Подход к синтезу системы обеспечения информационной безопасности корпоративной сети связи

An Approach to the Synthesis of an Information Security System for a Corporate Communication Network

УДК 004
Получено: 22.04.2022 Одобрено: 16.05.2022 Опубликовано: 25.06.2022

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

Аннотация
Совершенствование способов применения компьютерных атак в отношении корпоративных сетей связи, интегрированных в мировое информационное пространство, требует соответствующего развития их систем обеспечения информационной безопасности. Существующие научно-методические подходы к синтезу систем обеспечения информационной безопасности не позволяют в полном объеме обосновать выбор их оптимального состава и структуры. В статье предлагаются системные свойства, основные показатели оценки качества систем обеспечения информационной безопасности и порядок их использования. На основе их численных оценок возможно выбрать систему обеспечения информационной безопасности путем обоснования состава и структуры, которые наиболее точно удовлетворяют заданным требованиям.
Ключевые слова: система обеспечения информационной безопасности, синтез, качество.

Abstract
Improving the use of computer attacks against corporate communication networks integrated into the global information space requires the appropriate development of their information security systems. The existing scientific and methodological approaches to the synthesis of information security systems do not allow to fully justify the choice of their optimal composition and structure. The article proposes system

properties, key indicators for assessing the quality of information security systems and the procedure for their use. Based on their numerical estimates, it is possible to choose an information security system by justifying the composition and structure that most accurately meet the specified requirements.

Keywords: information security system, synthesis, quality.

Перевод экономической и социальной деятельности современного общества в цифровое пространство, а также динамика увеличения инцидентов информационной безопасности (ИБ) и ущерба от них в Российской Федерации способствовали тому, что задача обеспечения ИБ является одной из актуальных. В настоящее время рассматриваемую предметную область регламентируют 17 Федеральных законов Российской Федерации, 8 Указов Президента Российской Федерации, более 100 государственных стандартов (ГОСТ) и иных руководящих документов, что способствует возникновению неопределенностей в общих подходах оценки качества СОИБ КСС [1-3].

На основании обобщения ряда руководящих документов (ГОСТ Р ИСО/МЭК 13335-1-2006; ГОСТ Р ИСО/МЭК 17799-2005; ГОСТ Р ИСО/МЭК 27001-2006; ГОСТ Р ИСО/МЭК 27005-2010; ГОСТ Р ИСО/МЭК 27033-1-2011; ГОСТ Р 53110-2008; ГОСТ Р-53114-2008; ГОСТ Р 53801-2008; ГОСТ Р 54583-2011 и др.) сформулирована концептуальная модель изучаемого процесса (рис. 1). В общем виде модель объединяет объект воздействия (КСС) с СОИБ и определенные процессы применения компьютерных атак (КА) злоумышленником.

КСС объединяет программные, аппаратно-программные, аппаратные средства обработки, хранения и передачи информации. С другой стороны, стратегии ИБ формируют политику ИБ КСС и определяют организационные, организационно-технические механизмы защиты КСС от компьютерных атак (СЗ КА). СЗ КА являются основными элементами систем обеспечения информационной безопасности (СОИБ) КСС.

В зависимости от КСС применяются различные СЗ КА и их сочетания (рис. 2) [4-6].

