DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.4.3

УДК 621.391
ББК 32.811

МОДЕЛЬ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Светлана Сергеевна Козунова

Аспирант кафедры системы автоматизированного проектирования и поискового конструирования,
Волгоградский государственный технический университет
cad@vstu.ru
просп. им. Ленина, 28, 400005 г. Волгоград, Российская Федерация

Аннотация. В статье рассматриваются вопросы, связанные с управлением защитой информации в государственных информационных системах. В ходе анализа работ по этой тематике выявлено решение частных проблем. Поэтому актуальным является комплексный формализованный подход к решению задачи защиты информации в государственных информационных системах, учитывающий их специфику, угрозы и требования регуляторов. Разработана формализованная модель управления защитой информации в государственных информационных системах, определяющая эффективный набор средств защиты в соответствии с требованиями технических мер защиты, которая может быть использована для автоматизации процесса управления.

Ключевые слова: государственная информационная система, система управления, информационная безопасность, средства защиты, методы оптимизации, матрица бинарных отношений, система защиты информации, информационные технологии.

Введение

Управление защитой информации в государственных информационных системах (ГИС) актуально в связи с требованиями законодательства РФ, ценностью обрабатываемой в них информации, возрастающей ролью в становлении современного информационного общества в РФ, а также увеличением потребности в процедурах объединения информационных потоков организаций и предприятий в корпорации [2; 3; 5; 6; 16]. Построение систем защиты информации (СЗИ) в ГИС основывается на определении класса защищенности информационной системы (ИС) в зависимости от значимости обрабатываемой в ней информации, определении базового набора мер защиты информации и последующем его уточнении относительно актуальных угроз информационным ресурсам ГИС [3; 10]. Авторами работ [1; 2; 11; 17] отмечено, что при реализации угроз информационной безопасности (ИБ) ГИС возрастают материальные, репутационные, экологические и социальные риски.

Анализ проблемы и ранее проведенные исследования

Исследованию проблемы управления защитой информации в ГИС посвящены работы [3; 6; 16].

В работе [15] представлена задача формализации и определения качества данных в ГИС. Обозначены факторы и предложены меры для обеспечения их достоверности на всех этапах обмена данными. В статье [11] предлагается подход к решению задачи определения требуемого класса защищенности ГИС от угроз безопасности информации в зависимости от видов ущерба.

Некоторые авторы [7] рассматривают практические вопросы, связанные с построением СЗИ ГИС в соответствии с требованиями международных стандартов. В работе [14] описана процедура организации контроля защищенности информации в ГИС.

В статье [16] предлагается определение эффективности управления СЗИ в ГИС, основанное на оценке вероятности своевременного сбора всей необходимой информации для принятия решения.

В работе [14] рассматривается оценка и анализ влияния метрической сложности ИС на их безопасность и защищенность. Предлагается формулировка классификационных требований и мер обеспечения безопасности информации с учетом сложности ИС.

Отметим, что большинство проведенных исследований посвящены частным проблемам защиты информации в ГИС. Управление защитой информации в государственных информационных системах является актуальной проблемой. Целью данной работы является разработка формальной модели управления защитой информации в ГИС.

Угрозы нарушения информационной безопасности в государственных информационных системах

Особенностями ГИС, влияющих на защищенность информации, являются:

– сложный состав программно-аппаратных платформ и СЗИ;

– деление информационного потока на внутренний и внешний;

– территориальная распределенность компонентов;

– взаимодействие с открытыми сетями передачи данных;

– различные виды обрабатываемой информации, определяющие ее ценность;

– требования правовых, технических и иных норм эксплуатации ГИС на различных этапах ЖЦ.

В работе [11] отмечается, что ГИС подвержены таким угрозам, как кибератаки, стихийные бедствия, структурные отказы и человеческие ошибки.

По статистическим данным компании Infowatch [4] внутренний нарушитель является наиболее частой причиной утечек информации – 64,5 %, на внешние атаки приходится 35,5 %. Наиболее ценными сведениями в первом полугодии 2018 г. для злоумышленников стали персональные данные (69 %) и платежная информация (21,3 %) (рис. 1).

