УПРАВЛЕНИЕ АКТИВАМИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КАК ОБЯЗАТЕЛЬНЫЙ ЭТАП УПРАВЛЕНИЯ ИХ УЯЗВИМОСТЯМИ

Милославская Н. Г.[1], Толстой А. И.[2]

DOI: 10.21681/2311-3456-2025-1-73-85

Цель работы: *систематизация подходов к управлению активами (УА) информационно-телекоммуникационных сетей (ИТКС) организаций как обязательному этапу управления их уязвимостями для последующего исключения возможности эксплуатации (использования) обнаруженных уязвимостей в рамках управления сетевой безопасностью ИТКС и разработки краткой инструкции по реализации процесса УА ИТКС.*

Методы исследования: *анализ релевантных нормативных документов и научных публикаций, концептуальное моделирование, экспертная оценка, синтез комплексного подхода к управлению активами в рамках управления сетевой безопасностью.*

Полученные результаты: *в статье вводится понятийная база УА ИТКС и на основе специально подобранной нормативной базы систематизируются подходы к УА ИТКС организаций как обязательному этапу управления их уязвимостями с целью последующего устранения этих уязвимостей. Выделяются мероприятия, реализуемые в ходе процесса УА ИТКС, особенно при идентификации активов ИТКС, и обсуждается состав системы УА (СУА) ИТКС, ориентированный на минимизацию возможности осуществления компьютерных атак на ИТКС организации. Кратко рассматриваются основные документы СУА ИТКС – стратегический план УА ИТКС, планы УА нижнего уровня и политика УА ИТКС, предназначенные для достижения целей УА ИТКС. На основе проведенного исследования с соблюдением принципа разумной достаточности разработана краткая пошаговая инструкция по реализации процесса УА ИТКС.*

Практическая значимость *заключается в разработке краткой инструкции по реализации процесса УА ИТКС, особенно процесса идентификации активов ИТКС, в рамках управления сетевой безопасностью ИТКС при решении задач устранения найденных для активов ИТКС уязвимостей, что, в свою очередь, приведет к минимизации возможностей реализации компьютерных атак на ИТКС организаций.*

Ключевые слова: *информационно-телекоммуникационная сеть, управление активами, процесс управления активами, система управления активами, управление уязвимостями активов, управление сетевой безопасностью.*

Введение

Деятельность современных организаций в различных сферах человеческой деятельности невозможно представить без использования информационных технологий (ИТ) и построенных на их основе ***информационно-телекоммуникационных сетей (ИТКС)***. В Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ИТКС определена как технологическая система (ТС), предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (СВТ)[3]. В свою очередь ТС представляет собой совокупность технических и программных средств, обеспечивающая передачу информации на значительные расстояния с использованием коммутируемых и выделенных линий или специальных каналов связи[4], а СВТ — это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[5].

Используя ИТКС организации, ее сотрудники работают на постоянной или временной основе, выполняя свои функциональные обязанности и пользуясь всем спектром предоставляемых услуг [1]. Но в то же время по единодушным оценкам различных аналитиков каждый день фиксируется огромное

1 Милославская Наталья Георгиевна, доктор технических наук, Ph.D. in Cybersecurity, доцент, НИЯУ МИФИ, Москва, Россия. E-mail: NGMiloslavskaya@mephi.ru, https://orcid.org/0000-0002-1231-1805

2 Толстой Александр Иванович, кандидат технических наук, доцент, НИЯУ МИФИ, Москва, Россия. E-mail: aitolstoj@mephi.ru, https://orcid.org/0000-0001-9265-1510

3 Об информации, информационных технологиях и о защите информации / Федеральный закон от 27 июля 2006 г. № 149-ФЗ, статья 2: принят Гос. Думой 8 июля 2006 г.; одобрен Советом Федерации 14 июля 2006 г. – 2006. – 88 с.

4 Руководство по организации эксплуатации информационно-телекоммуникационной системы Банка России: в 2 томах. [Электронный ресурс]. М.: АС «Сфинкс», 2008. № НМД-4. 1 электрон, опт. диск (CD-ROM).

5 ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – Введен 1996-01-01. – М., Госстандарт РФ, 1995. – 8 с.

количество компьютерных атак (КА), направленных на получение любой ценной информации – коммерческой, служебной, технической, персональных данных (ПДн), сведений об учетных записях пользователей, почтовых сообщений, конфигурационных файлов, журналов регистрации событий и т.п. [2–4]. А далее для реализации новых КА (поиска уязвимых ресурсов, получения первичного доступа к ИТКС, кражи данных и т.д.) используются полученные в результате предыдущих КА данные, находящиеся в открытом доступе (англ. *Open Source Intelligence – OSINT*) [5].

На SOC-форуме[6], состоявшемся в Москве 6–8 ноября 2024 г., сотрудники ПАО «Сбербанк» подчеркнули, что ПДн 90 % населения есть в интернете[7]. В начале года фиксировалось около 20 млн попыток дозвона мошенников до граждан в сутки, но благодаря новым разработкам эта цифра снизилась к концу года до 6–8 млн. На межотраслевой конференции «Безопасность клиента на первом месте» (19 ноября 2024 г.) было уточнено, что 50 % этих звонков осуществляется с мессенджеров с применением технологий SIM-box (устройства, поддерживающего несколько SIM-карт, подключенных к одному шлюзу) и виртуальных автоматических телефонных станций (АТС).

Представители ФСТЭК России в своих выступлениях 2023–2024 гг. неоднократно отмечали КА через критические уязвимости на периметре и цепочки поставок (англ. *supply chains*) [7], а также неистребимый фишинг, основанный на доверии людей [8]. Среди главных целей атакующих – нарушение функционирования ИТ-инфраструктур компаний или даже их разрушение и уничтожение, стирание информации, чтобы информационные системы (ИС) больше не могли работать [9], а также ее шифрование с целью выкупа [10].

Компьютерные преступления могут приобретать и еще более изощренные формы, особенно в период нестабильной политической ситуации. Отключения провайдеров от крупных магистральных каналов, атаки на СМИ для создания инфоповодов и вызова общественного резонанса, появление вредоносного кода в обновлениях программного обеспечения (ПО) – вот лишь некоторые из них.

Новые технологии, такие как беспроводной доступ (*Wi-Fi*), виртуализация, интернет вещей (англ. *Internet of Things – IoT*), системы искусственного интеллекта (англ. *Artificial Intelligence*), изначально разрабатываемые без учета требований по обеспечению информационной безопасности (ИБ, ОИБ), также предоставляют злоумышленникам возможности для КА.

По данным МВД[8], 45 % компьютерных преступлений в 2024 г. связано с ИТКС, что в 2025 г. уже приблизится к 50 %.

Эксперты считают, что многие проблемы возникают из-за пренебрежения элементарными мерами ОИБ (например, неправильно сконфигурированные системы и оборудование), недостатка или даже отсутствия самых необходимых средств защиты информации (СЗИ) типа антивирусов из-за низкой приоритетности вопросов ОИБ при распределении ресурсов, недостаточно защищенных точек удаленного доступа к ИТКС, отсутствия разработанных и внедренных процессов реагирования на инциденты ИБ и выяснения причин произошедших нарушений ИБ, человеческого фактора, включая неправильное распределение обязанностей работников во избежание ситуаций, когда все зависит от одного человека, и недостаточного внимания, уделяемого непрерывному обучению специалистов по ИБ и повышению информированности остальных работников, и много другого.

