Александр В. Барабанов[1], Алексей С. Марков[2], Валентин Л. Цирлов[3]
[1, 2]Московский государственный технический университет имени Н.Э. Баумана,
ул. 2-я Бауманская, 5, г. Москва, 105005, Россия
[3]Научно-производственное объединение «Эшелон»,
ул. Электрозаводская, 24, г. Москва, 107023, Россия
[1]e-mail: mail@cnpo.ru, https://orcid.org/0000-0003-4061-6611
[2]e-mail: a.markov@npo-echelon.ru, https://orcid.org/0000-0003-0111-7377
[3]e-mail: v.tsirlov@bmstu.ru, https://orcid.org/0000-0003-2657-4179

О СИСТЕМАТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦЕПЕЙ ПОСТАВКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2019.3.06

Аннотация. В работе представлены результаты систематизации мер защиты информационных ресурсов от компьютерных атак на цепи поставок программного обеспечения и программно-аппаратных комплексов. Отмечены феномены, актуальность и востребованность тематики защиты цепей поставки ИТ-продукции. Приведена статистика по заимствованным компонентам программной продукции и программных комплексов. Приведены примеры компьютерных атак на ресурсы и процессы цепи поставок программного обеспечения. Проведен анализ существующей терминологической базы в области безопасности цепей поставок программного обеспечения. Сформулированы основные свойства, характерные для терминов «цепь поставок» и «атака на цепь поставок». Проведен анализ существующих моделей угроз информационной безопасности, связанных с компьютерными атаками на цепи поставок программной продукции. Выявлены ограничения моделей угроз информационной безопасности цепи поставок программного обеспечения. Выполнен обзор и систематизация мер защиты информации от угроз информационной сферы, связанных с компьютерными атаками на цепи поставок программного обеспечения. Рассмотрены известные нормативные и методическое документы в области цепи поставок ИТ-продукции. Сделан вывод о необходимости развития российской законодательной и нормативно-правовой базы информационной безопасности по тематике цепей поставок программного обеспечения. Предложен вариант систематики мер защиты информации в жизненном цикле поставки программного обеспечения информационных систем. Предложены признаки классификации, как-то: используемые механизмы безопасности, методы защиты информации, фазы процесса разработки программного обеспечения. Сформулированы возможные направления совершенствования мер защиты информации от компьютерных атак на цепи поставок программного обеспечения в национальной и международной сфере информационной безопасности.

Ключевые слова: логистическая цепочка, цепочка поставки, атаки на цепь поставки, информационная безопасность, поставка программ, менеджмент безопасной цепи поставки, таксономия угроз информационной безопасности, систематика мер защиты информации.
Для цитирования: БАРАБАНОВ, Александр В.; МАРКОВ, Алексей С.; ЦИРЛОВ, Валентин Л. О СИСТЕМАТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦЕПЕЙ ПОСТАВКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 68-79, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1218>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.06.

Alexander V. Barabanov[1], Alexey S. Markov[2], Valentin L. Tsirlov[3]
[1, 2]Bauman Moscow State Technical University,
2-nd Baumanskaya, 5, Moscow, 105005, Russia
[2]NPO Echelon, Elektrozavodskaya, 24, Moscow, 107023, Russia
[1]e-mail: mail@cnpo.ru, https://orcid.org/0000-0003-4061-6611
[2]e-mail: a.markov@npo-echelon.ru, https://orcid.org/0000-0003-0111-7377
[3]e-mail: v.tsirlov@bmstu.ru, https://orcid.org/0000-0003-2657-4179

Information security systematics of software supply chains

DOI: http://dx.doi.org/10.26583/bit.2019.3.06

Abstract. The results of the systematization of measures to protect information resources from attacks on the supply chain of software and computer systems are presented. The phenomena, relevance and popular topics of protecting the supply chains of IT products are noted. Statistics on borrowed components of software products and software systems are presented. Examples of computer attacks on resources and processes of the software supply chain are given. The analysis of the existing terminological base in the field of security of supply chains of software is carried out. The features of the terms for supply chain and supply chain attack are formulated. The analysis of existing models of information security threats associated with computer attacks on the supply chain of software products is done. Limitations of models of threats to information security of the software supply chain are revealed. A review and systematization of measures to protect information from threats in the information sphere related to computer attacks on the software supply chain has been carried out. Known regulatory and methodological documents in the field of the supply chain of IT products are considered. It is concluded that it is necessary to develop the Russian legislative and regulatory framework for information security on the subject of software supply chains. A version of the systematics of information security measures in the life cycle of software delivery of information systems is proposed. Classification signs such as the used controls, information security methods, phases of the software development process are proposed. Possible directions of improving measures to protect information from computer attacks on the supply chain of software in the national and international information security are formulated.