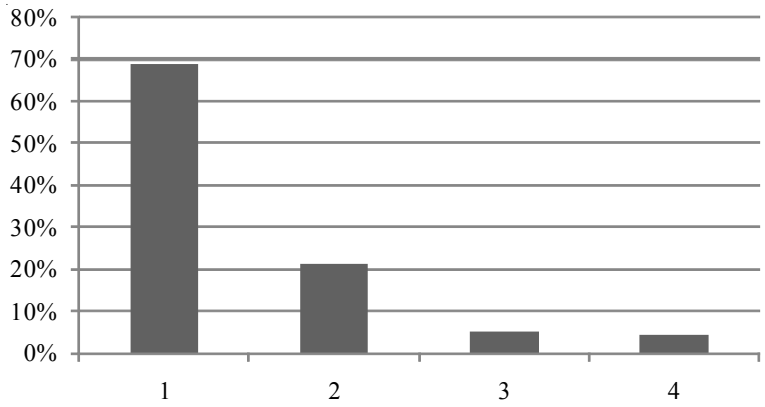

Рис. 1. Распределение утечек по типам информации:

1 – персональные данные; *2* – платежная информация; *3* – государственная тайна; *4* – коммерческая тайна

Наиболее вероятными каналами утечки информации в первом полугодии 2018 г. являются сеть и бумажные документы (рис. 2).

Отметим, что наряду с традиционными угрозами нарушения конфиденциальности, целостности и доступности для информации в ГИС характерны:

– угроза несанкционированного доступа (НСД);

– угроза отказа сетевого оборудования;

– вредоносное программное обеспечение;

– хищение данных;

– промышленный шпионаж;

– компрометация учетных данных;

– подмена исполнительных модулей;

– человеческий фактор.

Наибольший ущерб государственным информационным системам наносят угрозы нарушения целостности и угрозы, присущие центрам обработки данных (ЦОД), серверам и базам данных [6; 11]. Среднему ущербу могут подвергнуть угрозы получения НСД к информации ГИС, автоматизированным рабочим местам (АРМ) пользователей или файловому серверу [6; 11]. Анализ угроз информации в ГИС позволяет соотнести угрозы нарушения ИБ с техническими мерами и средствами ее предотвращения [8; 9; 12; 13].

Формальная модель управления защитой информации в государственных информационных системах

Пусть $K = (V, M, PC, S, TS, SB, K, R)$ – модель управления защитой информации в государственных информационных системах, где:

– V – виды информации в ГИС, определяются вектором $V = (v_1, v_2, v_3, v_4, v_5)$, каждый из которых описывается базовыми значениями $\{yes, no\}$ для v_1, v_2, v_3 и {1, 2, 3, 4} для v_4, v_5 (1– персональные данные, 2 – уровень ПДн, 3 – конфиденциальная информация, 4 – класс защищенности ИС, 5 – коммерческая тайна);

– M – масштаб ГИС, $M = \{федеральная, региональная, объектовая\}$;

– PC – параметры сети ГИС. $PC = (pc_1, pc_2, pc_3, pc_4)$, где:

- pc_1 – число АРМ в ГИС, обрабатывающих конфиденциальную информацию,
- pc_2 – число филиалов,
- pc_3 – число удаленных пользователей,
- pc_4 – взаимодействие с внешними сетями и принимающее $\{yes, no\}$;

– S – этапы жизненного цикла ГИС с определением актуальных угроз;

– TS – угрозы безопасности информации в ГИС;

– SB – множество средства защиты от угроз. $SB_i = (C_i, E_i)$, где:

- C_i – стоимость средства защиты от угрозы информации в ГИС,
- E_i – стоимость технической поддержки средства защиты в год;

– K – множество критериев оценки защищенности информации в ГИС;

– R – требования к системе защиты информации в ГИС, установленные в: [2; 12; 13].

