www.volsu.ru

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.2.1

УДК 004.942
ББК 32.971.35

РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ СОСТАВОМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Алексей Александрович Бабенко

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

Аннотация. Рассмотрена проблема управления составом системы технической защиты информации в государственных информационных системах. Проанализированы угрозы безопасности информации в государственных информационных системах. Определены критерии оценки технических средств защиты информации в государственных информационных системах. Разработана формальная модель управления составом системы технической защиты информации в государственных информационных системах.

Ключевые слова: государственная информационная система, информационная безопасность, технические средства защиты, система управления, система защиты информации.

Введение

Актуальность проблемы обеспечения информационной безопасности (ИБ) информации в государственных информационных системах (ГИС) обоснована высоким спросом на системы такого класса. Эффективность ГИС в значительной степени зависит от уровня ее безопасности. Защита информации в ГИС обусловлена требованиями Федерального закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [6; 9; 11].

В [8] отмечается роль ГИС – «для устойчивого функционирования информационной

инфраструктуры Российской Федерации устанавливается необходимость обеспечения единства государственного регулирования, централизованные мониторинг и управление функционированием информационной инфраструктуры РФ на уровне информационных систем и центров обработки данных».

Исходя из этого, сформулируем цель данного исследования: формализация процесса управления составом системы технической защиты информации в государственных информационных системах.

Анализ угроз безопасности информации в государственных информационных системах

Особенностями ГИС, влияющих на защищенность информации являются:

– сложный состав программно-аппаратных платформ и систем защиты информации (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 жизненного цикла.

По статистическим данным компании Infowatch статистике в I кв. 2017 года больше половины всех атак было направлено на автоматизированные рабочие места (АРМ) (табл. 1), внутренний нарушитель является наиболее частой причиной утечек информации – 64,5 %, на внешние атаки приходится 35,5 % [1].

Наиболее ценной информацией для злоумышленников являются персональные данные (ПДн) и платежная информация. Наиболее вероятными каналами утечки этих видов информации являются сеть и бумажные документы.

Отметим, что наряду с традиционными угрозами нарушения конфиденциальности, целостности и доступности для информации, обрабатываемой 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 для ГИС наносят угрозы нарушения целостности и угрозы, присущие центрам обработки данных (ЦОД), серверам и баз данных [3; 7]. Среднему ущербу могут подвергнуть угрозы получения НСД к информации в ГИС, АРМ пользователей или файловому серверу [4]. Анализ угроз информации в ГИС позволяет соотнести угрозы нарушения ИБ с техническими мерами и средствами ее предотвращения [5; 6; 9].

Таблица 1

Угрозы АРМ ГИС

Угроза	Техника воздействия
Подбор паролей	Попытки подбора аутентификационной информации для доступа к сервисам и ресурсам контролируемых организаций – RDP, SSH, SMB, DB, Web
Нарушение политик ИБ	Нарушение пользователями/администраторами контролируемых ресурсов требований политик ИБ в части использования устаревших версий или недоверенного ПО, которое может быть использовано злоумышленником для атаки путем эксплуатации уязвимости. Также использование ресурсов компании для получения собственной выгоды (майнинг bitcoin/ethereum). Использование торрент-трекеров
Вредоносное ПО	Заражение конечной системы, распространение вируса по локальной сети, отключение/блокировка служб, препятствующих распространению вируса, попытки проведения иных атак внутри сети для получения критичной информации и передачи на командные серверы
Попытки эксплуатации уязвимостей	Использование недостатков в системе для нарушения контроля целостности данных и воздействие на правильную работу системы. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ошибки конфигурации, отсутствия обновлений. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты

Определение критериев оценки технических средств защиты информации в государственных информационных системах

Состав мер защиты информации в ГИС представлен в [6; 9]. Если организация подключена к ГИС, то [9] обязывает аттестовать систему, а для защиты информации должны применяться только сертифицированные средства защиты информации, имеющие действующие сертификаты ФСТЭК или ФСБ. Государственный реестр сертифицированных СЗИ и перечень СЗИ, сертифицированных ФСБ России представлен в [10], а перечень ФСТЭК в [2].

Мера защиты информации считается выполненной, если:

1. В организационно-распорядительных документах по обеспечению безопасности информации определена процедура установки средств безопасности в ГИС.