Keywords: logistics chain, supply chain, supply chain attacks, information security, software delivery, secure supply chain management, threat taxonomy, controls systematics.

For citation: BARABANOV, Alexander V.; MARKOV, Alexey S.; TSIRLOV, Valentin L. Information security systematics of software supply chains. IT Security (Russia), [S.l.], v. 26, n. 3, p. 68-79, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1218>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.06.

Введение

Актуальность тематики информационной безопасности цепей поставки (supply chain) программ определена двумя феноменами: объективным ростом количества заимствованных компонентов (модулей, библиотек) и развитием сетей дистрибуции и логистики ИТ-продуктов. Так, современная статистика показывает, что:

- более половины организаций-разработчиков программного обеспечения привлекают сторонних разработчиков[1];
- более 70% разработчиков используют компоненты свободного программного обеспечения[2];
- встроенное (микропрограммное) обеспечение программно-аппаратных комплексов, как известно, имеет мульти происхождение из многих зарубежных стран (зачастую даже достоверно неустановленным странам).

Что касается современных систем дистрибуции и логистик, то за последнее десятилетие, к сожалению, стало практикой, когда современные интеграторы, завязанные на ряд иерархически выстроенных сторонних организаций (поставщиков и соисполнителей), не могут контролировать промежуточные цепочки подсистем безопасности и их узкие места [1-3].

С учетом настоящих требований по информационной и кибербезопасности конечного потребителя указанные моменты определяют появление проблемной ситуации, в свою очередь касающейся новых, мало изученных пока типов рисков ИБ,

[1] https://codingsans.com/state-of-software-development-2018
[2] https://www.sonatype.com/2019ssc

связанных:

- с появлением взаимного разного рода мультидоступа к информационным ресурсам головного заказчика, интеграторов, множественных соисполнителей и поставщиков;
- с поставкой конечным пользователям программного обеспечения (ПО) с уязвимостями и не декларированными возможностями заимствованных компонент;
- с поставкой конечным пользователям ИТ-продуктов и систем с вредоносными закладками, преднамеренно внесенными на недостаточно контролируемых множественных этапах внедрения и поставки.

Следует отметить, что в настоящее время наблюдается уверенный рост атак на цепи поставок, особенно на нижние уровни иерархии, касающиеся фрилансеров, а также атаки на интернет вещей [4-6]. Востребованность тематики отмечается даже на самом высоком межгосударственном уровне – в резолюции Генеральной ассамблеи ООН A/RES/73/27[3].

В табл. 1 показаны примеры популярных атак на цепи поставок. Примечательно, что ShadowHammer-атака известна еще и тем, что в расшифрованном фрагменте кода было идентифицировано около 200 MAC-адресов устройств, находящихся на территории России. Можно напомнить, что и известная Stuxnet-атака [7] также относится к атакам на логистическую цепочку[4].

Таблица 1. Известные атаки на цепи поставок программ

Наименование атаки	Краткая характеристика	Годы
Triada	Внедрение вредоносного ПО на этапе установки ПО в смартфоны	2016–2019
The Big Hack	Внедрение аппаратной закладки в материнские платы	2018
ShadowHammer	Распространение вредоносного ПО через утилиту ASUS Live Update. Внедрение вредоносного кода было выполнено на этапе компиляции ПО	2018, 2019

Следует указать, что в ряде передовых стран весьма озабочены данной проблемной ситуацией, что выражается в публикации ряда тематических нормативных документов и обзоров (например, [8-10]). В то же время в нашей стране пока отсутствует общий нормативно-методический документ, посвященный именно безопасности информации программного обеспечения в цепи поставок.