Таким образом, можно сказать, что главный вопрос сегодня – не случится ли КА на организацию или отдельного индивидуума, а когда это произойдет, что во многом зависит от причин и условий реализации КА. Следовательно, как никогда ранее необходимо уделять должное внимание вопросам, связанным с управлением уязвимостями активов ИТКС. Поэтому целью данной статьи является систематизация подходов к управлению активами (УА) ИТКС организаций как обязательному этапу управления их уязвимостями для последующего исключения возможности эксплуатации (использования) обнаруженных уязвимостей в рамках управления сетевой безопасностью ИТКС и разработка краткой инструкции по реализации процесса УА (ПУА) ИТКС.

1. Нормативная база управления активами

Российская нормативная база УА представлена следующими стандартами:

1) группа ГОСТ Р 55.0.0Х «Управление активами» в составе:
   - ГОСТ Р 55.0.00-2014[9], основополагающего в данной группе и устанавливающего общие положения и структуру национальной системы стандартов в области управления физическими и нематериальными активами;

6 SOC Forum 2024: подводя итоги. 12 ноября 2024 г. [Электронный ресурс]. – Режим доступа: https://ib-bank.ru/bisjournal/post/2333 (дата обращения: 30.12.2024).

7 Кошкин В. Топ-менеджер Сбербанка: Данные 90 % взрослых россиян есть в открытом доступе. 6 ноября 2024. // Российская газета [Электронный ресурс]. – Режим доступа: https://rg.ru/2024/11/06/top-menedzher-sberbanka-dannye-90-vzroslyh-rossiianest-v-otkrytom-dostupe.html (дата обращения: 30.12.2024).

8 МВД оценило ущерб от преступлений в бюджетной сфере в 2024 г. в 112 млрд рублей. 16 декабря 2024 г. [Электронный ресурс]. – Режим доступа: https://smotrim.ru/article/4269430 (дата обращения: 30.12.2024).

9 ГОСТ Р 55.0.00-2014 Управление активами. Национальная система стандартов. Основные положения. – Введ. 2015-04-01. – М., Стандартинформ, 2015. – 12 с.

- ГОСТ Р 55.0.01-2014/ИСО 55000:2014[10], дающего общее представление об УА и системе УА (СУА) и содержащего принципы УА и соответствующую терминологию, а также демонстрирующего ожидаемые выгоды от осуществления УА в большей степени для использования при управлении физическими активами;
- ГОСТ Р 55.0.02-2014/ИСО 55001:2014[11], устанавливающего требования к разработке, внедрению, поддержанию в рабочем состоянии и улучшению СУА в большей степени при управлении физическими активами с учетом внешнего и внутреннего контекста организации, что может повлиять на способность организации достичь намеченных результатов ее СУА;
- ГОСТ Р 55.0.03-2021[12], содержащего рекомендации по применению СУА в соответствии с требованиями ГОСТ Р 55.0.02 и дающего пояснения к указанным в ГОСТ Р 55.0.02 требованиям с примерами, демонстрирующими выполнение этих требований;
- ГОСТ Р 55.0.05-2016[13], устанавливающего требования к порядку выбора метода УА на этапе эксплуатации для принятия оптимального решения по повышению безопасности и надежности активов, основанного на оценке рисков и обеспечивающего выполнение активами своих функций;
- ГОСТ Р 55.0.06-2021[14], содействующего организациям в обеспечении согласованности финансовой и нефинансовой деятельности всех подразделений при УА как «по вертикали», так и «по горизонтали» с целью улучшить внутренний контроль при управлении организацией;

2) два стандарта по УА при управлении непрерывностью бизнеса:

   - ГОСТ Р 55235.1-2012[15], устанавливающий требования к СУА, направленные на обеспечение оптимального управления производственными активами и системами активов (информационных, нематериальных, финансовых и человеческих) на всех этапах их жизненного цикла;
   - ГОСТ Р 55235.2-2012[16], формулирующий основные принципы применения требований ГОСТ Р 55235.1 к оптимальному управлению производственными активами и содержащий руководство по созданию, внедрению, поддержке и улучшению системы управления производственными активами и ее взаимодействия с другими системами менеджмента организации;

3) ГОСТ Р ИСО/МЭК 27005-2010[17], описывающий весь процесс управления рисками ИБ, включая установление контекста (выходные данные процесса – спецификация основных критериев, область применения и границы, организационная структура для процесса управления рисками ИБ), идентификации рисков ИБ (выходные данные процесса – перечень активов, подлежащих управлению рисками, и перечень бизнес-процессов, связанных с активами, а также их ценность, выявление уязвимостей (выходные данные процесса – перечень уязвимостей, связанных с активами, угрозами и мерами ОИБ, и перечень уязвимостей, не связанных с выявленной угрозой, подлежащей рассмотрению), общая оценка и обработки рисков ИБ, а также принятие, обмен информацией (коммуникация), мониторинг и переоценка рисков ИБ.

Международная нормативная база УА опирается на стандарты ISO и ISO/IEC, указанные выше для идентичных им стандартов РФ, и их новые редакции, например, ISO 55000:2024, ISO 55001:2024, ISO/TS 55010:2024, ISO/IEC 27005:2022.

Отдельно разработана группа стандартов ISO/IEC 19770-X для управления ИТ-активами, первый из которых наиболее интересен в рамках тематики исследования, поскольку в нем изложены дополнительные или более подробные требования к управлению ИТ-активами. В РФ существует ГОСТ Р ИСО/МЭК 19770-1-2021[18], идентичный стандарту ISO/IEC 19770-1. Основным его отличием от стандартов ГОСТ Р 55.0.02-2014 и ИСО 55001:2014 является обоснование необходимости управления программными активами с их особыми характеристиками.

10 ГОСТ Р 55.0.01-2014/ИСО 55000:2014 Управление активами. Национальная система стандартов. Общее представление, принципы и терминология. – Введ. 2015-04-01. – М., Стандартинформ, 2015. – 24 с.

11 ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Национальная система стандартов. Система менеджмента. – Введ. 2015-04-01. – М., Стандартинформ, 2015. – 16 с.

12 ГОСТ Р 55.0.03-2021 Управление активами. Система менеджмента. Руководство по применению ИСО 55001. – Введ. 2021-09-01. – М., Стандартинформ, 2021. – 58 с.

13 ГОСТ Р 55.0.05-2016 Управление активами. Повышение безопасности и надежности активов. Требования. – Введ. 2016-10-01. – М., Стандартинформ, 2018. – 15 с.

14 ГОСТ Р 55.0.06-2021 Управление активами. Руководство по обеспечению согласованности финансовой и нефинансовой деятельности при управлении активами. – Введ. 2016-09-01. – М., Стандартинформ, 2021. – 21 с.

15 ГОСТ Р 55235.1-2012 Практические аспекты менеджмента непрерывности бизнеса. Менеджмент активов. Требования к оптимальному управлению производственными активами. – Введ. 2013-12-01. – М., Стандартинформ, 2020. – 30 с.

16 ГОСТ Р 55235.2-2012 Практические аспекты менеджмента непрерывности бизнеса. Менеджмент активов. Руководство по применению требований к оптимальному управлению производственными активами. – Введ. 2013-12-01. – М., Стандартинформ, 2020. – 62 с.

17 ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Введ. 2011-12-01. – М., Стандартинформ, 2011. – 47 с.

18 ГОСТ Р ИСО/МЭК 19770-1-2021 Информационные технологии. Управление ИТ-активами. Часть 1. Системы управления ИТ-активами. Требования. – Введ. 2013-12-01. – М., Российский институт стандартизации, 2021. – 36 с.

