УДК: 004.03004.62+004.04

ОБЕСПЕЧЕНИЕ ПРОАКТИВНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Бурый А.С., д-р техн. наук, Российский институт стандартизации, г. Москва
Исаенко И.В., аспирант, Российский институт стандартизации, г. Москва

В условиях активного развития информационно-коммуникационных технологий (ИКТ) в технико-экономической и социальной среде вопросы защиты информации и данных приобретают все большую актуальность. Разработчики программных продуктов должны понимать, что уязвимость их продукции к несанкционированному доступу можно значительно сократить уже на этапе проектирования, т.е. в проактивной фазе.

Целью исследования является развитие идеи проактивного подхода к обеспечению безопасности ИКТ с учетом их функциональных, архитектурно-технологических особенностей на начальных этапах жизненного цикла.

Задача решается на основании системного анализа, концептуально-логического агентного моделирования и категорийно-алгебраического представления исследуемой предметной области. На основе анализа информационных факторов, характерных для различных этапов жизненного цикла программной продукции, показаны пути реализации свойства проактивной безопасности при разработке, проектировании и испытаниях программных продуктов.

Ключевые слова: безопасность информации, безопасность информационно-коммуникационных технологий, кибербезопасность, проактивная безопасность, жизненный цикл, большие данные.

Цитирование: Бурый А.С., Исаенко И.В. Обеспечение проактивной безопасности информационно-коммуникационных технологий // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 5(80). С. 73–78.

ВВЕДЕНИЕ

Безопасность информационно-коммуникационных технологий остается актуальной и сложной проблемой в современном мире. Специалисты по кибербезопасности должны постоянно развивать и совершенствовать свои навыки, а организации – инвестировать в современные технологии и методы защиты, чтобы эффективно противостоять киберугрозам и обеспечить надежную защиту своих данных и ресурсов.

Следует различать безопасность информационно-коммуникационных технологий (БИКТ) и информационную безопасность. БИКТ обеспечивает безопасность получаемой на базе данной технологии информации, а также безопасность информационной системы, в которой она реализована. Информационная безопасность (ИБ) больше приближена непосредственно к объектам защиты, основная цель ИБ – обеспечение конфиденциальности, доступности и целостности информации[1].

Все чаще аналитики сталкиваются с рисками в области ИБ одновременно и на технологическом, и на организационном уровне [1]. В большинстве случаев в утечках информации виноваты сами сотрудники компаний, воздействие на которых ведется по хорошо спланированному сценарию под управлением искусственного интеллекта, что требует внедрения усовершенствованных механизмов защиты[2]. Ландшафт кибервоздействий постоянно расширяется, что обусловлено:

1) развитием сервисов облачных услуг;
2) использованием сетевых приложений (сетевых редакторов, программных платформ для проведения моделирования и расчетов);
3) удаленной работой и взаимодействием с клиентами и сотрудниками через Интернет. В результате во внутренней информационной сети компании формируются «слепые зоны» и возникает необходимость устранения большого количества потенциальных (скрытых) уязвимостей.

[1] ГОСТ ISO/IEC 17788–2016. Информационные технологии. Облачные вычисления. Общие положения и терминология (Дата введ. 2017-11-01); п. 3.1.3. qwertyuiop[asdfghjkl;'zxcvbnm,./

[2] 2024: Аналитики Gartner назвали 3 главных тренда в сфере кибербезопасности в 2024 году // TAdviser [сайт]. – URL: https://www.tadviser.ru (дата обращения: 05.08.2024).

Анализ за 2022 г. показал, что по объему атак на первом месте информационные ресурсы госсектора – 14%, далее идут медицинские учреждения – 11%, потом промышленность и ИТ-компании – по 8% [2]. Применяемые сегодня многими компаниями системы управления событиями безопасности (Security Information and Event Management – SEIM) и системы обнаружения вредоносной активности (Endpoint Detection and Response – EDR) практически не справляются с участившимися кибератаками. Если большинство информационно-коммуникационных систем специального назначения [3, 4] на предыдущем этапе развития в основном использовали выделенные каналы связи, то сегодня, например, околоземная спутниковая система становится неотъемлемой частью глобальной информационной системы [4], включая вопросы обработки и хранения всё новых объемов данных. Последние уже представляются как «большие данные» или Big Data (BD) [5], а объем инструментов BD по итогам 2023 г. оценивался в $220,2 млрд[3], причем все чаще кибербезопасность и оперативность выявления мошенничества связывают с анализом BD.