Исследованию указанных вопросов и посвящена данная статья.

1. Постановка задачи

Объектом исследования в работе являются цепи поставок ПО в контексте ИБ. Предметом исследования стали элементы систематики угроз ИБ (связанных с возможностью проведения компьютерных атак на цепи поставок ПО) и организационных и технических мер защиты информации от этих угроз. Цель исследования состоит в систематизации существующих мер защиты информации от угроз, связанных с атаками на цепи поставок, и формировании предложений по их совершенствованию. Для достижения поставленной цели в рамках исследования решаются следующие задачи:

- анализ понятийной базы;

[3] https://undocs.org/A/RES/73/27
[4] https://www.kaspersky.com/content/en-global/images/repository/pr/161)Stuxnet_infogr_en_05_640px.png

- обзор существующих моделей угроз, связанных с атаками на цепи поставок;
- обзор и систематизация мер защиты информации от атак на цепи поставок;
- разработки рекомендаций по совершенствованию соответствующих мер защиты информации.

2. Определение терминологической базы цепи поставок

На основании определения MITRE, NIST SP 800-161, ISO 27036-1 и ISO 28000 (ГОСТ Р 53663), под *цепью поставок ПО*, в целом понимают систему ее участников с взаимосвязанным набором ресурсов и процессов, которые вовлечены в жизненный цикл перемещения ПО от исполнителя к конечному клиенту, а именно: проектирование, разработку, производство, поставку, внедрение, сопровождение программ и выполнение сопутствующих услуг. Следует выделить следующие ключевые характеристики цепи поставок (рис.1):

- цель создания цепи поставок – доставка конечным пользователям программного продукта или услуги (например, по схеме «Platform-as-a-Service» или «Software-as-a-Service»);
- наличие связей (оформленных договорными отношениями) между различными организациями (разработчики, логистические центры, центры дистрибуции и сборки), которые выступают в роли поставщика и (или) потребителя;
- наличие двух потоков передачи материалов/услуг: потоки, связанные с созданием продукта из компонентов сторонних поставщиков («Upstream»), и потоки, связанные с поставкой продукта конечным пользователям через сеть дистрибуции («Downstream»);
- в случае многозвеньевой цепи поставки – самый распространенный вариант – одна и та же организация может выступать одновременно в роли потребителя (по отношению к организации, находящейся в цепи ниже) и поставщика (по отношению к организации, находящейся в цепи выше);
- слабая возможность мониторинга потребителем контроля качества поставляемых продуктов и услуг всей цепи поставки в случае многозвеньевых цепей.

В общем случае связь «поставщик – потребитель» направлена на получение потребителем:

- компонентов ПО, которые будут использоваться потребителем для формирования продукта (услуги или системы), передаваемого конечному пользователю или далее по цепи поставки;
- услуги, которая будет использоваться потребителем для формирования продукта (услуги или системы), передаваемого конечному пользователю или далее по цепи поставки.

Компрометирующие злонамеренные действия на процессы и ресурсы цепи поставок в компьютерной среде принято называть компьютерной *атакой на цепь поставок* (supply chain attack). В общем случае основными целями атакующего являются:

- добавление (вставка) недекларированных возможностей, вредоносного ПО, вредоносного аппаратного обеспечения (закладок, имплантов [11, 12]) или ложной (неверной) информации в объекты цепей поставок;
- замена доверенных элементов (компоненты ПО, документация, конфигурационные файлы) на недоверенные;
- несанкционированная модификация поставляемых объектов.