2. Принятые организационные и технические меры, а также используемые СЗИ исключают несанкционированную установку, использование неразрешенных средств или их компонент.

3. В ГИС отсутствуют запрещенные к использованию программные и технические средства или их компоненты, целостность установленного СЗИ не нарушена.

4. Обеспечивается периодический контроль установленного в ГИС средства защиты на предмет его соответствия перечню, разрешенных к установке средств защиты в ГИС.

Для СЗИ, применяемых в ГИС, регулятор предъявляет требования. Так в ГОСТ Р ИСО / МЭК 15408 определяется профиль защиты (ПЗ) – совокупность требований безопасности в отношении определенной категории изделий ИТ, независящую от реализации.

Для ГИС, обрабатывающих информацию, не содержащую сведения, отнесенные к ГТ, актуальным ПЗ является четвертый класс.

В результате анализа технических СЗИ в ГИС установлены классы используемых СЗИ: межсетевые экраны (МЭ), средства обнаружения вторжений (СОВ), средства антивирусной защиты информации (САВЗ), средства доверенной загрузки (СДЗ), средств контроля съемных носителей (СКН). Эти классы были проанализированы по следующей схеме: 1) выявление нормативно-правовых актов, содержащих требования к классу СЗИ; 2) определение класса СЗИ, типа и области его применения; 3) определение соответствия классов защищенности ГИС и классов защиты СЗИ; 4) определение соответствия СЗИ с типом и классом защиты ГИС. Данная процедура является универсальной и может быть использована для выбора не только технических средств защиты информации, но и программных и применятся для всех классов информационных систем.

Учитывая требования нормативно-правовых актов, сформулируем критерии оценки для анализа технических средств защиты информации в ГИС (табл. 2).

Таблица 2

Критерии оценки для анализа технических СЗИ в ГИС

Обозначение	Название
K_1	Срок действия сертификата ФСТЭК/ФСБ
K_2	Многофункциональность, выполнение СЗИ нескольким требованиям, например к САВЗ и МЭ
K_3	Уровень контроля на отсутствие НДВ в ПО СЗИ
K_4	Стоимость СЗИ

Перечисленные критерии будут использоваться для определения наиболее эффективных СЗИ ГИС.

Формальная модель управления составом системы технической защиты информации в государственных информационных системах

Под управлением составом системы технической защиты информации в ГИС будем понимать оценку эффективности средств защиты информации в ГИС и выбор наиболее эффективных СЗИ для защиты информации в ГИС.

Формализовано процедуру оценки эффективности средств защиты информации в ГИС можно представить вектором критериев.

$$K = (K_1, K_2, K_3, K_4), \qquad (1)$$

K_1 – срок действия сертификата ФСТЭК/ФСБ:

$$K_1 = \begin{cases} 0, \text{заканчивается в 2019} \\ 0{,}5 \text{ заканчивается в 2020} \\ 1, \text{заканчивается в 2021} - 2023 \end{cases} \quad (2)$$

K_2 – многофункциональность – выполнение средством защиты нескольких функций защиты (например, программный комплекс Электронный замок «Витязь» версия 2.2, на соответствие требованиям СДЗ (ИТ.СДЗ.УБ2.ПЗ) и САВЗ (ИТ.САВЗ.Г2.ПЗ)).

$$K_2 = \begin{cases} 0 - \text{нет} \\ 1 - \text{да} \end{cases} \quad (3)$$

K_3 – соответствие заявленного в программном обеспечении средства защиты информации уровня контроля на отсутствие недекларированных возможностей (НДВ):

$$K_3 = \begin{cases} 0 - \text{нет} \\ 1 - \text{да} \end{cases} \quad (4)$$

K_4 – стоимость СЗИ ГИС;

$$K_4 = \begin{cases} 0, \text{высокая}, \mathrm{C}_i > \mathrm{C}_{\text{ср}} \\ 1, \text{низкая}, \mathrm{C}_i < \mathrm{C}_{\text{ср}} \end{cases} \quad (5)$$

где C_i – стоимость *i*-го СЗИ ГИС, $\mathrm{C}_{\text{ср}}$ – среднее значение стоимости в группе СЗИ ГИС, *n* – количество в группе СЗИ ГИС.