Отношения между SB и TS, а также R задаются матрицей бинарных отношений M_n^t и L_k^t, где $m_j^i \in M_n^t$ и $l_c^i \in L_k^t$ показывают

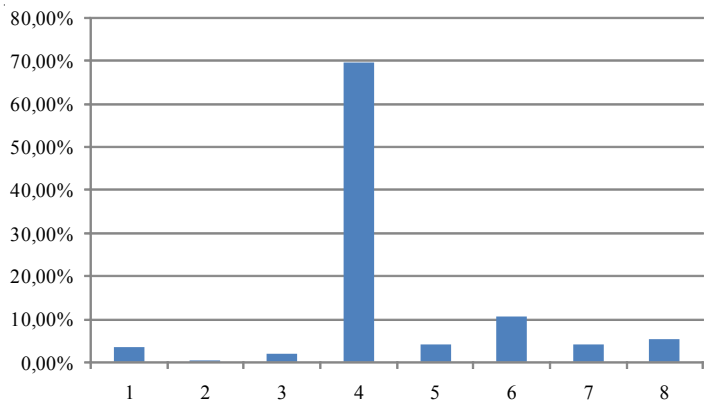

Рис. 2. Распределение каналов утечек информации:

1 – кража/потеря оборудования; *2* – мобильные устройства; *3* – съемные носители; *4* – сеть (браузер, cloud); *5* – электронная почта; *6* – бумажные документы; *7* – Instant Messenger; *8* – другие каналы

возможность перекрытия TS_j угрозы и выполнения R_c требования SB_i средством защиты. При этом:

$$m_j^i \begin{cases} 1, \text{если } TS_j \text{ перекрывается } SB_i \text{ средством защиты} \\ 0, \text{если } TS_j \text{ не перекрывается } SB_i \text{ средством защиты} \end{cases} \quad (1)$$

$$m_j^i \begin{cases} 1, \text{если } R_c \text{ перекрывается } SB_i \text{ средством защиты} \\ 0, \text{если } R_c \text{ не перекрывается } SB_i \text{ средством защиты} \end{cases} \quad (2)$$

Эффективность перекрытия n^* угроз и выполнения z^* требований СЗИ в ГИС:

$$ET = \frac{1}{n^*} \sum_{j=1}^{n^*} \sum_{i=1}^{SB} m_j^i, \quad (3)$$

$$EL = \frac{1}{z^*} \sum_{c=1}^{z^*} \sum_{i=1}^{SB} l_c^i. \quad (4)$$

Эффективность защиты информации в ГИС через определение критерия каждого средства защиты $\forall SB_i \in SB$ зададим вектором $EK = (K_1, \ldots, K_n)$, где K_i – i-критерий. EK считается эталоном, если $\forall K_i = 1$. Эффективность средства защиты вычисляется по формуле:

$$E(EM, EF_{SBi}) = \sqrt{\sum_{i=1}^{n} (EK_i - EF_{SBi})^2}. \quad (5)$$

Эффективными признаются средства защиты, которые имеют минимальное значение $E(EK, EF_{SBi})$. Выполнение требований к защите и перекрытию угроз является обязательным. При выборе критериев, выбираются в первую очередь те средства защиты информации в ГИС, которые имеют максимальные значения соответствующих критериев. Если остались невыполненные требования, неперекрытые угрозы, то соответственно у средства защиты информации отсутствуют необходимые для этого функции. Дальнейший выбор происходит только с учетом упущенных моментов.

После определения выбранных средств защиты необходимо решить следующую задачу оптимизации: t^* средства защиты информации в ГИС должны перекрывать все актуальные угрозы, удовлетворять максимальному количеству требований по защите информации и обеспечивать минимальную стоимость СЗИ:

$$\begin{cases} \sum_{i=1}^{t^*} (SB_i C_i + 5 SB_i E_i) \to \min \\ \sum_{i=1}^{t^*} SB_i m_j^i = 1 \\ \sum_{i=1}^{t^*} SB_i l_j^i = 1 \end{cases} \quad (6)$$