Также заслуживает отдельного внимания опубликованный в США (2018 г.) документ NIST SP 1800-5[19] «IT Asset Management» в трех частях (NIST SP 1800-5A «Executive Summary», NIST SP 1800-5B «Approach, Architecture, and Security Characteristics» и NIST SP 1800-5C «How-To Guides»), который является подробным практическим руководством, демонстрирующим конкретные технологии и средства, подлежащие внедрению для отслеживания местоположения и конфигурации сетевых устройств и ПО в организации, включая традиционное отслеживание физических активов, информацию об ИТ-активах, физическую безопасность, а также информацию об уязвимостях и соответствии требованиям.

Представленные далее результаты работы базируются на данной нормативной базе.

2. Активы ИТКС

Как следует из названия, ИТКС представляет собой симбиоз двух видов сетей — информационной и телекоммуникационной. Эти сети территориально распределены по месту размещения, объединяют большое количество разнообразных технических средств обработки, передачи и хранения информации, различаются по масштабу, решаемым задачам и типам обрабатываемых данных.

Чаще всего ИТКС рассматривают как часть организации, реализующей определенные бизнес-процессы. При этом можно считать, что ИТКС оказывает организации внутренние ИТ-услуги (англ. *IT services*) на основе реализации совокупности процессов, связанных со сложными режимами автоматизированной обработки данных и совмещением выполнения информационных запросов различных категорий пользователей — потребителей информации и ИТ-услуг. При этом все составляющие ИТКС должны функционировать непрерывно и устойчиво в условиях высокой интенсивности информационных потоков [11] и существования угроз нанесения ущерба информации и ущерба функциональной устойчивости (ФУ) ИТКС (англ. *resilience*).

С учетом этого можно определить цели, которые необходимо достичь при использовании ИТКС в конкретной организации – это выполнение требований по реализации определенного набора процессов ИТКС для предоставления ИТ-услуг (функционал ИТКС), ОИБ ИТКС и обеспечению ФУ (ОФУ) ИТКС.

При ОИБ и ОФУ ИТКС как некоторого объекта прежде всего обращают внимание на ту его часть, которая признается наиболее ценной для его владельца и которую принято[20] называть активом объекта. В данной работе принимаются следующие термины [12] и их определения.

Актив (англ. *asset*) ***объекта*** (ИТКС) — наиболее ценная для владельца часть объекта (ИТКС).

Владелец актива – субъект, осуществляющий владение и пользование активом и реализующий полномочия распоряжения им в пределах, установленных законом.

Ценность актива объекта (ИТКС) будет определяться исходя из влияния актива на реализацию процессов самого объекта. При этом возможны принципиально отличающиеся два варианта: ИТКС как уникальный объект, реализующий определенные процессы, и ИТКС как часть организации, реализующая вспомогательные (обеспечивающие) процессы для ее бизнес-процессов.

При реализации соответствующих угроз ИБ (например, КА) на ИТКС их целью прежде всего являются активы ИТКС. Поэтому актуальным будет выполнение следующей совокупности необходимых действий для определения и описания активов ИТКС: формирование перечня активов с учетом их ценности, определение их свойств, классификация активов с учетом их видов и определение уязвимостей активов. Совокупность этих действий будем называть ***идентификацией активов объекта*** (ИТКС). При их выполнении необходимо учитывать следующие факторы.

В перечень активов ИТКС должны быть включены только те активы, которые непосредственно влияют на результативность процессов, реализуемых ИТКС, а также бизнес-процессов организации, если ИТКС рассматривается как объект этой организации. Причем ценность активов будет определяться с учетом уровня влияния активов на вышеуказанные процессы.

Поскольку активы ИТКС рассматриваются в контексте ОИБ и ОФУ ИТКС, то основными свойствами активов будут свойства ИБ (конфиденциальность, целостность, доступность[20]) и свойства ФУ (доступность и целостность процессов, реализуемых ИТКС, и свойства, определяющие готовность ИТКС к обеспечению непрерывности бизнеса[21]).

Активы ИТКС целесообразно классифицировать, разделив их на виды и группы[16]. При дальнейших рассуждениях возьмем за основу два вида активов ИТКС: основные и вспомогательные, которые разделяются на две группы: основные активы (информационные активы и процессы ИТКС) и вспомогательные активы (аппаратное обеспечение (АО), ПО, телекоммуникационное и сетевое оборудование (ТСО), бизнес-приложения, персонал, сама ИТКС (и, возможно, сама организация), место функционирования ИТКС и организации).

19 Stone M., Irrechukwu C., Perper H., Wynne D., Kauffman L. IT Asset Management. NIST SP 1800-5. September 2018. 237 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf. (дата обращения: 10.01.2025).

20 ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

21 ГОСТ Р ИСО 27031-2012 «Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».

Иногда в отдельный класс выделяют ***ИТ–актив*** (англ. *IT asset*) – это любая принадлежащая организации информация, система или оборудование, используемые в ее деятельности с применением ИТ. Из анализа приведенных выше примеров активов ИТКС можно сделать вывод, что ИТ-активы являются подмножеством как основных (информационные активы), так и вспомогательных (АО, ПО, ТСО) активов.

Для уточнения понятия «информационный актив» воспользуемся определениями понятия «информация», данные в Федеральном законе № 149-ФЗ[3] и в стандарте ГОСТ Р 50922-2006[22]. ***Информационный актив*** (ИА) (англ. *information asset*) – это информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для организации, находящаяся в распоряжении этой организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме[23]. При выделении ИА необходимо учитывать категории информации (общедоступная или ограниченного доступа) и возможные разновидности свойств ИБ, присущих отдельным ИА.

Именно вспомогательным активам присущи уязвимости, которые могут быть использованы угрозами ИБ, нацеленными на нанесение ущерба активам ИТКС.

Теперь определим важное понятие исследования – «***уязвимость (актива объекта)***» (англ. *vulnerability*). Это любая характеристика или свойство актива объекта, которое может быть использовано для реализации или способствовать реализации угрозы ИБ [11].

Если уязвимость соответствует угрозе, то существует риск нарушения свойств активов ИТКС. Уязвимости, например, активов ИС, могут использоваться для компрометации (взлома) объекта, в данном случае ИТКС. Деятельность по анализу и исключению возможностей их использования (эксплуатации) выявленных уязвимостей активов ИТКС обобщенно называют ***управлением уязвимостями***. Согласно методическому документу ФСТЭК России[24], этот процесс включает в себя пять основных этапов: мониторинг уязвимостей и оценка их применимости, оценка уязвимостей, определение методов и приоритетов исключения возможностей их использования (эксплуатации) уязвимостей угрозами нарушения безопасности информации (угрозами ИБ) в ИТКС или угрозами нарушения ФУ ИТКС, собственно реализация этих методов и контроль исключения возможностей использования (эксплуатации) уязвимостями. Очевидно, что перед началом осуществления процесса управления уязвимостями, необходимо идентифицировать все активы ИТКС, в которых эти уязвимости могут быть обнаружены. Такие действия выполняются в рамках реализации процессов идентификации и процессов управления активами ИТКС.

Имеется еще один аспект, относящийся к идентификации активов объектов (ИТКС). Результатом управления уязвимостями активов объекта может быть использование на объекте (в ИТКС) определенных мер ОИБ (средств и систем ОИБ и ОФУ объекта (ИТКС). Эти средства и системы имеют свои активы, возможно, обладающие уязвимостями, требующими реализации своих процессов идентификации активов и управления этими уязвимостями. В противном случае добавление в ИТКС средств и систем ОИБ может привести не к улучшению, а к ухудшению ситуации, связанной с ОИБ и ОФУ ИТКС.