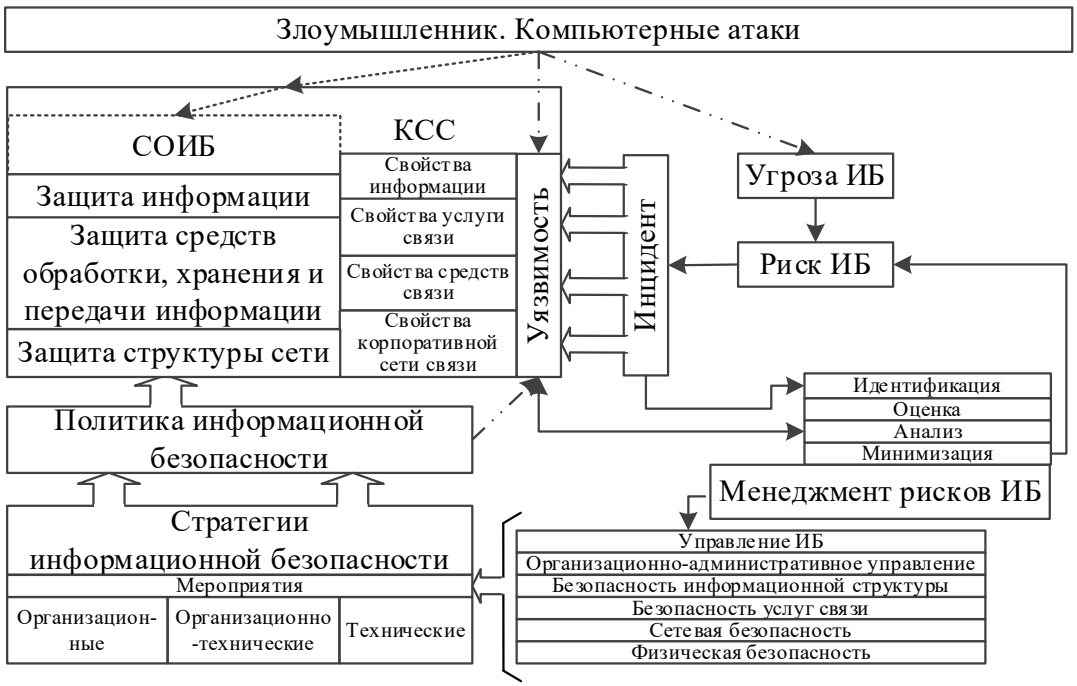

Рис. 1. Концептуальная модель процесса обеспечения ИБ КСС

Результаты анализа основных принципов и этапов синтеза СОИБ КСС свидетельствуют о том, что синтез сводится к задачам оптимизации значений показателей качества создаваемой системы путем изменения варьируемых параметров [7, 8]. С точки зрения системного анализа СОИБ представляет собой совокупность СЗ КА и связей между ними. Основными варьируемыми параметрами являются технические характеристики применяемых СЗ КА. Концептуально возможна разработка СЗ КА, полностью удовлетворяющих требованиям заказчика, однако с практической стороны это приведет к существенным финансовым и временным затратам. Вследствие чего синтез СОИБ сводится к рациональному выбору СЗ КА, обеспечивающему требуемое качество СОИБ [7, 9].