Обеспечение БИКТ на основе BD видится в возможности реализации моделей поведения злоумышленников, построения сценариев предупреждения нарушений безопасности и алгоритмов повышения уровней защищенности [6]. При этом высокий уровень обновления программного обеспечения также обеспечивается совершенствованием систем обнаружения вредоносных программ на основе методов интеллектуального анализа данных [7].

Целью исследования является развитие идеи проактивного подхода к обеспечению безопасности информационно-коммуникационных систем и комплексов с учетом их функциональных, архитектурно-технологических особенностей на всех этапах жизненного цикла.

СУЩНОСТЬ КОНЦЕПЦИИ ИССЛЕДОВАНИЯ

Применительно к вычислительным комплексам и системам (ВК) проактивная безопасность (ПБ) основывается на решаемых функциональных задачах, инфраструктуре и реализуемых технологиях, характеристиках внешней среды, а также этапах жизненного цикла (ЖЦ), предшествующих этапу эксплуатации (применению по назначению). Таким образом, это структурное свойство ВК, обеспечивающее его функциональность (работоспособность), даже если некоторые из компонентов ВК становятся в силу ряда причин «неработоспособными» [8].

Свойство ПБ позволяет на этапе эксплуатации ВК (в том числе и ВК в составе систем управления сложных объектов – систем проектирования, технологического управления и др.) не выделять ресурсы на внедрение дополнительных механизмов (ресурсов) для своей поддержки.

[3] 2023: Объем глобального рынка инструментов Big Data оценен в 220,2 млрд. (Там же).

На рис. 1 условно показаны основные этапы ЖЦ ВК: проектирование, обоснование состава, реализация, испытания, ввод в действие и эксплуатация, сопровождение. Для каждого этапа выделены два способа управления по достигнутому результату:

1) по результатам процесса эксплуатации (целевого применения) изделия;

2) по факту полученных результатов (отчетов) от следующего относительно текущего этапа ЖЦ.

Первые ориентированы на возможные доработки при модификации продукции, улучшение характеристик, повышение качества. Вторые используются для оперативного управления, например в ходе эксплуатации по результатам проводимого периодического обслуживания в установленные сроки, в том числе и неплановые. Кроме того, оперативное управление широко используется и на этапах проектирования, изготовления опытного образца и т. д.

Известно, что устранение ошибок на этапе проектирования, отладки программных продуктов во многом определяет количество программных сбоев и вычислительных ошибок, возможных в процессе применения [9].

Таким образом, безопасность ИКТ во многом обеспечивается до изготовления окончательной версии программного продукта, т.е. по результатам автономных и комплексных испытаний, проводимых на ВК [8]. В отличие от БИКТ ПБ

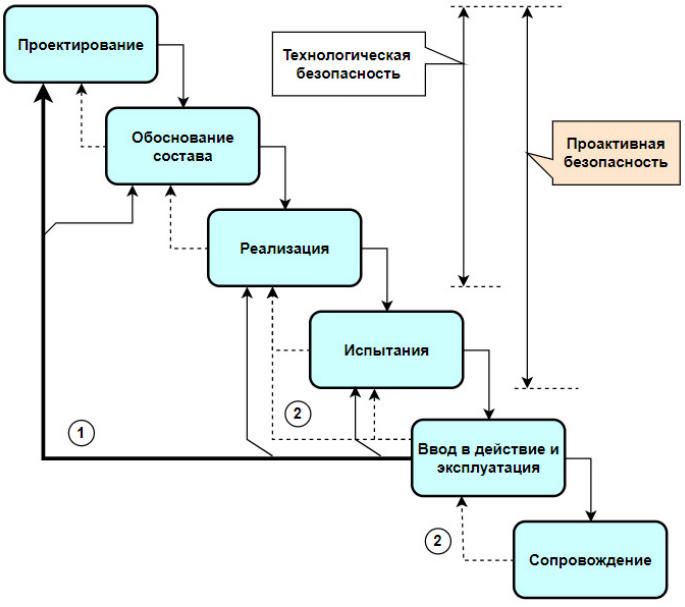

Рис. 1. Взаимосвязь технологической и проактивной безопасности с жизненным циклом ВК