Источником информации для формирования перечня активов ИТКС в аспекте необходимости ОИБ и ОФУ ИТКС является спецификация ИТКС, дополненная перечнем информации, обрабатываемой в ИТКС. Спецификация создается на этапе разработки (планирования) ИТКС с учетом требований к функционалу ИТКС на основе выполнения следующих действий (процессов): определение и описание основного процесса (бизнес-процесса) организации; определение и описание процессов, которые должны быть реализованы ИТКС в рамках оказания внутренних ИТ-услуг (вспомогательные процессы); разработка архитектуры ИТКС; обоснование и выбор информационных технологий и средств, которые будут использованы в ИТКС; разработка набора схем ИТКС (структурная, функциональная и принципиальная схемы).

Полную совокупность элементов спецификации можно назвать перечнем активов ИТКС. По сути, формируется три перечня активов ИТКС: полный перечень активов в контексте обеспечения реализации функционала, перечень активов в контексте ОИБ и перечень активов в контексте ОФУ ИТКС.

Эти перечни активов имеют следующие различия:

1) максимальное количество активов ИТКС имеет первый перечень;
2) разные подходы к определению ценностей активов;
3) активы из второго и третьего перечней являются обоснованной выборкой активов из первого перечня. Их количество не может превышать количество активов первого перечня. Второй и третий перечень могут включать разные активы;
4) выделение в качестве главных разных активов: все активы (первый перечень), ИА (второй перечень), процессы, реализуемые в рамках ИТ-услуг (третий перечень);
5) при идентификации активов их уязвимости не определяются для активов первого перечня;
6) уязвимости активов второго и третьего перечня могут быть разными.

22 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
23 Милославская Н. Г., Толстой А. И. Управление информационной безопасностью. Конспект лекций: учебное пособие. М., НИЯУ МИФИ, 2020. 534 с.
24 Федеральная служба по техническому и экспортному контролю. Методический документ. Руководство по организации процесса управления уязвимостями в органе (организации) (утв. ФСТЭК России 17 мая 2023 г.)

При идентификации активов рекомендуется определенный порядок действий: сначала идентификация активов первой, затем второй и далее третьей групп.

3. Процессы идентификации активов ИТКС

При идентификации активов ИТКС будем использовать процессный подход, который базируется на понятии «процесс». Опираясь на определения Большого толкового словаря русского языка [14] и ГОСТ Р ИСО 9000–2015, введем следующее «интегрирующее» определение: процесс – это совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующая входы (входные данные) в выходы (выходные данные) и требующая для этого определенных ресурсов и управляющих воздействий (управления) [15]. Входами для процесса обычно являются выходы других процессов, а выходы процессов – входами для других процессов. Выходные данные являются результатом процесса, в той или иной степени удовлетворяющие сформулированным заранее требованиям. Два или более взаимосвязанных и взаимодействующих процессов совместно могут также рассматриваться как процесс.

Действия, связанные с идентификацией активов объекта (ИТКС), можно рассмотреть как совокупность связанных процессов идентификации активов. В табл. 1 представлено описание этих процессов в части определения входных данных (К1i) и выходных данных (К2i) для каждого i-ого процесса, где $i = 1, \ldots, N$, N – количество процессов ($N = 4$).

Следует отметить, перечень процессов, представленных в табл. 1, относится к активам всех трех перечней, за исключением отсутствия процесса 4 для активов первого перечня.

Анализ данных из табл. 1 показывает, что все выделенные процессы связаны друг с другом. Причем во входные данные, начиная со второго процесса, входят выходные данные одного или нескольких предыдущих процессов. Входные данные первого процесса содержат данные описания процессов объекта (ИТКС) и бизнес-процессов организации, если объект является частью организации, выполненных в виде процессных моделей организации и объекта, а также данные функциональной схемы объекта (ИТКС) и его спецификации.

При описании процессов идентификации активов объекта (ИТКС) важным является определение целей реализации таких процессов. В данном случае цель реализации конкретного процесса идентификации совпадает с выходом этого процесса (табл. 1).

Необходимо отметить дополнительные различия в описании процессов идентификации активов объекта (ИТКС), относящихся к различным перечням активов.

1. Идентификация активов в контексте ОИБ ИТКС и ОФУ ИТКС осуществляется на стадии планирования (проектирования) системы ОИБ (СОИБ) и системы ОФУ (СОФУ) ИТКС соответственно.
2. Идентификация активов в контексте обеспечения функционала ИТКС должна проводится в отношении процессов различных стадий жизненного цикла

Таблица 1.

Описание процессов идентификации активов объекта (ИТКС)

№ п/п	Процессы идентификации активов объекта	Входные данные К1i	Выходные данные К2i
1	Формирование перечня активов с учетом их ценности	К11: Процессная модель объекта и организации, функциональная схема и спецификация объекта	К12: Перечень активов с определением их связей с процессами объекта и организации и определением их ценности
2	Определение свойств активов	К21 = К12 Перечень активов с определением их связей с процессами объекта и организации и определением их ценности	К22: Перечень активов с определением их свойств и указанием приоритетов по сохранению этих свойств
3	Проведение классификации активов	К31 = К11 + К21 + К22	К32: Результаты классификации активов с учетом их видов, типов и категорий
4	Определение уязвимостей активов	К41 = К32	К42: Перечень и описание уязвимостей активов объекта

активов ИТКС. К таким процессам, например, можно отнести процессы, связанные с приобретением, учетом (инвентаризацией), эксплуатацией, обслуживанием, модернизацией и выводом из эксплуатации (утилизацией) активов ИТКС.

3. Возможны разные варианты регламента идентификации активов с учетом необходимости формирования разных перечней активов ИТКС:
   - первый (наиболее простой) основан на последовательной раздельной разработке ИТКС, СОИБ ИТКС и СОФУ ИТКС. Такой подход предусматривает сначала формирование первого перечня активов с учетом только требований к функционалу ИТКС. Далее этот перечень фиксируется и остается неизменным при формировании второго и третьего перечней активов;
   - второй (итерационный, более сложный) предусматривает итерацию следующих действий: разработка ИТКС, СОИБ и СОФУ, анализ выполнимости требований по ОИБ и/или ОФУ ИТКС с этим набором ИТ и/или реализующих их средств, определение необходимости их замены, выбор новых ИТ и/или реализующих их средств, возврат к разработке ИТКС, СОИБ и СОФУ с корректированными перечнями активов. Этот итерационный процесс необходимо продолжать до удовлетворения всех требований по обеспечению функционала, ОИБ и ОФУ ИТКС.

4. Процессы управления активами ИТКС

Процессный подход предполагает, что достижение определенной цели реализации конкретного процесса возможно только при результативном управлении этим процессом. С учетом этого, взяв за основу стандарт ГОСТ Р 55235.1, можно сформулировать определение следующего понятия: ***управление активами объекта (УА)*** (англ. *asset management*) – это постоянная и скоординированная деятельность по реализации ценности от активов объекта для стабильного достижения основных целей деятельности организации [16]. Все действия (бизнес-практики) по управлению активами необходимо выполнять и поддерживать на разных уровнях управления организацией.

Учитывая положения группы стандартов ГОСТ Р 55.0.0Х, можно определить следующие принципы, на которых должно базироваться УА ИТКС:

- ценность, предоставляемая активами ИТКС, которая может быть материальной или не материальной, финансовой или не финансовой, непосредственно связана с удовлетворением требований заинтересованных сторон;
- согласованность целей УА ИТКС (т.е. результаты, которые должны быть достигнуты при УА ИТКС) с целями организации;
- лидерство и приверженность на всех уровнях управления, которые необходимы для успешного создания, функционирования и улучшения УА ИТКС в организации;
- предоставление гарантий того, что активы ИТКС будут выполнять требуемые от них функции.