Заключение

Предложенная формализованная модель управления защитой информации в ГИС, учитывающая класс защищенности, структуру, виды обрабатываемой информации, актуальные угрозы, требования к СЗИ, позволяет определить эффективные средства защиты информации для реализации технических мер защиты информации, перекрывающие все актуальные угрозы. При этом удовлетворяется максимальное количество требований по защите информации и обеспечивается минимальная стоимость СЗИ. Данная формализованная модель управления защитой информации в ГИС может быть реализована в виде программного комплекса.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ информационных рисков в системах обработки данных на основе «туманных» вычислений / А. А. Финогеев, А. Г. Финогеев, И. С. Нефёдова, Е. А. Финогеев, В. А. Камаев // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 4. – С. 38–46.

2. Бабенко, А. А. Модель профиля угроз информационной безопасности корпоративной информационной системы / А. А. Бабенко, С. С. Козунова // НБИ технологии. – 2018. – Т. 12, № 1. – С. 6–11. – DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.1

3. Бабенко, А. А. Разработка системы управления аномальными событиями информационной безопасности / А. А. Бабенко, С. Ю. Микова, В. С. Оладько // Информационные системы и технологии. – 2017. – № 5 (103). – С. 108–116.

4. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года. – Электрон. текстовые дан. – Режим доступа: https://www.infowatch.ru/report2018_half (дата обращения: 01.12.2018). – Загл. с экрана.

5. Козунова, С. С. Information security model in the segment of corporate information system / С. С. Козунова, А. А. Бабенко // Информационные системы и технологии. – 2017. – № 1 (99). – С. 87–91.

6. Козунова, С. С. Методика инвестирования информационной безопасности организации / С. С. Козунова, А. А. Бабенко // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. – 2017. – Т. 11, № 4. – С. 11–14. – DOI: https://doi.org/10.15688/jvolsu10.2017.4.2.

7. Макарова, Д. Г. Построение системы защиты информации государственной информационной системы с применением международных стандартов / Д. Г. Макарова, А. А. Старикова, У. В. Таратынова // Интерэкспо Гео-Сибирь. – 2017. – Т. 8. – С. 226–230.

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных : (утв. зам. директора ФСТЭК России 14 февраля 2008 г.). – Электрон. текстовые дан. – Режим доступа: https://fstec.ru/component/attachments/download/290 (дата обращения: 06.04.2018). – Загл. с экрана.

9. Методический документ «Меры защиты информации в государственных информационных системах» : утв. ФСТЭК России от 11 февраля 2014 г. – Электрон текстовые дан. – Режим доступа: https://fstec.ru/component/attachments/download/675 (дата обращения: 01.12.2018). – Загл. с экрана.

10. Моделирование сетевых атак злоумышленников в корпоративной информационной системе / В. А. Гнеушев, А. Г. Кравец, С. С. Козунова, А. А. Бабенко // Промышленные АСУ и контроллеры. – 2017. – № 6. – С. 51–60.

11. Нестеровский, И. П. Возможный подход к оценке ущерба от реализации угроз безопасности информации, обрабатываемой в государственных информационных системах / И. П. Нестеровский, Ю. К. Язов // Вопросы кибербезопасности. – 2015. – № 2 (10). – С. 20–25.

12. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11 февраля 2013 г. № 17 : (ред. от 15.02.2017). – Электрон. текстовые дан. – Режим доступа: http://fstec.ru/component/attachments/download/567 (дата обращения: 03.04.2018). – Загл. с экрана.

13. Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования : Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31 августа 2010 г. – Электрон. текстовые дан. – Режим доступа: http://fstec.ru/component/attachments/download/283 (дата обращения: 03.04.2018). – Загл. с экрана.

14. Осовецкий, Л. Г. Меры по обеспечению безопасности и защиты информации для сложных информационных систем / Л. Г. Осовецкий, А. В. Суханов, В. В. Ефимов // Системы управления, связи и безопасности. – 2017. – № 1. – С. 16–25.

15. Романова, Е. В. Обеспечение качества данных в государственных информационных системах / Е. В. Романова // Прикладная информатика. – 2017. – 6 (72). – С. 15–23.