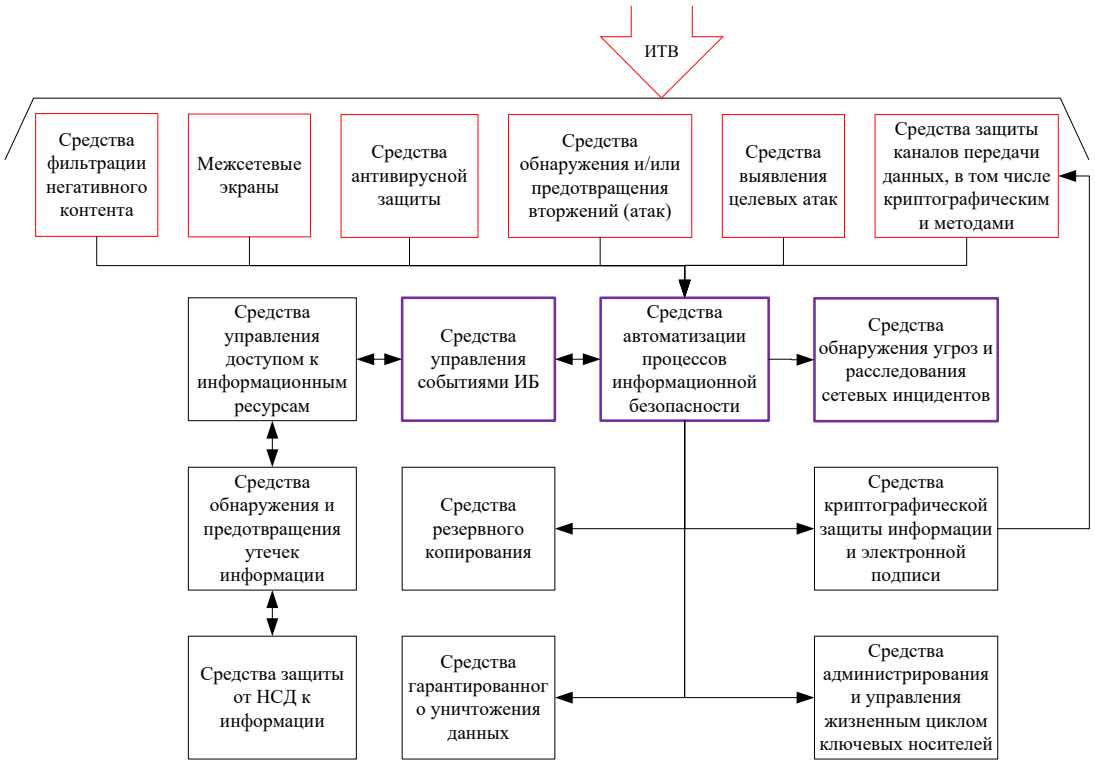

Рис. 2. Классификация средств защиты от компьютерных атак и вариант их взаимодействия

Под качеством СОИБ понимается онтологическая категория, раскрывающая закономерности формирования структуры, целостности, свойств объектов и процессов, их развития и реализации. Проведенные исследования показали, что для оценки качества создаваемой (модернизируемой) СОИБ целесообразно применять следующую группу показателей, отражающих основные свойства СОИБ на системном уровне [10, 11].

Своевременность – способность СОИБ выявлять, противодействовать (минимизировать) и устранять последствия информационно-технических воздействий в заданное время. В качестве основных показателей своевременности СОИБ используются:

– вероятность выявления признаков КА $\left(P_{\text{выявл}}(t)\right)$;

– вероятность успешного противодействия КА $\left(P_{\text{против}}(t)\right)$;

– вероятность устранения последствий КА $\left(P_{\text{устран}}(t)\right)$.

Оперативность – способность СОИБ прогнозировать развитие выявленных признаков КА, формировать стратегии применения и использовать СЗ КА для устранения (минимизации) ущерба, расследовать инциденты информационной безопасности.

В качестве основных показателей оперативности СОИБ используются:

– достоверность результатов прогнозирования $\left(D_{\text{прогн}}\right)$;

– количество сценариев развития ИТВ и защиты от них $\left(N_{\text{сцен}}\right)$;

– время прогнозирования $\left(T_{\text{прогн}}\right)$;

– вероятность своевременного прогнозирования $\left(P_{\text{прог}}(t)\right)$;

– время управленческого цикла (активации) $\left(T_{\text{упр}}\right)$;

– вероятность нахождения требуемого средства и механизма защиты в работоспособном состоянии $\left(P_{\text{прог}}(t)\right)$;

– время расследования инцидента информационной безопасности $\left(T_{\text{упр}}\right)$.

Полнота – способность СОИБ обеспечить защиту от актуальных на момент эксплуатации видов информационно-технических воздействий. В качестве основных показателей полноты СОИБ используется коэффициент полноты $\left(K_{\text{п}} = \frac{N_{\text{ИТВ}}^{\text{защ}}}{N_{\text{ИТВ}}^{\text{акт}}}\right)$, отражающий долю КА, от которых способна защитить СОИБ.

Модернизируемость – способность СОИБ в заданное время обновлять или дополнять состав программного обеспечения и технических средств защиты от КА с заданными режимами работы.