Согласно ГОСТ Р 55235.Х, основными принципами УА ИТКС с несколько иной точки зрения являются целостность, систематичность, системность, обоснованность с точки зрения риска, оптимальность, жизнеспособность, интегрированность.

Принципиально важным является определение целей УА ИТКС. Цели УА ИТКС определяют направления деятельности организации для обеспечения того, чтобы активы ИТКС могли выполнить предъявляемые к ним требования, следуют из целей организации и должны учитывать требования соответствующих заинтересованных сторон, а также другие финансовые, технические, нормативные, законодательные и организационные требования. Согласно ГОСТ Р 55.0.00, эти цели могут быть определены как количественно (например, готовность производственных мощностей или количественные критерии приемлемости риска), так и качественно (например, ощущение социальной ответственности, репутация или нравственные ценности) и должны регулярно пересматриваться.

Для двух разных групп процессов, относящихся к активам ИТКС (процессы идентификации активов, относящиеся к базовым процессам управления их уязвимостями, и процессы, относящиеся к этапам жизненного цикла активов), то цели УА ИТКС будут отличаться:

- цель УА ИТКС в отношении процессов идентификации активов ИТКС: обеспечение необходимого качества реализации этих процессов в контексте достижения требуемого уровня ОИБ и ОФУ ИТКС в условиях воздействия КА;
- цель УА ИТКС в отношении процессов этапов жизненного цикла активов ИТКС: обеспечение необходимого качества реализации этих процессов в контексте достижения требуемого функционала ИТКС.

Указанные цели достигаются путем реализации ***процессов управления активами*** (ПУА) ИТКС, которые представляют собой совокупность согласованных действий, направленных на процессы идентификации активов ИТКС, или на процессы этапов жизненного цикла активов ИТКС на стадиях планирования, реализации, контроля и совершенствования этих процессов.

Общей методологической базой формирования и реализации ПУА ИТКС является процессный подход и использование циклической модели PDCA[25].

Примером может быть формулировка типового ПУА ИТКС: организационное и документационное сопровождение планирования, реализации, контроля и совершенствования конкретного процесса идентификации (или процесса, этапа жизненного цикла) актива ИТКС.

Согласно ГОСТ Р 55.0.00, ПУА ИТКС включает в себя следующие действия:

- согласование целей УА ИТКС и стратегического плана УА (СПУА) ИТКС с целями и стратегическим планом организации;
- определение необходимых активов ИТКС (формирование портфеля активов ИТКС), их функций и производительности для достижения целей;
- выбор методов, критериев и подходов для эффективного УА ИТКС с последующей разработкой процессов;
- идентификация и оценка рисков, связанных с активами ИТКС (только при формировании первого перечня активов);
- выработка и принятие оптимальных инвестиционных решений на этапах жизненного цикла активов ИТКС;
- планирование деятельности на всех этапах жизненного цикла активов ИТКС;
- мониторинг, измерение, анализ и оценка достигнутых результатов;
- выработка решений по улучшениям.

На основе анализа многочисленных зарубежных публикаций на тему управления ИТ-активами (например, [17, 18]) обобщенно определим два ключевых процесса, отличающихся от представленных в рассмотренных стандартах и конкретизирующих те из них, которые связаны с ОИБ:

1) ***управление учетностью активов*** (англ. *accountability management*), что включает в себя, например, следующие подпроцессы:
   - обнаружение (англ. *discovery*) активов вручную или автоматизировано (с использованием агентов, установленных на подключенных к ИТКС устройствах, или без использования агентов посредством сканирования диапазона IP-адресов, чему может помешать МЭ или политика безопасности);
   - периодически проводимая на систематической основе инвентаризация (англ. *inventory operations*) с фиксацией названия актива, серийного номера, модели, локации и т.п.;
   - осуществление порядка поставок активов (англ. *supply discipline*), их размещения в необходимых локациях и определение ответственных за них;
   - управление поставщиками (англ. *vendor management*), что важно, например, при замене или ремонте части активов;
   - аудит БД активов (англ. *asset database audit*), содержащей записи обо всех активах в области применения управления ИТ-активами, на регулярной основе;
2) ***управление операциями с активами*** (англ. *asset operations management*), что включает в себя следующие подпроцессы:
   - управление ИТ-операциями (англ. *IT operations management*) с активами на протяжении их жизненного цикла;
   - управление лицензиями на ПО (англ. *software license management*);
   - управление на основе «службы поддержки» (англ. *service desk*);
   - техническое управление (англ. *technical management*) для диагностики и решения технических проблем за пределами полномочий «службы поддержки».

5. Система управления активами ИТКС

Для руководства, координации и контроля всей деятельности организации по управлению всеми ее активами предназначена соответствующая ***система управления активами*** (СУА) (англ. *asset management system*). Определим СУА ИТКС как совокупность взаимосвязанных и взаимодействующих элементов организации для разработки политики УА (ПолУА) ИТКС и целей УА ИТКС и процессов, необходимых для достижения этих целей. СУА ИТКС обеспечивает структурированный подход к разработке, координации и управлению всей деятельностью по УА ИТКС на всех этапах жизненного цикла активов ИТКС, а также для согласования этой деятельности с основной деятельностью организации. Такая система призвана способствовать долгосрочному и устойчивому подходу к принятию решений в области обеспечение функционала ИТКС, ОИБ и ОФУ ИТКС организации. СУА ИТКС может способствовать более полному пониманию активов, их производительности, рисков, связанных с УА ИТКС, требуемых инвестиций и ценности активов ИТКС, что важно в качестве исходных данных для принятия решений и стратегического планирования организации.

Для результативного и эффективного функционирования СУА ИТКС организации необходимо решить следующие задачи:

25 Циклическая модель улучшения процессов Шухарта-Деминга, или цикл, PDCA: от англ. Plan-Do-Check-Act – «планируй – выполняй – проверяй –действуй».

- определить, документально оформить и поддерживать в актуальном состоянии организационную структуру и состав ее элементов, отразив подчиненность руководства СУА ИТКС и их основные функции;
- определить состав процессов СУА ИТКС и документально оформить схему их взаимодействия;
- определить состав и разработать процедуры, включая документированные, с учетом требований, применяемых организацией стандартов на системы управления и потребностей самой организации.

Согласно ГОСТ Р 55.0.0Х и ГОСТ Р 55235.Х, помимо соответствующей деятельности СУА, включает в себя все необходимые политики, планы, процессы, средства и ресурсы, которые интегрируются для обеспечения гарантии, что деятельность по УА будет осуществлена. Структура и состав элементов СУА ИТКС определяются ее предназначением и целями УА ИТКС, организационной структурой, используемыми ресурсами и процессами, которые реализуются при УА ИТКС для достижения основных бизнес-целей организации.

СУА ИТКС должна быть обязательно интегрирована в структуру общего управления и управления рисками, включая управление рисками ИБ, организации (рис. 1).

Рис. 1. Взаимоотношение между управлением организацией и УА, СУА и портфелем активов ИТКС

Область применения (действия) СУА ИТКС предполагает определение ее границы (рамки) и объема использования и должна быть задокументирована. Такая область следует из СПУА ИТКС и ПолУА ИТКС и согласована с этими документами. Область применения СУА ИТКС необходимо определять для того, чтобы все значимые с точки зрения ОИБ активы ИТКС были приняты в расчет, а исключения некоторых активов из этой области должным образом обоснованы.