16. Старикова, А. А. Оценка эффективности управления системой защиты информации в государственных информационных системах / А. А. Старикова, Д. Г. Макарова // Интерэкспо Гео-Сибирь. – 2017. – Т. 8. – С. 188–192.

17. Шилов, А. К. Безопасность информации в государственных информационных системах / А. К. Шилов, В. И. Мищенко // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 12–2. – С. 189–191.

REFERENCES

1. Finogeev A.A., Finogeev A.G., Nefedova I.S., Finogeev E.A., Kamaev V.A. Analiz informatsionnykh riskov v sistemakh obrabotki dannykh na osnove «tumannykh» vychisleniy [Analysis of Information Risks in the System of Distributed Monitoring Based on the Fog Computing Model]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seria. Upravlenie, vychislitelnaya tekhnika i informatika* [Bulletin of the Astrakhan State Technical University. Series: Management, Computer Facilities and Informatics], 2015, no. 4, pp. 38-46.

2. Babenko A.A., Kozunova S.S. Model profilya ugroz informatsionnoy bezopasnosti korporativnoy informatsionnoy sistemy [The Profile Model of Information Security Threats to Corporate Information System]. *NBI tekhnologii* [NBI Technology], 2018, no. 12 (1), pp. 6-11. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.1

3. Babenko A.A., Mikova S.Yu., Oladko V.S. Razrabotka sistemy upravleniya anomalnymi sobytiyami informatsionnoy bezopasnosti [Development of Information Security's Abnormal Events Control System. Information Systems and Technologies]. *Informatsionnye sistemy i tekhnologii*, 2017, no. 5, pp. 108-116.

4. *Globalnoe issledovanie utechek konfidentsialnoy informatsii v I polugodii 2018 goda* [Global Study of Confidential Information Leaks in the First Half of 2018]. URL: https://www.infowatch.ru/report2018_half (accessed 1 December 2018).

5. Kozunova S.S., Babenko A.A. Information Security Model in the Segment of Corporate Information System. *Informatsionnye sistemy i tekhnologii*, 2017, no. 1, pp. 87-91.

6. Kozunova S.S., Babenko A.A. Metodika investirovaniya informatsionnoy bezopasnosti organizatsii [The Methods of Investing in Information

Security Organization]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10, Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Innovations], 2017, vol. 11, no. 4, pp. 11-14. DOI: https://doi.org/10.15688/jvolsu10.2017.4.2.

7. Makarova D.G., Starikova A.A., Taratynova U.V. Postroenie sistemy zashchity informatsii gosudarstvennoy informatsionnoy sistemy s primeneniem mezhdunarodnykh standartov [Construction of the Information Protection System of the State Information System with the Use of International Standards]. *Interekspo Geo-Sibir*, 2017, vol. 8, pp. 226-230.

8. *Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh: (utv. zam. direktora FSTEK Rossii 14 fevralya 2008 g.)* [The Methods of Detecting Pressing Threats to Personal Data Security during Their Processing in the Information Systems of Personal Data]. URL: https://fstec.ru/component/attachments/download/290 (accessed 6 April 2018).

9. *Metodicheskiy dokument «Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh»: utv. FSTEK Rossii ot 11 fevralya 2014 g.* [The Methodical Document 'Measures of Data Protection in State Information Systems': Approved by the Federal Service of Technical and Export Control of Russia on 11 February 2014]. URL: https://fstec.ru/component/attachments/download/675 (accessed 1 December 2018).

10. Gneushev V.A., Kravets A.G., Kozunova S.S., Babenko A.A. Modelirovanie setevykh atak zloumyshlennikov v korporativnoy informatsionnoy sisteme [Modeling Network Attacks in the Corporate Information System]. *Promyshlennye ASU i kontrollery*, 2017, no. 6, pp. 51-60.