включает в себя все возможные фазы (виды) испытаний, т.е. все до ввода изделий в эксплуатацию, после чего следует

говорить о реактивной безопасности объекта (изделия), когда качество уровня безопасности будет актуализировано уровнем реальных и потенциальных угроз по месту эксплуатации программного продукта или ВК.

Представим информационное взаимодействие при разработке программной продукции в ходе ее жизненного цикла с целью обеспечения свойства ПБ в виде многоагентной системы [10]. Будем считать, что агент характеризуется гибридной архитектурой, для которой свойственны, как делиберативная (обдумывающая решения) символьная модель мира (внешней среды) для принятия глобальных решений, так и реактивное реагирование на происходящие в системе события. В качестве агентов выступают, как некоторые технологии, процессы переработки информации и коммуникационные действия, обеспечивающие формирование, представление, транспортирование информационных блоков (данных), сопровождающие решение функциональных задач в ходе проектирования сложных объектов на примере разработки программных продуктов.

Для начального этапа (концептуального проектирования) целесообразно представить модельную среду в виде многоагентной системы (MAS), как совокупность множеств вида (1):

$$MAS = (A, E, R, \Xi), \quad (1)$$

где $A = \{a_1, a_2, ..., a_i, ..., a_n\}$ – множество всех агентов, а каждый агент a_i $(i = \overline{1,n})$ есть кортеж вида

$$a_i = \langle s_i,\ v_i,\ d_i\ , \varphi_i \rangle, \quad (2)$$

объединяющий соответственно элементы множества состояний среды (E), множества функций восприятий (R), множества действий $d_k \in D$, $k = \overline{1, |D|}$ и множества базовых организационных структур – Ξ. Элементы Ξ представим в виде отображения

$$\varphi_j : s_j \times v_j \rightarrow s_j \times d_j\ . \quad (3)$$

Здесь $\varphi_j \in \Xi$, $j = \overline{1, |\Xi|}$, модуль от множества обозначает мощность или число элементов множества Ξ. Функция восприятия среды в общем случае есть отображение вида

$$R : E \rightarrow (v_1 \times \cdots \times v_m).$$

Множество базовых организационных структур (Ξ) соответствует конкретным функциям агентов и взаимоотношениям между ними. Агент рассчитывает состояние, в котором он находится, исходя из своего восприятия ситуации, что соответствует реакции процессов проектирования (этапов ЖЦ) на окружающие изменения (например, результаты тестирования, обновления базы инцидентов [3], завершение разработки необходимой технологии, завершение производственного процесса изготовления определенного продукта и др.). Это отражается в переходе между элементами множества Ξ.

Тогда имеет смысл представлять связи типа 2 (см. рис. 1) как взаимодействие соответствующих агентов на этапах ЖЦ, например:

$$a_{i+1} \rightarrow a_i\ . \quad (4)$$

Цель данного взаимодействия – возможная доработка проектируемого образца, пополнение базы данных и т. д.

Отношения вида (4) могут образовывать семейства отношений, характерные для типов агентов, а цепочки из отношений вида (4) позволяют сформировать сценарии управления взаимодействием агентов в ходе реализации заданной технологии (проектирования, контроля и др.). Они отражают коммуникации между агентами и могут характеризоваться объемом переданных данных, количеством проведенных сеансов связи и другими параметрами.