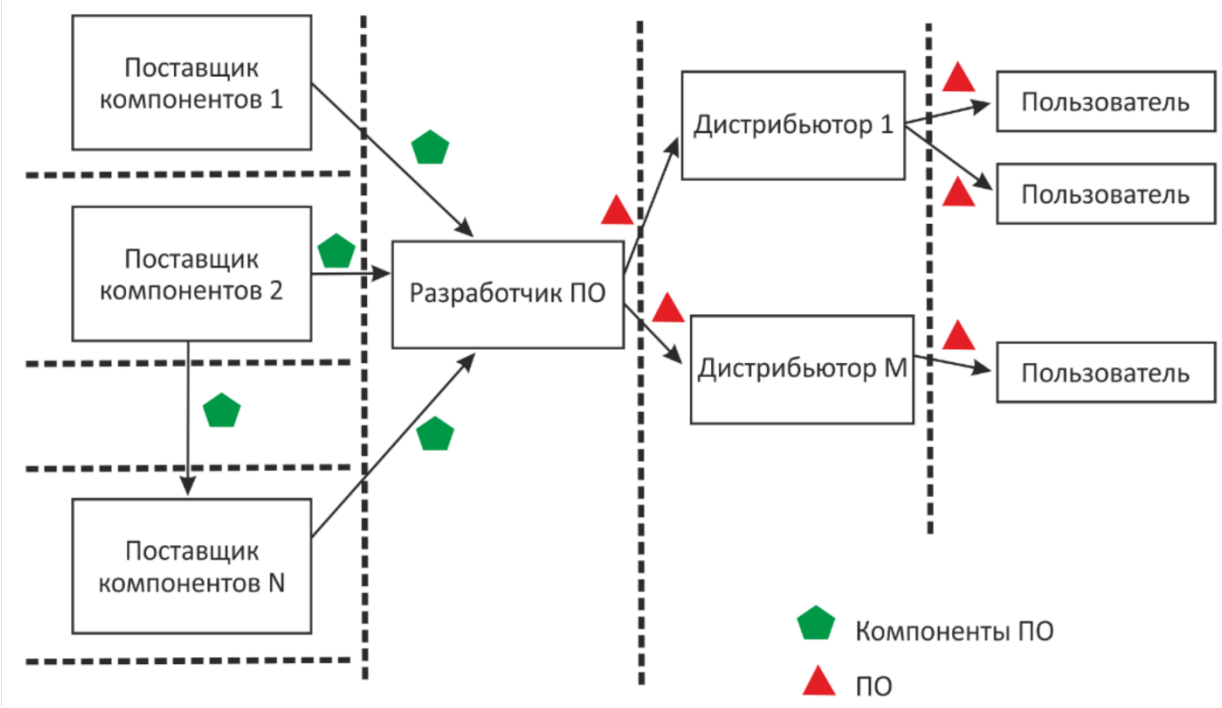

Рис. 1. Типовая структура цепи поставок программ
(Fig. 1. Typical program supply chain structure)

3. Обзор существующих моделей угроз, связанных с атаками на цепи поставок

Решению задачи перечисления угроз, связанных с атаками на цепи поставок, посвящен ряд работ международных научных институтов.

В работе [10] представлены результаты моделирования угрозы для цепей поставок ПО в интересах объектов Минобороны США. Формирование перечня типовых угроз выполнялось с использованием методов анализа и систематизации информации, связанной с реальными инцидентами информационной безопасности, возникшими из-за атак на цепи поставок. Кроме систематизированного перечня (включает в себя 41 наименование), в работе представлены: способ описания угроз и перечень рекомендуемых к внедрению контрмер для нейтрализации идентифицированных угроз. Идентифицированные в работе угрозы связаны с атаками на цепи поставок ПО или преднамеренными действиями нарушителей в среде разработки ПО, - угрозы, связанные с непреднамеренными действиями сотрудников организации – разработчика ПО, не рассматриваются. Следует отметить, что категория «Supply Chain» «Перечня шаблонов атак и их классификации» (Common Attack Pattern Enumeration and Classification, CAPEC[5]) [13] содержит номенклатуру атак на цепи поставок, разработанную на основе публикации [10].

Национальный институт стандартов и технологий NIST разрабатывает перечни угрозы в интересах операторов государственных информационных систем США. В работе [14] представлена номенклатура угроз, актуальных в целом для информационных систем. Отдельная группа из пяти угроз связана с внедрением в информационную систему ПО, содержащего уязвимости или недекларированные возможности, из-за атак на цепи поставок (табл. 2). Следует отметить, что представленная в документе

[5] https://capec.mitre.org

классификация угроз не учитывает особенностей информационных систем, являющихся средами разработки ПО.