В качестве основных показателей модернизируемости СОИБ используются:

– количество операций $\left(N_{\text{опер}}^{\text{обн}}\right)$;

– среднее время, необходимое для обновления программного обеспечения и установления требуемых режимов работы $\left(\bar{t}_{\text{опер}}^{\text{обнПО}}\right)$;

– количество дополнительных операций $\left(N_{\text{опер}}^{\text{доп}}\right)$;

– среднее время, необходимое для дополнения состава техническим средством и установления требуемых режимов работы $\left(\bar{t}_{\text{опер}}^{\text{обнТС}}\right)$.

Устойчивость – способность СОИБ функционировать в условиях различных дестабилизирующих факторов, в заданных режимах работы и заданном расходе ресурсов элемента КС, на котором эта система установлена. Устойчивость включает надежность, стойкость и структурную живучесть.

Под надежностью СОИБ понимается способность системы сохранять во времени значения эксплуатационных показателей в пределах, соответствующих работоспособному состоянию. В качестве основного показателя надежности СОИБ используют коэффициент готовности $\left(K_{\text{г}}\right)$.

Под стойкостью СОИБ понимается способность системы выполнять функциональные задачи в условиях КА на ее элементы. В качестве основных показателей стойкости СОИБ используют:

– вероятность нахождения СОИБ в работоспособном состоянии $\left(p_i^{\text{работ}}(t)\right)$ при применении в отношении нее *i*-го вида КА;

– обобщенная вероятность нахождения СОИБ в работоспособном состоянии при КА на нее $\left(P^{\text{работ}}(t)\right)$;

– время восстановления работоспособности после выхода из строя СОИБ $\left(T_{\text{упр}}\right)$.

Под структурной живучестью СОИБ понимается способность функционировать в условиях выхода их строя части ее элементов. В качестве основных показателей структурной живучести СОИБ используют:

– количество элементов, при выходе которых СОИБ переходит в неработоспособное состояние $\left(N_{\text{эл}}^{\text{нрс}}\right)$;

– время восстановления работоспособности КСС после выхода ее или части элементов из строя $\left(T_{\text{упр}}\right)$.

Ресурсопотребляемость – характеризует затраты (финансовые, материальные, системные), используемые при разработке и функционировании СОИБ. В качестве основных показателей ресурсопотребляемости СОИБ используют:

– затраты на разработку (модернизацию) $\left(C_{\text{фин}}^{\text{разр}}\right)$;

– производство $\left(C_{\text{фин}}^{\text{СОИБ}}\right)$;

– эксплуатацию (в том числе утилизацию) $\left(C_{\text{фин}}^{\text{экспл}}\right)$;

– используемый системный ресурс при нормальной эксплуатации СОИБ $\left(R_{\text{эксп}}^{\text{норм}}\right)$;

– используемый системный ресурс при КА на элемент СССН $\left(R_{\text{эксп}}^{\text{возд}}\right)$;

– используемый системный ресурс при КА на СОИБ $\left(R_{\text{эксп}}^{\text{ИТВ}}\right)$.

Учитывая перечисленные параметры и их разнонаправленность, одним из важных этапов синтеза СОИБ является решение многокритериальной задачи, по выбору оптимальной структуры СОИБ. Указанную задачу, возможно, решить при помощи нахождения векторов, характеризующих эффективность каждого варианта построения СОИБ, который определяется на основании метода отклонений нормированных значений от требуемых значений [12-14].

Для решения данной задачи предлагается на первом этапе сформировать систему оценки качества СОИБ, включающую систему показателей качества КСС (требования к качеству предоставляемых услуг связи, технические характеристики и требования сетевых соединений и применяемых средств обработки, хранения и передачи данных) [15-17], систему показателей качества СОИБ, систему показателей качества СЗ КА [18-20], систему внешних воздействий (модель угроз и нарушителя), причем актуальную на момент ввода СОИБ в эксплуатацию, а не действующую на момент формирования технического задания) [21-23], систему измерений и систему правил сравнения [24-26]. Определить критерии принятия решения об уровне качества – правило сравнения текущих значений и эталонных.