$$\mathrm{C}_{\text{ср}} = \frac{\sum_{i=1}^{n} \mathrm{C}_i}{n} \quad (6)$$

Идеальному СЗ соответствует вектор K^*, в котором все значения критериев равны единице. Для оценки эффективности СЗИ вводится скалярная величина, равная Евклидову расстоянию между наилучшим вектором и вектором критериев, полученным для *i*-го оцениваемого СЗИ:

$$K^i = \left(K_1^i, K_2^i, K_3^i, K_4^i\right) \quad (7)$$

Евклидово расстояние для *i*-ой группы СЗИ ГИС рассчитывается по формуле:

$$E^i = \sqrt{\sum_{j=1}^{4} \left(K_j^* - K_j^i\right)^2} \quad (8)$$

СЗИ, для которой расстояние до наилучшего вектора окажется наименьшим, можно считать наиболее эффективным для защиты информации в ГИС.

Предложенная формальная модель позволяет принимать управляющие решения по выбору наиболее эффективных СЗИ в ГИС.

Результаты экспериментальных исследований

В результате проведенных экспериментов были установлены эффективные технические средства для защиты информации в ГИС:

1. МЭ «Универсальный шлюз безопасности “UserGate UTM”», выполняющий требования к МЭ ИТ.МЭ.А4.ПЗ, ИТ.МЭ.Б4.ПЗ и требования к СОВ ИТ.СОВ.С4.ПЗ.

2. Маршрутизаторы ESR-1000, ESR-200, ESR-100, выполняющие требования к МЭ ИТ.МЭ.А5.ПЗ.

3. МЭ Huawei Eudemon (модель Eudemon 8000E-X3) версии V500, маршрутизаторы серии Huawei AR (модели: AR2220E, AR2240, AR161FG-L) версии V200, МЭ серии Cisco ASA 5500-X (модели: ASA 5506-X, ASA 5508-X, ASA 5516-X) с установленным ПО Cisco ASA версии 9.x, выполняющие требования к МЭ ИТ.МЭ.А6.ПЗ и ИТ.МЭ.Б6.ПЗ.

4. ПАК «Горизонт-ВС», выполняющий требования к ИТ.СДЗ.ПР4.ПЗ.

Перечисленные технические СЗИ рекомендуются для защиты информации в ГИС, не обрабатывающих сведения, отнесенные к государственной тайне, содержащих в своем составе ИСПДн и имеющие подключения к сетям общего пользования 2 класса.

Заключение

Разработанная модель управления составом технических средств защиты информации в государственных информационных системах, позволяет определить наиболее эффективный состав системы защиты информации в ГИС. Если изменятся требования к анализируемым средствам защиты информации, то изменив значения в оптимальном векторе K^*, можно прийти к верному решению. Следовательно, разработанная модель управления составом технических средств защиты информации в ГИС является универсальной и эффективной.

СПИСОК ЛИТЕРАТУРЫ

1. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года. – Электрон. текстовые дан. – Режим доступа: https://www.infowatch.ru/report2018_half (дата обращения: 05.03.2019). – Загл. с экрана.

2. Государственный реестр сертифицированных средств защиты информации. – Электрон. текстовые дан. – Режим доступа: https://fstec.ru/tekhnicheskaya-zaschita-informatsii/dokumenty-po-sertifickatsii/153-sistemasertifikatsii/591 (дата обращения: 05.03.2019). – Загл. с экрана.

3. Козунова, С. С. Автоматизация управления инвестициями в информационную безопасность предприятия / С. С. Козунова, А. А. Бабенко // Вестник компьютерных и информационных технологий. – 2015. – № 3 (127). – С. 38–44.

4. Козунова, С. С. Система оптимизации рисков инвестирования информационной безопасности промышленных предприятий / С. С. Козунова, А. А. Бабенко // Вестник компьютерных и информационных технологий. – 2016. – № 7 (145). – С. 22–29.

5. 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: 05.03.2019). – Загл. с экрана.

6. 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: 05.03.2019). – Загл. с экрана.

7. 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.

8. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

9. 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: 05.03.2019). – Загл. с экрана.

10. Перечень средств защиты информации, сертифицированных ФСБ России. – Электрон. текстовые дан. – Режим доступа: http://clsz.fsb.ru/certification.htm (дата обращения: 05.03.2019). – Загл. с экрана.

11. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2017. – № 31 (Ч. I). – Ст. 4736.