Таблица 2. Векторы атак на цепи поставок ПО (по публикации NIST SP 800-30)

Вектор атаки	Краткая характеристика
Создание и задействование ложных организаций с целью внедрения вредоносных компонентов в цепь поставок	Злоумышленник создает ложные организации, имитирующие легитимных поставщиков, которые задействуются в жизненный цикл поставки с целью компрометации компонентов информационной системы в цепи поставки
Внедрение контрафактного или подделанного технического оборудования в цепочку поставок	Злоумышленник перехватывает технические средства у законных поставщиков с целью нелегитимной замены или модификации
Внедрение поддельных критических компонентов в систему организации	Злоумышленник, используя инсайдера и/или цепь поставок, вносит нелегитимные изменения в критические компоненты информационных систем
Проведение атак на цепь поставок, направленных на использование критически важного оборудования, программного обеспечения или встроенного ПО	Злоумышленник проводит атаки на работающие информационные системы путем внедрения вредоносных программ, встроенного программного обеспечения и аппаратного обеспечения, которое выполняет критические функции для организаций
Координация кибератаки с учетом внешних и внутренних (инсайдерских) возможностей и компрометации цепи поставки	Злоумышленник проводит непрерывные (итерационные) скоординированные атаки, используя все три потенциальных вектора атаки (внешние атаки, внутренние атаки, атаки на поставщиков)

Отдельным направлением работы NIST является перечисление угроз, связанных с использованием в информационных системах мобильных устройств [8]. В работе NISTIR 8144 представлены общие сведения о классах таких угроз, приведена методика формирования перечня угроз, используемая специалистами NIST, предложена схема описания угроз по различным характеристикам. Сам каталог угроз доступен в информационной системе NIST[6] в сети интернет. Одной из категорий угроз являются угрозы, связанные с цепями поставки ПО для мобильных устройств и самих мобильных устройств в информационную систему (категория «Supply Chain»). Перечень угроз, представленных в данной категории, по сути, является адаптацией номенклатуры угроз из работы [10] для области мобильных устройств и содержит описание 22 угроз. Угрозы, связанные с непреднамеренными действиями разработчиков или поставщиков приложений для мобильных устройств (например, из-за ошибок или неверного применение практик по разработке безопасного ПО), в работе не рассматриваются.

Описание некоторых угроз, связанных со средой разработки ПО, можно найти в заданиях по безопасности на среду разработки[7] – документах, используемых международной системой сертификации «Common Criteria» при оценке производства объектов сертификации [15]. Перечень угроз, представленный в таких документах, как правило, не является структурированным, а угрозы, связанные с непреднамеренными действиями разработчиков или поставщиков ПО, не рассматриваются.

Следует отметить российские изыскания по линии ТК-362. Информационный ресурс «Банк данных угроз»[8] ведется ФСТЭК России и содержит периодически

[6] https://pages.nist.gov/mobile-threat-catalogue/
[7] https://www.ssi.gouv.fr/uploads/2017/10/anssi-cible-site-2017_07en.pdf
[8] https://bdu.fstec.ru/

обновляемый (в том числе, с учётом анализа реальных инцидентов) классифицированный перечень угроз, предназначенный для операторов и разработчиков информационных систем и используемый ими в процессе моделирования угроз безопасности информации. Угрозы, связанные с атаками на цепи поставок ПО, в явном виде в банке данных не представлены. Национальный стандарт ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения» содержит номенклатуру и описание угроз безопасности информации, которые могут возникать при разработке ПО, в том числе связанных с атаками на инфраструктуру разработчика ПО. Отличительными особенностями данной номенклатуры являются следующие моменты:

- в явном виде указаны угрозы, связанные со средой разработки ПО, реализация которых может привести к внедрению уязвимостей в программу или раскрытию чувствительной информации;
- учитываются непреднамеренные действия разработчиков ПО.

В качестве ограничений всех рассмотренных моделей угроз можно отметить следующие [16]:

- поскольку для угроз при разработке ПО не характерны источники, которые представляют собой физические явления, то рассматриваются только антропогенные угрозы, а угрозы, связанные со стихийными бедствиями, природными явлениями и утечкой информации по техническим каналам, не учитываются;
- представленные перечни угроз, как правило, не являются исчерпывающими и должны быть уточнены в процессе идентификации угроз для конкретной среды разработки ПО или информационной системы.

