеспечения информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2020. − № 2. − С. 9-15.
27. *Анисимов В.Г., Селиванов А.А., Анисимов Е.Г.* Методика оценки эффективности защиты информации в системе межведомственного информационного взаимодействия при управлении обороной государства // Информация и космос. − 2016. − № 4. − С. 76-80.
28. Анисимов Е.Г., Селиванов А.А., Анисимов В.Г. Расчет эффективности межведомственного информационного взаимодействия в области обороны государства // Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации: Сборник материалов II Межведомственной научно-практической конференции.- Национальный центр управления обороной Российской Федерации. − 2016. − С. 21-26.
29. *Стародубцев Ю.И.* Методика удалённой аутентификации личности // Интернет-журнал "Технологии техносферной безопасности" (http://ipb.mos.ru/ttb). – 2015. − № 5 (63). – С. 265–273.