Для этапа целевого использования могут регистрироваться факты выявленных угроз, кратность появления угрозы, ее новизна и ряд других, увеличивая число взаимодействующих агентов из числа взаимодействующих подсистем, отвечающих за базы данных, информационно-расчетного блока, реализующего, например, библиотеку алгоритмов интеллектуального анализа данных и др.

МЕСТО ПОНЯТИЙНОГО АНАЛИЗА

Анализ динамики агентного взаимодействия и уточнение решаемых задач в ходе концептуального моделирования, представленного выше на рис. 1, определяется существом предмета исследования. В качестве последнего может выступать и обеспечение информационной безопасности, БИКТ (см. выше), и кибербезопасность.

В таблице собраны типовые определения для данных понятий.

Задачи обеспечения кибербезопасности могут быть систематизированы как анализ механизмов нарушения защиты киберпространства, моделирование разрушающих воздействий; управление кибербезопасностью, определение зоны устойчивости объекта защиты, анализ киберрисков, разработка стандартов и нормативов безопасности киберпространства; синтез средств защиты киберпространства и контроль текущего состояния и функционирования компонентов киберпространства.

Таким образом, определение безопасности ИКТ очень похоже на определение информационной безопасности. Однако к определению добавляются дополнительные характеристики, которые в данном контексте можно понимать как расширение технологической составляющей

Таблица 1

Сопоставление понятийных объектов в области исследования

№	ПОНЯТИЙНЫЕ ОБЪЕКТЫ	ИСТОЧНИКИ
1	*Кибербезопасность* представляет собой совокупность методов и способов защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных	Д.П. Зегжда и др. [11]
2	*Безопасность информации* – состояние защищенности информации (данных), при котором обеспечивается ее (их) конфиденциальность, доступность и целостность[4]	ГОСТ ISO/IEC 17788–2016; п. 3.1.3
3	*Информационная безопасность* – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки	ГОСТ Р 53113.1-2008; п. 3.10[5]
4	*Безопасность ИКТ* – обеспечение целостности, доступности, конфиденциальности и других требований безопасности, предъявляемых к вычислительной и коммуникационной технике и информации, которую она хранит, обрабатывает и пересылает	Интернет-ресурс[6]

[4] ГОСТ ISO/IEC 17788–2016. Информационные технологии. Облачные вычисления. Общие положения и терминология. (Дата введ. 2017-11-01); п. 3.1.3.

[5] ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. (Дата введ. 2009-10-01); п. 3.10.

[6] Кибербезопасность, ИБ, безопасность ИТ – в чём разница? – URL: https://www.h-x.technology/ru/blog-ru/infosec-itsec-cybersecurity-defference-ru (дата обращения: 05.08.2024).

(применительно к информационной технологии[7]), организационных мер, а также применение алгоритмических процедур в обеспечении именно устойчивости к несанкционированному использованию информационных ресурсов.

Точно так же, как концепция ИБ включает в себя безопасность ИКТ, чтобы защитить саму информацию, независимо от ее текущей формы и/или местоположения, кибербезопасность необходимо рассматривать как расширение информационной безопасности. Кибербезопасность также связана с защитой человека (лиц, организаций), использующих ресурсы в киберпространстве, и с защитой любых других активов, в том числе принадлежащих обществу в целом, которые подверглись риску в результате уязвимостей, связанных с использованием ИКТ. Взаимосвязь между этими тремя пересекающимися понятиями проиллюстрирована на рис. 2 [12]. Объектами защиты для представленных трех областей являются:

1) информационные активы, хранящиеся и передаваемые без использования ИКТ (документы, архивы, объекты в неоцифрованном виде);
2) неинформационные активы, уязвимые угрозам с использованием ИКТ;
3) информационные активы, хранящиеся и передаваемые с использованием ИКТ.

Рис. 2. Взаимоотношения между информационной безопасностью, кибербезопасностью и безопасностью ИКТ

В алгебраической форме категорийное пространство указанных областей представим как

$$Q_3 = Q_1 \cap Q_2 ,$$

причем элементами множества Q_3 являются категории $\{q_l\} \in Q_3$, составляющие суть БИКТ.