На втором этапе с использованием метода отклонений нормированных значений от требуемых значений определить качество каждого из имеющихся СЗ КА путем нахождения обобщенной численной оценки качества. Для определения вектора определяющего качество каждого СЗ КА предлагается применять следующие свойства ИБ – целостность, доступность, конфиденциальность защищаемой информации. Исходные данные получаются на основании натурных или полунатурных экспериментов, с применением подходов диверсионного анализа. Сущность метода и пример расчета описан в [14].

На третьем этапе на основании принятых критериев исключаются СЗ КА, которые не удовлетворяют требуемым значениям (исключаются СЗ КА, которые обладают как неудовлетворительными характеристиками, так и избыточными).

На четвертом этапе формируются варианты структуры синтезируемой СОИБ [4, 5, 16], после чего при помощи метода отклонений нормированных значений от требуемых значений, производится определение значений качества каждого варианта построения (пятый этап). В качестве свойств, описывающих качество СОИБ, используют своевременность, оперативность, полноту, модернизируемость, устойчивость, ресурсопотребляемость.

Сформулированный подход позволяет найти рациональную структуру СОИБ, минимально отличающуюся от идеальной, при использовании известных СЗ КА. Данный подход позволяет сократить затраты на разработку новых СЗ КА и повысить обоснованность выбора структуры СОИБ за счет применения численных оценок. Основные положения подхода реализованы в патенте РФ на изобретение [27].

Литература

1. Информационная безопасность в 2021 году [Электронный ресурс] // Positive Technologies [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/informacionnaya-bezopasnost-v-2021-samye-gromkie-vzlomy-i-utechki (дата обращения 05.08.2022).
2. *Белов А.С., Добрышин М.М., Борзова Н.Ю.* Формирование модели угроз информационной безопасности на среднесрочный период // Приборы и системы. Управление, контроль, диагностика. 2021. – № 7. – С. 41-48.
3. *Добрышин М.М., Шугуров Д.Е.* Иерархическая многоуровневая модель таргетированных компьютерных атак в отношении корпоративных компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2020. – № 4. – С. 35-46.
4. *Добрышин М.М., Закалкин П.В., Горшков А.А., Манзюк В.В.* Вариант построения адаптивной системы мониторинга информационно-технических воздействий // Известия Тульского государственного университета. Технические науки. 2020. – № 9. – С. 14-21.
5. *Добрышин М.М.* Выбор структуры и механизмов адаптивного управления системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2022. – № 2. – С. 214-222.
6. *Дроботун Е.Б.* Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления // Монография. – СПб. : Наукоемкие технологии, 2017. – 120 с., ил.
7. *Добрышин М.М.* Тенденции развития теории информационной безопасности в условиях динамического изменения парадигмы применения информационно-технических воздействий / Экономика и качество систем связи. 2022. – № 1 (23). – С. 37-43.
8. *Анисимов В.Г.* Показатели эффективности защиты информации в системе информационного взаимодействия при управлении сложными распределенными организационными объектами / В.Г. Анисимов [и др.] // Проблемы информационной безопасности. Компьютерные системы. 2016. – № 4. – С. 140-145.
9. Anisimov V.G. A risk-oriented approach to the control arrangement of security protection subsystems of information systems / V. G. Anisimov, P. D. Zegzhda, E. G. Anisimov, D. A. Bazhin // Automatic Control and Computer Sciences. – 2016. – Т. 50. – № 8. – С. 717-721.
10. *Добрышин М.М.* Методика выбора последовательности применения информационно-технического оружия в отношении компьютерной сети с учетом стратегий распределения ресурсов обороняющейся стороны // Известия Тульского государственного университета. Технические науки. 2020. – № 9. – С. 232-237.