При определении области применения СУА ИТКС организация должна учитывать следующее:

- внешние и внутренние обстоятельства (контекст организации), включая, например, масштабы, компоновку и функциональные связи активов, участвующих в предоставлении сервиса клиентам или другим заинтересованным сторонам, а также структурные части организации, местоположение активов ИТКС и договорные условия;
- требования заинтересованных сторон в отношении УА ИТКС;
- взаимодействие с другими системами управления (при их использовании);
- портфель активов ИТКС (англ. *asset portfolio*) – активы ИТКС, включенные в область применения СУА ИТКС. СУА ИТКС может охватывать множество портфелей активов ИТКС. Портфели для физических активов могут быть отнесены к различным категориям (например, завод, оборудование, инструменты). Портфели ПО могут определяться по разработчику или по платформе (например, персональный компьютер, сервер, мэйнфрейм).

Схема планирования и внедрения элементов СУА ИТКС представлена на рис. 2, на котором показано важное значение этих двух процессов, обеспечивающих взаимодействие верхних и нижних уровней СУА ИТКС.

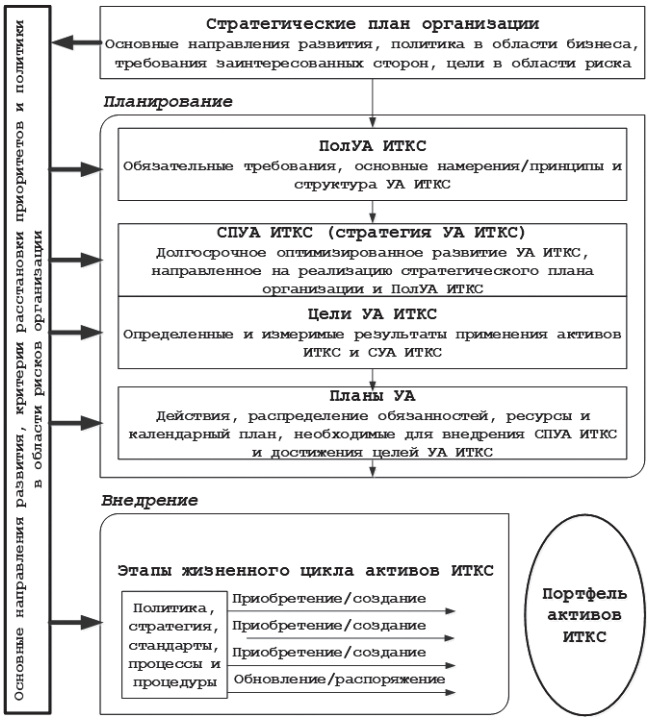

Рис. 2. Схема планирования и внедрения элементов СУА ИТКС

Долгосрочный оптимизированный ***стратегический план УА (СПУА) ИТКС организации***, иначе стратегия УА ИТКС, детализирует цели УА ИТКС, объясняет

их связь с целями организации и концептуальной моделью, необходимой для достижения целей УА ИТКС. Оптимизация распространяется на три составляющие: требуемые вмешательства (затраты, доходы, риск, план-график действий с активами), жизненный цикл актива ИТКС (затраты, производительность, риск, устойчивое развитие) с индивидуальными для отдельных активов планами по полному жизненному циклу и для интеграции систем активов с устойчивым повышением производительности и эффективности, а также программы действий (затраты, доходы, риск, план-график).

Стратегический план организации и СПУА ИТКС, используемые для долгосрочного планирования, должны быть связаны и согласованы, и созданы в рамках итеративного процесса. Цели организации разрабатываются согласно деятельности организации по УА ИТКС, а исходными данными для установления реалистичных и достижимых целей организации могут быть свойства активов ИТКС (например, их мощность и производительность) и результаты деятельности по УА ИТКС (например, планы УА).

СПУА ИТКС на верхнем уровне управления делает следующее:

- преобразует цели организации в цели УА ИТКС;
- идентифицирует и определяет процессы, которые организация использует для установления критериев принятия решений, связанных с активами ИТКС;
- предоставляет руководящие указания для разработки планов УА, в которых указываются действия на уровне активов ИТКС.

Планы УА ИТКС организации формулируют задачи, обеспечивающие выполнение каждой цели УА ИТКС, и содержат обоснование предполагаемых мероприятий по УА ИТКС, включая сами мероприятия, и описание целей, для достижения которых они предназначены, планы эксплуатации, технического обслуживания, капитальных инвестиций (капитальный ремонт, реконструкция, замена, модернизация и списание), а также финансовый и ресурсный планы.

Помимо прочего, СПУА ИТКС должен включать в себя принятую стратегию внедрения ПолУА ИТКС.

Политика УА (ПолУА) ИТКС – это краткое заявление с изложением принципов, с помощью которых организация намерена применять УА ИТКС для достижения своих целей. ПолУА ИТКС выражает общие намерения высшего руководства в отношении активов ИТКС, СУА ИТКС и всей деятельности по УА ИТКС и не относится к конкретным экземплярам активов. ПолУА ИТКС соответствует предназначению организации, согласована с ее целями, разрабатывается на основе стратегического плана организации, действует на высшем уровне и соответствует другим политикам организации, таким как корпоративная политика, политика управления безопасностью труда и охраной здоровья, политика управления качеством, политика управления рисками и политика финансового управления и отчетности. Эта политика устанавливается и утверждается высшим руководством для демонстрирования его заинтересованности и ответственного отношения к УА ИТКС в поддержку достижения целей организации. Кроме этого, ПолУА ИТКС должна включать положение о соответствии законодательным, обязательным и иным требованиям, предъявляемым к организации и принимаемым ею.

ПолУА ИТКС разрабатывается с учетом классификации активов ИТКС. Она содержит обязательства организации и ее ожидания в отношении постоянного улучшения активов ИТКС, УА ИТКС и СУА ИТКС.

Необходимо отметить, что результаты идентификации активов в контексте ОИБ должны быть отражены в Политике ОИБ ИТКС, а результаты идентификации активов в контексте ОФУ – в Стратегии готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса организации, в состав которой входит ИТКС.

6. Краткая инструкция по реализации процесса управления активами ИТКС

Обобщим вышеизложенное применительно к ПУА ИТКС организации в виде следующей краткой пошаговой инструкции, включающей в себя двадцать ключевых мероприятий.

1. Составьте перечень всех активов ИТКС (название, серийный номер, модель, локация...) вручную и автоматизировано.
2. Распределите активы ИТКС по категориям в зависимости от типа (компьютеры/серверы/сетевое оборудование/хранилище/ПО...) и местоположения (офис1/офис2/центр обработки данных...).
3. Определите подразделения, ответственные за каждый актив ИТКС, и их владельцев.
4. Проанализируйте жизненный цикл каждого актива ИТКС (история использования, производительности, технического обслуживания и ожидаемый срок службы).
5. Выполните оценку рисков ИБ для каждого актива ИТКС (уязвимость, угрозы ИБ, потенциальные последствия отказа активов, соответствие нормативным требованиям, выбор подходящих мер ОИБ и обеспечение функциональной устойчивости).
6. Подготовьте финансовый анализ активов ИТКС (стоимость приобретения, амортизация (износ), затраты на техническое обслуживание и т.п, в итоге получив общую стоимость каждого актива).