[7] Здесь к традиционным функциям сбора, хранения, обработки, передачи и использования данных добавляются задачи обеспечения технологической безопасности.

В качестве категории «программно-алгоритмических средств безопасности» могут выступать процедуры обеспечения защиты данных в базах данных (при пополнении запросов к базе данных). Соответственно обеспечение этого процесса осуществляется при проектировании в рамках требований проактивной безопасности.

В общем случае для БИТК активом (активами), подлежащим защите, является информация вместе с базовыми технологиями. Однако в случае кибербезопасности цель, очевидно, состоит не в том, чтобы обезопасить киберпространство, а скорее в том, чтобы обезопасить тех, кто функционирует в киберпространстве, будь то отдельные лица или организации. Поскольку роль ИКТ в обществе становится все более распространенной, то и роль, человека (человека-оператора) также возрастает, что отчетливо отражается и в вопросах БИКТ. Люди по-прежнему считаются как угрозой, так и уязвимым местом, т.е. они также считаются активом, который нуждается в защите в киберпространстве [12]. В свете вышеизложенного кибербезопасность можно определить как защиту самого киберпространства, электронной информации, ИКТ, поддерживающих киберпространство, и пользователей киберпространства в их личном, общественном и национальном качестве, включая любые их интересы, как материальные, так и нематериальные, которые уязвимы для кибератак.

ЗАКЛЮЧЕНИЕ

Эффективность конкретного сценария взаимодействия агентов позволяет оценить влияние выбранной технологии на произведенный продукт, возможную реакцию рынка и, как следствие, на выполнимость поставленной задачи развития, например, отрасти или производства. Существующий изоморфизм многоагентной среды позволяет производить декомпозицию агента на множество субагентов, а также редуцировать многоагентную среду до одноагентного состояния.

Категорийное представление исследуемой предметной области позволяет точечно управлять процессом проактивной безопасности на этапах разработки и проектирования новых изделий аппаратно-программной продукции.

ЛИТЕРАТУРА / REFERENCES

1. **Об одном подходе к обеспечению безопасности данных в информационной системе средствами ОС и СУБД / Г.П. Акимова, А.Ю. Даниленко, Е.В. Пашкина [и др.] // Информационные технологии и вычислительные системы. 2022. № 1. С. 33–39. https://doi.org/ 10.14357/20718632220104** / Akimova G.P., Danilenko A.Y., Pashkina E.V., et ai. Ob odnom podhode k obespecheniyu bezopasnosti dannyh v informacionnoj sisteme sredstvami OS i SUBD. Journal of information technologies and computing systems. 2022; 1:33–39. (In Russ.).
2. **Кибербезопасность объектов критической инфраструктуры / Г.В. Федотова, Ю.А. Капустина, А.Г. Чураев, З.Ю. Юлдашбаева // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2023. Т. 13, № 4. С. 111–122. https://doi.org/10.21869/2223-1552-2023-13-4-111-122 /** Fedotova G.V., Kapustina Y.A., Churaev A.G., Yuldashbaeva Z.Y. Kiberbezopasnost' ob»ektov kriticheskoj infrastruktury. Proceedings of the Southwest State University. Series: Economy. Sociology. Management. 2023;13(4):111–122. (In Russ.).
3. **Бурый А.С., Усцелемов В.Н. Информационная безопасность автоматизированных систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2023. № 2(72). С. 31–37. /** Buryi A.S., Ustselemov V.N. Informacionnaya bezopasnost' avtomatizirovannyh sistem. Information and Economic Aspects of Standardization and Technical Regulation. 2023;2(72):31–7. (In Russ.).
4. **Статьев В.Ю., Докучаев В.А., Маклачкова В.В. Информационная безопасность на пространстве «Больших данных» // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 4. С. 21–28. https://doi.org/10.36724/2072-8735-2022-16-4-21-28 /** Statev V.Y., Dokuchaev V.A., Maklachkova V.V. Information security in the big data space. T-Comm. 2022;16(4):21–28. (In Russ.).
5. **Бурый А.С., Погодин И.М. Оценка качества больших данных. Часть 1. Основные понятия и метрики // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 3(78). С. 49–58. /** Buryi A.S., Pogodin I.M. Evaluating the quality of big data. Part 1. Basic concepts and metrics. Information and Economic Aspects of Standardization and Technical Regulation. 2024;3(78):49–58. (In Russ.).
6. **Цао Л. Образ мышления в науке о данных: Наступающая научно-техническая и экономическая революция. – СПб.: Изд-во Европейского ун-та в Санкт-Петербурге, 2022. – 552 с. /** Cao L. Data Science Thinking; The Next Scientific, Technological and Economic Revolution. St. Petersburg: Publ. House of the European University; 2022. 552 p. (In Russ.).
7. **Комашинский Д.В., Котенко И.В. Концептуальные основы использования методов Data Mining для обнаружения вредоносного программного обеспечения // Защита информации. Инсайд. 2010. № 2(32). С. 74–82. /** Komashinskij D.V., Kotenko I.V. Konceptual'nye osnovy ispol'zovaniya metodov Data Mining dlya obnaruzheniya vredonosnogo programmnogo obespecheniya. Zaŝita informacii. Inside. 2010;2(32): 4–82. (In Russ.).