11. *Белов А.С., Добрышин М.М., Струев А.А., Горшков А.А.* Модель компьютерной сети, функционирующая в условиях деструктивных программных воздействий и учитывающая требуемый уровень восстанавливаемости // Известия Тульского государственного университета. Технические науки. 2022. – № 2. – С. 83-89.
12. *Зегжда П.Д.* Эффективность функционирования компьютерной сети в условиях вредоносных информационных воздействий // Проблемы информационной безопасности. Компьютерные системы. 2021. – № 1 (45). – С. 96-101.
13. *Анисимов В.Г.* Эффективность обеспечения живучести подсистемы управления сложной организационно-технической системы // Телекоммуникации. 2020. – № 11. – С. 41-47.
14. *Добрышин М.М.* Подход к формированию обобщенного критерия оценки эффективности системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2021. – № 9. – С. 113-121.
15. *Петухов Г.Б.* Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем / Г. Б. Петухов, В. И. Якунин Москва : АСТ, 2006. – 504 с.
16. *Белов А.С., Добрышин М.М.* Предложение по удаленному мониторингу программных средств автономных комплексов связи // Авиакосмическое приборостроение. 2021. – № 6. – С. 13-20.
17. *Анисимов В.Г., Анисимов Е.Г., Гречишников Е.В., Белов А.С., Орлов Д.В., Добрышин М.М., Линчихина А.В.* Способ моделирования и оценивания эффективности процессов управления и связи / Патент на изобретение RU 2673014 C1, 21.11.2018. Заявка № 2018103844 от 31.01.2018.
18. *Добрышин М.М., Закалкин П.В.* Способ мониторинга защищенности информационно-телекоммуникационных сетей от информационно технических воздействий / Информационные системы и технологии. 2018. – № 5 (109). – С. 74-82.
19. *Добрышин М.М., Горшков А.Н., Белов А.С., Борзова Н.Ю.* Вариант применения диверсионного анализа при разработке систем обеспечения информационной безопасности для корпоративной сети связи // Известия Тульского государственного университета. Технические науки. 2021. – № 9. – С. 67-72.
20. *Сауренко Т.Н.* Прогнозирование инцидентов информационной безопасности / Т.Н. Сауренко [и др.] // Проблемы информационной безопасности. Компьютерные системы. 2019. – № 3. – С. 24-28.
21. *Добрушин М.М., Гуцын Р.В.* Модель разнородных групповых компьютерных атак, проводимых одновременно на различные уровни ЭМВОС узла компьютерной сети связи // Известия Тульского государственного университета. Технические науки. 2019. – № 10. – С. 371-384.
22. *Добрышин М.М.* Модель разнородных компьютерных атак, проводимых одновременно на узел компьютерной сети связи // Телекоммуникации. 2019. – № 12. – С. 31-35.
23. *Зегжда П.Д.* Модель оптимального комплексирования мероприятий обеспечения информационной безопасности / П.Д. Зегжда [и др.] // Проблемы информационной безопасности. Компьютерные системы. 2020. – № 2. – С. 9-15.
24. *Шрейдер Ю.А.* Равенство, сходство, порядок / Ю. А. Шрейдер, Издательство Наука. Москва : Главная редакция физико-математической литературы, 1971. – 256 с.

25. *Башарин, Г.П.* Управление качеством и вероятностные модели функционирования сетей связи следующего поколения / Г.П. Башарин, Ю. В. Гайдамака, К. Е. Самуйлов Н. В. Яркина: Учеб. пособие. – Москва : РУДН, 2008. – 157 с.
26. *Гасюк Д. П.* Научно-методический подход по оцениванию живучести компьютерных систем в условиях внешних специальных программно-технических воздействий / Д. П. Гасюк, А. С. Белов, Е. Л. Трахинин. Проблемы информационной безопасности. Компьютерные системы. 2018. – № 4. – С. 86-90.
27. *Макаров В.Н., Гречишников Е.В., Добрышин М.М., Климов С.М., Манзюк В.В., Локтионов А.Д.* Способ выбора и обоснования тактико-технических характеристик системы защиты от групповых разнородных компьютерных атак на среднесрочный период / Патент РФ на изобретение № 2760099 22.11.2021 Бюл. № 33 Заявка 2020124308, от 22.07.2020. Патентообладатель: Академия ФСО России. G06F 21/57 (2013.01).