7. Создайте ПолУА ИТКС с руководящими принципами, ограничениями и ответственностью (должное использование, злоупотребления, НСД и т.п.).
8. Утвердите ПолУА ИТКС.
9. Отслеживайте и записывайте изменения в активах ИТКС (история состояний, изменений и техобслуживания, включая модернизацию, ремонт или перемещение).
10. Регулярно проводите аудит активов ИТКС (с предварительной самооценкой), чтобы идентифицировать любые пропавшие, поврежденные или несанкционированные активы и предпринять необходимые действия для устранения выявленных несоответствий.
11. Регулярно готовьте отчеты по активам ИТКС для обобщения ключевых показателей и информации по активам, включая их состояние, финансовый анализ, статистику использования и результаты оценки рисков ИБ.
12. Выработайте рекомендации по оптимизации активов ИТКС для максимизации их ценности и обеспечения их соответствия целям организации (за счет повышения эффективности и общей окупаемости инвестиций в активы и сокращения времени их простоя).
13. Утвердите рекомендации по оптимизации активов ИТКС.
14. Внедрите утвержденные стратегии оптимизации активов ИТКС и проводите мониторинг их внедрения.
15. Выведите из эксплуатации, замените или модернизируйте устаревшие активы ИТКС.
16. Удалите (сотрите, уничтожьте, переработайте) вышедшие из эксплуатации активы ИТКС защищенным образом.
17. Регулярно пересматривайте и обновляйте ПолУА ИТКС, чтобы соответствовать развивающимся и возникающим технологиям, мерам ОИБ и потребностям организации.
18. Утвердите обновленную ПолУА ИТКС.
19. Обучайте политикам, руководящим принципам и передовой практике УА ИТКС сотрудников организации, что снизит риски и повысит соответствие требованиям и общую эффективность УА ИТКС.
20. Создайте систему, позволяющую сотрудникам немедленно сообщать о проблемах с активами ИТКС (по электронной почте или иным образом).

Выводы

На основе специально подобранной нормативной базы в статье вводится понятийная база УА ИТКС и систематизируются подходы к УА ИТКС организаций как обязательному этапу управления их уязвимостями с целью последующего исключения возможности эксплуатации (использования) обнаруженных уязвимостей. Выделяются мероприятия, реализуемые в ходе процесса УА ИТКС, и обсуждается состав СУА ИТКС, ориентированный на минимизацию возможности осуществления КА на ИТКС организация. Кратко рассматриваются важные составляющие СУА ИТКС, а именно ее основные документы – СПУА ИТКС, планы УА нижнего уровня и ПолУА ИТКС, предназначенные для достижения целей УА ИТКС.

На основе проведенного исследования с соблюдением принципа разумной достаточности разработаны рекомендации по реализации процесса УА ИТКС организации, в виде краткой пошаговой инструкции, состоящей из двадцати основных мероприятий. Эта инструкция имеет непосредственную практическую значимость для управления сетевой безопасностью ИТКС при решении задач устранения найденных для активов ИТКС уязвимостей, что, в свою очередь, приведет к минимизации возможностей реализации КА на ИТКС организаций, использующих конкретные уязвимости активов.

В заключении можно сделать вывод, что чем более качественно разработаны и спланированы все подпроцессы в рамках УА ИТКС организации и чем более своевременно и грамотно они внедрены и пересматриваются с целью совершенствования в течение жизненного цикла всех активов ИТКС, тем более высок уровень зрелости организации и ее готовность к эффективному управлению сетевой безопасностью ИТКС, включающему в себя такие процессы, как управление рисками ИБ, управление инцидентами ИБ, управление уязвимостями, изменениями, управление конфигурациями, управление непрерывностью бизнеса и киберустойчивостью ИТКС [19-20], поддерживающей его.

Литература

1. *Чичков С. Н. Безопасность информационно-телекоммуникационных сетей // Сборник научных статей 7-й Международной молодежной научной конференции. 2019. Т. 4. С. 279–282.*
2. *Савченко М. Ю. Способы совершения преступлений в сфере компьютерной информации и меры их профилактики // Вестник Краснодарского университета МВД России. 2024. № 2 (62). С. 24–27.*
3. *Григорян Д. К., Кондратенко Е. Н. Характерные особенности современных информационных войн политической направленности // Государственное и муниципальное управление. Ученые записки. 2024. № 2,. С.178–183. DOI: 10.22394/2079-1690-2024-1-2-178-183.*
4. *Беседина В. Актуальные киберугрозы: III квартал 2024 года. 5 ноября 2024 г. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/ (дата обращения: 30.12.2024).*

5. *Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 131–135.*
6. *Башарин А. Атаки на цепочки поставок: какие существуют риски и как от них защититься. 18 сентября 2023. [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Supply-Chain-Attack (дата обращения: 30.12.2024).*
7. *Шерстяных А. С. Фишинг как инструмент социальной инженерии // Материалы XXV международной научно-практической конференции «Актуальные проблемы борьбы с преступность: вопросы теории и практики». В 2-х частях. Часть 2. Красноярск, 2022. С. 299–301. DOI: 10.51980/978-5-7889-0334-7_2022_5_2_299*
8. *Баянов Э. И. Новые модификации программ-шифровальщиков // Материалы XVIII Всероссийской студенческой научно-практической конференции «Первые шаги в науку третьего тысячелетия». Уфа, 2022 С. 98–100.*
9. *Таков А. З. Проблемы обеспечения кибербезопасности в современных цифровых системах // Пробелы в российском законодательстве. Т. 16, № 5, 2023. С. 232–236.*
10. *Милославская Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. М.: Горячая линия – Телеком, 2021. – 432 с.*
11. *Серова Т. С., Филимонцев Д. А. Терминология в выражении структуры и функций дефиниций ключевых понятий в подъязыке сферы информационной безопасности // Вестник ПНИПУ. Проблемы языкознания и педагогики. № 3, 2021. С. 8–23. DOI: 10.15593/2224-9389/2021.3.1*
12. *Ушаков Д. Н. Большой толковый словарь русского языка. М., Стандарт, 2021. 816 с.*
13. *Толстой А. И. Системотехника обеспечения безопасности объектов и информационной сфере // Вопросы кибербезопасности. 2024. № 5 (63). С. 47–57. DOI: 10.21681/2311-3456-2024-5-47-57.*
14. *Пушкин С. Как определить ценность использования актива // МСФО на практике. № 6, 2014. [Электронный ресурс]. – Режим доступа: https://msfo-practice.ru/341197 (дата обращения: 30.12.2024).*
15. *Alkhard A. Leveraging Digital Asset Management and Meta-Data Integration for Enhanced Asset Management // Construction Economics and Building, Vol. 24, No. 3 July 2024. Pp. 76–94. DOI: 10.5130/ajceb.v24i3.8741*
16. *Rijadi S. C. R., Suakanto S. Development of an Information System for Asset Management // JURNAL INOVTEK POLBENG – SERI INFORMATIKA, VOL. 9, No. 2, 2024. Pp. 940–952.*
17. *Будзко В. И., Мельников Д. А., Фомичёв В. М. Основы организации обеспечения информационной безопасности и киберустойчивости в централизованных информационно-телекоммуникационных системах высокой доступности // Радиотехника. 2023. Т. 87, № 2. С. 157–162. DOI: 10.18127/j20729472-201901-08*
18. *Канзюба Е. Д. Обеспечение информационной безопасности и киберустойчивости телекоммуникационных сетей, автоматизированных систем управления // Материалы VI Международной молодежной научно-практической конференции в рамках Десятилетия науки и технологий в Российской Федерации «ЭНЕРГОСТАРТ». Кемерово, 2023. С.405-1 – 405-4.*

INFORMATION AND TELECOMMUNICATION NETWORK ASSET MANAGEMENT AS A MANDATORY STAGE OF THEIR VULNERABILITIES MANAGEMENT

Miloslavskaya N. G.[26], Tolstoy A. I.[27]