8. Казарин О.В., Скиба В.Ю. Парадигма проактивной безопасности компьютерных систем // Защита информации. Инсайд. 2009. № 5(29). С. 68–75. / Kazarin O.V., Skiba V.Y. Paradigma proaktivnoj bezopasnosti komp'yuternyh sistem. Zaŝita informacii. Inside. 2009;5(29):68–75. (In Russ.).
9. **Бурый А.С. Тестирование качества программного обеспечения в процессе его сертификации // Правовая информатика. 2019. № 1. С. 46–55. /** Buryi A.S. Testirovanie kachestva programmnogo obespecheniya v processe ego sertifikacii. Legal informatics. 2019;(1):46–55. (In Russ.).
10. Бурый А.С. Картирование технологий как метод в Форсайт-исследованиях // Транспортное дело России. 2014. № 5. С. 155–157. / Buryi A.S. Kartirovanie tekhnologij kak metod v Forsajt-issledovaniyah. Transport business of Russia. 2014;(5):155–157. (In Russ.).
11. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Д.П. Зегжда, Ю. С. Васильев, М. А. Полтавцева [и др.] // Вопросы кибербезопасности. 2018. № 2(26). С. 2–15. https://doi.org/10.21681/2311-3456-2018-2-2-15 / Zegzhda D.P., Vasilev Y.S., Poltavtseva M.A., et al. Kiberbezopasnost' progressivnyh proizvodstvennyh tekhnologij v epohu cifrovoj transformacii. Cybersecurity issue. 2018;2(26):2–15. (In Russ.).
12. Von Solms, R., van Niekerk, J. From information security to cyber security. Comput. Secur. 2013;38:97–102.

PROACTIVE SECURITY SUPPORT FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Buryi A.S., Doctor of Sciences in Technology, Russian Standardization Institute

Isaenko I.V., graduate student of the Russian Standardization Institute

In the context of the active development of information and communication technologies (ICT) in the techno-economic and social environment, the issues of information and data protection are becoming increasingly relevant. Software developers should understand that the vulnerability of their products to unauthorized access can be significantly reduced already at the design stage, i.e. in the proactive phase.

The purpose of the study is to develop the idea of a proactive approach to ensuring the security of ICTs, taking into account their functional, architectural and technological features at the initial stages of the life cycle.

The problem is solved on the basis of system analysis, conceptual-logical agent modeling and categorical-algebraic representation of the subject area under study. Based on the analysis of information factors characteristic of various stages of the life cycle of software products, the ways of realizing the property of proactive safety in the development, design and testing of software products are shown.

Keywords: information security, information and communication technology security, cybersecurity, proactive security, lifecycle, Big Data.

For citation: Buryi A.S., Isaenko I.V. Proactive Security Support for Information and Communication Technologies. Information and Economic Aspects of Standardization and Technical Regulation. 2024; 5(80): 73–78. (In Russ.).