REFERENCES

1. *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 5 March 2019).

2. *Gosudarstvennyy reestr sertifitsirovannykh sredstv zashchity informatsii* [State Register of Certified Means of Information Protection]. URL: https://fstec.ru/tekhnicheskaya-zaschita-informatsii/dokumenty-po-sertifickatsii/153-sistemasertifikatsii/591 (accessed 5 March 2019).

3. Kozunova S.S., Babenko A.A. Avtomatizatsiya upravleniya investitsiyami v informatsionnuyu bezopasnost predpriyatiya [Automation of Investment Management in Enterprise Information Security]. *Vestnik kompyuternykh i informatsionnykh tekhnologiy* [Herald of Computer and Information Technologies], 2015, no. 3 (127), pp. 38-44.

4. Kozunova S.S., Babenko A.A. Sistema optimizatsii riskov investirovaniya informatsionnoy bezopasnosti promyshlennykh predpriyatiy [The System of Optimizing Risks of Investing Information Security of Industrial Enterprises]. *Vestnik kompyuternykh i informatsionnykh tekhnologiy* [Herald of Computer and Information Technologies], 2016, no. 7 (145), pp. 22-29.

5. *Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh : utv. zam. direktora FSTEK Rossii 14 fevralya 2008 g.)* [Methods of Detecting Pressing Threats to Personal Data Security During Their Processing in the Information Systems of Personal Data. Approved by the Deputy Director of the Federal Service for Technical and Export Control of the Russian Federation on February 14, 2008]. URL: https://fstec.ru/component/attachments/download/290 (accessed 5 March 2019).

6. *Metodicheskiy dokument «Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh» : utv. FSTEK Rossii ot 11 fevralya 2014 g.* [Methodical Document “Measures of Data Protection in State Information Systems”. Approved by the Federal Service of Technical and Export Control of the

Russian Federation on February 11, 2014]. URL: https://fstec.ru/component/attachments/download/675 (accessed 5 March 2019).

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

8. *O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody : Ukaz prezidenta RF ot 09.05.2017 № 203* [On the Strategy of Information Society Development in the Russian Federation for 2017–2030. Decree of the President of the Russian Federation from of May 9, 2017 no. 203]. *Sobranie zakonodatelstva RF*, 2017, no. 20, art. 2901.

9. *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 the Statement of Requirements for Protecting Information Which is not the State Secret Containing in State Information Systems. Order of the Federal Service for Technical and Export Control of the Russian Federation of February 11, 2013 no. 17 (amended 15 February 2017)]. URL: http://fstec.ru/component/attachments/download/567 (accessed 5 March 2019).

10. *Perechen sredstv zashchity informatsii, sertifitsirovannykh FSB Rossii* [List of Information Security Tools Certified by the Federal Security Service of the Russian Federation]. URL: http://clsz.fsb.ru/certification.htm (accessed 5 March 2019).

11. Federalnyy zakon ot 26.07.2017 g. № 187-FZ «О bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Federal Law of July 26, 2017 no. 187-FZ "On Security of Critical Information Infrastructure of the Russian Federation]. *Sobranie zakonodatelstva RF*, 2017, no. 31 (Part 1), art. 4736.

DEVELOPING A MODEL FOR MANAGING THE STRUCTURE OF INFORMATION PROTECTION TECHNICAL MEANS IN STATE INFORMATION SYSTEMS

Alexei A. Babenko

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

Abstract. The urgency of the issue of information security in state information systems is justified by the high demand for systems of this class. The effectiveness of public information systems largely depends on the level of their security. Based on this, we formulate the purpose of this study: formalization of the process of managing the composition of the system of information technical protection in state information systems.

The paper deals with the problem of managing the composition of the system of information technical protection in state information systems. The author analyzes threats to information security in state information systems. The article defines the criteria of evaluating technical means of information protection in state information systems. The researcher develops a formal model of managing the structure of information technical protection system in state information systems.

The developed model of managing the structure of information protection technical means in state information systems allows to determine the most effective structure of the information protection system in state information systems. If the requirements for the analyzed means of information security change, then changing the values in the optimal vector, you can come to the right decision. Consequently, the developed model of managing the structure of information protection technical means in state information systems is universal and effective.

Key words: state information system, information security, technical protection means, management system, information protection system.