11. Nesterovskiy I.P., Yazov Yu.K. Vozmozhnyy podkhod k otsenke ushcherba ot realizatsii ugroz bezopasnosti informatsii, obrabatyvaemoy v gosudarstvennykh informatsionnykh sistemakh [A Possible Approach to the Assessment of Damage Caused by Threats to the Security of Information Processed in State Information Systems]. *Voprosy kiberbezopasnosti*, 2015, no. 2 (10), pp. 20-25.

12. *Ob utverzhdenii Trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh: Prikaz FSTEK Rossii ot 11 fevralya 2013 g. № 17: (red. ot 15.02.2017)* [On Approval of Requirements to the Protection of Information Not Classified as State Secret and Contained in State Information Systems: Order of the Federal Service of Technical and Export Control of Russia of February 11, 2013 No. 17 (ed. of February 15, 2017)]. URL: http://fstec.ru/component/attachments/download/567 (accessed 3 April 2018).

13. *Ob utverzhdenii Trebovaniy o zashchite informatsii, soderzhashcheysya v informatsionnykh sistemakh obshchego polzovaniya: Prikaz FSB RF № 416, FSTEK RF № 489 ot 31 avgusta 2010 g.* [On the Approval of Requirements to the Protection of Information Contained in Public Information Systems: Order of the Federal Security Service of the Russian Federation No. 416, the Federal Service for Technical and Export Control No. 489 of August 31, 2010]. URL: http://fstec.ru/component/attachments/download/283 (accessed 3 April 2018).

14. Osovetskiy L.G., Sukhanov A.V., Efimov V.V. Mery po obespecheniyu bezopasnosti i zashchity informatsii dlya slozhnykh informatsionnykh sistem [Information Security and Protection Measures for Complex Information Systems]. *Sistemy upravleniya, svyazi i bezopasnosti*, 2017, no. 1, pp. 16-25.

15. Romanova E.V. Obespechenie kachestva dannykh v gosudarstvennykh informatsionnykh sistemakh [Data Quality Assurance in State Information Systems]. *Prikladnaya informatika*, 2017, no. 6 (72), pp. 15-23.

16. Starikova A.A., Makarova D.G. Otsenka effektivnosti upravleniya sistemoy zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh [Evaluation of the Effectiveness of Information Security System Management in State Information Systems]. *Interekspo Geo-Sibir*, 2017, vol. 8, pp. 188-192.

17. Shilov A.K., Mishchenko V.I. Bezopasnost informatsii v gosudarstvennykh informatsionnykh sistemakh [Information Security in State Information Systems]. *Mezhdunarodnyy zhurnal prikladnykh i fundamentalnykh issledovaniy*, 2014, no. 12-2, pp. 189-191.

THE MODEL OF INFORMATION SECURITY CONTROL IN STATE INFORMATION SYSTEMS

Aleksey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor of Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Svetlana S. Kozunova

Postgraduate Student, Department of Computer-Aided Design and Search Design,
Volgograd State Technical University
cad@vstu.ru
Prosp. Lenina, 28, 400005 Volgograd, Russian Federation

Abstract. The control of information protection in state information systems is relevant due to the requirements of the legislation of the Russian Federation, to the value of the information processed in them, to its increasing role in the formation of the modern information society in the Russian Federation, as well as the increasing need for procedures for combining information flows of organizations and enterprises. The article deals with the issues related to the control of information security in state information systems. The analysis of works on this subject reveals a solution to particular problems. Therefore, an integrated formalized approach to solving the problem of protecting information in state information systems, taking into account their specifics, threats and requirements of regulators, is relevant. The information leaks, leakage channels in such systems, as well as threats to information security breaches in state information systems have been analyzed. The most likely threats are cyber-attacks, natural disasters, structural failures and human errors. A formalized model for managing information security in state information systems has been developed, which defines an effective set of protection tools in accordance with the requirements of technical protection measures that can be used to automate the process of monitoring. The formal model aimed at solving the problem of optimizing the used protection mechanisms in relation to the overlapping threats has been proposed. The prospects for the development of this study have been determined.

Key words: state information system, control system, information security, means of protection, optimization methods, matrix of binary relations, information security system, information technologies.