Keywords: *information and telecommunication network, asset management, asset management process, asset management system, asset vulnerability management, network security management.*

Purpose of work: *systematization of approaches to organizations' information and telecommunication networks (ITCN) asset management (AM) as a mandatory stage of managing their vulnerabilities for the subsequent elimination of the possibility of exploitation (usage) of identified vulnerabilities within the framework of ITCN network security management and development of brief instructions for the implementation of the ITCN AM process.*

Research methods: *analysis of relevant regulatory documents and scientific publications, conceptual modeling, expert assessment, synthesis of an integrated approach to asset management within the framework of network security management.*

Results obtained: *the article introduces the conceptual framework of the ITCN management system and, based on a specially selected regulatory framework, systematizes approaches to the organization's ITCN AM as a mandatory stage of managing their vulnerabilities with the aim of subsequently eliminating these vulnerabilities. The activities implemented during the ITCN AM process, especially when identifying ITCN assets, are highlighted and the composition of the ITCN AM system (AMS) is discussed, aimed at minimizing the possibility of computer attacks against the organization's ITCN. The main documents of the ITCN AMS are briefly considered, namely the strategic plan of the ITCN AMS, lower-level AM plans and the ITCN AM policy, designed to achieve the goals of the ITCN AM. Based on the research conducted, in compliance*

26 Natalia G. Miloslavskaya, Dr.Sc., Ph.D in Cybersecurity, Associate Professor, Professor of Dep. of Information Security of Banking Systems of National Research Nuclear University MEPhI, Moscow, Russia. E-mail: NGMiloslavskaya@mephi.ru
27 Alexander I. Tolstoy, Ph.D, Associate Professor, Head of Dep. of Information Security of Banking Systems of National Research Nuclear University MEPhI, Moscow, Russia. E-mail: AITolstoj@mephi.ru

with the principle of reasonable sufficiency, a brief step-by-step instruction for implementing the ITCN AM process has been developed.

Practical significance *consists in developing brief instructions for implementing the ITCN AM process, especially the process of identifying ITCN assets, within the framework of ITCN network security management when solving the problems of eliminating vulnerabilities found for ITCN assets, which, in turn, will lead to minimizing the possibilities of implementing computer attacks against the organizations' ITCN.*

References

1. *Chichkov S. N. Bezopasnost' informatsionno-telekommunikatsionnykh setey // Sbornik nauchnykh statey 7-y Mezhdunarodnoy molodezhnoy nauchnoy konferentsii. T. 4, 2019. S. 279–282.*
2. *Savchenko M. YU. Sposoby sovershenіya prestupleniy v sfere komp'yuternoy informatsii i mery ikh profilaktiki // Vestnik Krasnodarskogo universiteta MVD Rossii. № 2(62), 2024. S. 24–27.*
3. *Grigoryan D. K., Kondratenko Ye. N. Kharakternyye osobennosti sovremennykh informatsionnykh voyn politicheskoy napravlennosti // Gosudarstvennoye i munitsipal'noye upravleniye. Uchenyye zapiski. № 2, 2024. S178-183. DOI: 10.22394/2079-1690-2024-1-2-178-183*
4. *Besedina V. Aktual'nyye kiberugrozy: III kvartal 2024 goda. 5 noyabrya 2024 g. [Elektronnyy resurs]. – Rezhim dostupa: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/ (data obrashcheniya: 30.12.2024).*
5. *Yangayeva M. O., Pavlenko N. O. OSINT. Polucheniye kriminalisticheski znachimoy informatsii iz seti Internet // Altayskiy yuridicheskiy vestnik. № 2(3), 2022. S. 131–135.*
6. *Basharin A. Ataki na tsepochki postavok: kakiye sushchestvuyut riski i kak ot nikh zashchitit'sya. 18 sentyabrya 2023. [Elektronnyy resurs]. – Rezhim dostupa: https://www.anti-malware.ru/analytics/Threats_Analysis/Supply-Chain-Attack (data obrashcheniya: 30.12.2024).*
7. *Sherstyanykh A. S. Fishing kak instrument sotsial'noy inzhenerii // Materialy XKHV mezhdunarodnoy nauchno-prakticheskoy konferentsii «Aktual'nyye problemy bor'by s prestupnost': voprosy teorii i praktiki». V 2-kh chastyakh. Chast' 2. Krasnoyarsk, 2022. S. 299–301. DOI: 10.51980/978-5-7889-0334-7_2022_5_2_299*
8. *Bayanov E. I. Novyye modifikatsii programm-shifroval'shchikov // Materialy XVIII Vserossiyskoy studencheskoy nauchno-prakticheskoy konferentsii «Pervyye shagi v nauku tret'yego tysyacheletiya». Ufa, 2022 S. 98–100.*
9. *Takov A. Z. Problemy obespecheniya kiberbezopasnosti v sovremennykh tsifrovykh sistemakh // Probely v rossiyskom zakonodatel'stve. T. 16, № 5, 2023. S. 232–236.*
10. *Miloslavskaya N. G. Nauchnyye osnovy postroyeniya tsentrov upravleniya setevoy bezopasnost'yu v informatsionno-telekommunikatsionnykh setyakh. M.: Goryachaya liniya – Telekom, 2021. – 432 s.*
11. *Serova T. S., Filimontsev D. A. Terminologiya v vyrazhenii struktury i funktsiy definitsiy klyuchevykh ponyatiy v pod"yazyke sfery informatsionnoy bezopasnosti // Vestnik PNIPU. Problemy yazykoznaniya i pedagogiki. № 3, 2021. S. 8-23. DOI: 10.15593/2224-9389/2021.3.1*
12. *Ushakov D. N. Bol'shoy tolkovyy slovar' russkogo yazyka. M., Standart, 2021. 816 s.*
13. *Tolstoy A. I. Sistemotekhnika obespecheniya bezopasnosti ob"yektov i informatsionnoy sfere // Voprosy kiberbezopasnosti. № 5(63), 2024. S. 47–57. DOI: 10.21681/2311-3456-2024-5-47-57.*
14. *Pushkin S. Kak opredelit' tsennost' ispol'zovaniya aktiva // MSFO na praktike. № 6, 2014. [Elektronnyy resurs]. – Rezhim dostupa: https://msfo-practice.ru/341197 (data obrashcheniya: 30.12.2024).*
15. *Alkhard A. Leveraging Digital Asset Management and Meta-Data Integration for Enhanced Asset Management // Construction Economics and Building, Vol. 24, No. 3 July 2024. Pp. 76-94.*
16. *Rijadi S.C.R., Suakanto S. Development of an Information System for Asset Management // JURNAL INOVTEK POLBENG – SERI INFORMATIKA, VOL. 9, No. 2, 2024. Pp. 940–952.*
17. *Budzko V. I., Mel'nikov D. A., Fomichov V. M. Osnovy organizatsii obespecheniya informatsionnoy bezopasnosti i kiberustoychivosti v tsentralizovannykh informatsionno-telekommunikatsionnykh sistemakh vysokoy dostupnosti // Radiotekhnika. 2023. T. 87, № 2. S. 157–162. DOI: 10.18127/j20729472-201901-08*
18. *Kanzyuba Ye. D. Obespecheniye informatsionnoy bezopasnosti i kiberustoychivosti telekommunikatsionnykh setey, avtomatizirovannykh sistem upravleniya // Materialy VI Mezhdunarodnoy molodezhnoy nauchno-prakticheskoy konferentsii v ramkakh Desyatiletiya nauki i tekhnologiy v Rossiyskoy Federatsii «ENERGOSTART». Kemerovo, 2023. S. 405-1 – 405-4.*