4. Обзор мер защиты от угроз, связанных с атаками на цепи поставок

В настоящее время наиболее доступны изыскания по тематике безопасности цепей поставки ряда национальных и международных комитетов по стандартизации, среди которых можно выделить US NIST, UK NCSC и ISO.

Так, в публикации NIST - SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations приведен подход к решению задач идентификации, оценки, выбора и внедрения процесса управления рисками, связанными с угрозами информационной безопасности в цепях поставок ПО [17]. Основным содержанием документа являются:

- руководящие указания по внедрению в организацию процесса (гармонизированного с NIST SP 800-39 и NIST SP 800-30) управления рисками, связанными с угрозами безопасности информации в цепях поставок ПО;
- меры защиты информации (в нотации NIST SP 800-53), связанные с защитой от выявленных угроз.

Риск-ориентированный подход, предлагаемый в документе NIST SP 800-161 для оценки рисков, связанных с реализацией угроз из-за атак на цепи поставок, определяется совокупностью фаз [18]:

- определение структуры: сбор требований, определение границ области действия мер по защите цепей поставок;
- оценка: идентификация угроз, оценка рисков информационной безопасности;
- разработка контрмер, связанных с нейтрализацией критичных угроз;
- мониторинг с целью определения эффективности реализованных контрмер.

Технические комитеты Великобритании разрабатывают нормативные и методические документы в области защиты цепей поставок, ориентированные как на

коммерческие, так и на государственные организации. В публикации Supply chain security guidance[9] представлены 12 принципов обеспечения защиты цепей поставок NCSC (UK National Cyber Security Center), среди которых: повышение осведомлённости в области защиты цепей поставок, встраивание мер защиты информации на уровне договорных обязательств, разработка мер, связанных с реагированием на инциденты в цепях поставок. В документе Минобороны Великобритании Defence Cyber Protection Partnership Cyber Security Model Industry Buyer and Supplier Guide[10] представлены указания для потребителей и поставщиков по защите цепей поставок от угроз раскрытия информации, связанной с обороноспособностью Великобритании, на основе риск-ориентированного подхода.

Международные стандарты линейки ISO/IEC 27036 содержат нормативно-методические требования и рекомендации, связанные с защитой информации при взаимодействии класса «поставщик-потребитель». Так, стандарт ISO/IEC 27036-2 предъявляет высокоуровневые требования безопасности информации в случае привлечения к работе субподрядных организаций. Стандарт предлагает использование риск-ориентированного подхода к формированию перечня мер защиты информации. Стандарт ISO/IEC 27036-3 уточняет требования при использовании субподрядных организаций с целью получения услуг (сервисов) или компонентов ПО. В стандарте представлены меры защиты цепей поставок, стандарт гармонизирован с ISO/IEC 27001, ISO/IEC 15288 и ISO/IEC 12207 – меры определены с учетом процессов разработки ПО и систем по ISO/IEC 15288 и ISO/IEC 12207. Следует отметить, что наряду с классическими мерами защиты в последнее время разрабатываются подходы к защите цепей поставки ПО на основе технологии блокчейн [19-21].

Кратко отметим состояние отечественной законодательной и нормативной базы с точки зрения раскрытия вопросов обеспечения безопасности цепей поставок. Например, в доктринных документах нашей страны указаны технологические угрозы со стороны зарубежных стран, но (в отличие, скажем, от Национальной стратегии кибербезопасности США) вопрос безопасности логистических цепочек не фигурирует. В текущих версиях нормативных правовых актов по тематике ГИС, АСУ ТП, КИИ и пр. наблюдается аналогичная ситуация. Национальный стандарт ГОСТ Р 56939 содержит требования к безопасной разработке, а новое положение по сертификации средств защиты информации ужесточает требования к сертификации зарубежной продукции, однако в явном виде вопросы безопасности цепей поставок представлены в них весьма лаконично.

С учетом выше сказанного, проведенное исследование позволило авторам представить на суд читателям вариант систематизации мер защиты информации от угроз, связанных с атаками на цепи поставок (рис. 2).

[9] https://www.ncsc.gov.uk/collection/supply-chain-security
[10] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/718566/20180203_Cyber_Industry_Buyer_and_Supplier_Guide_v2_1.pdf

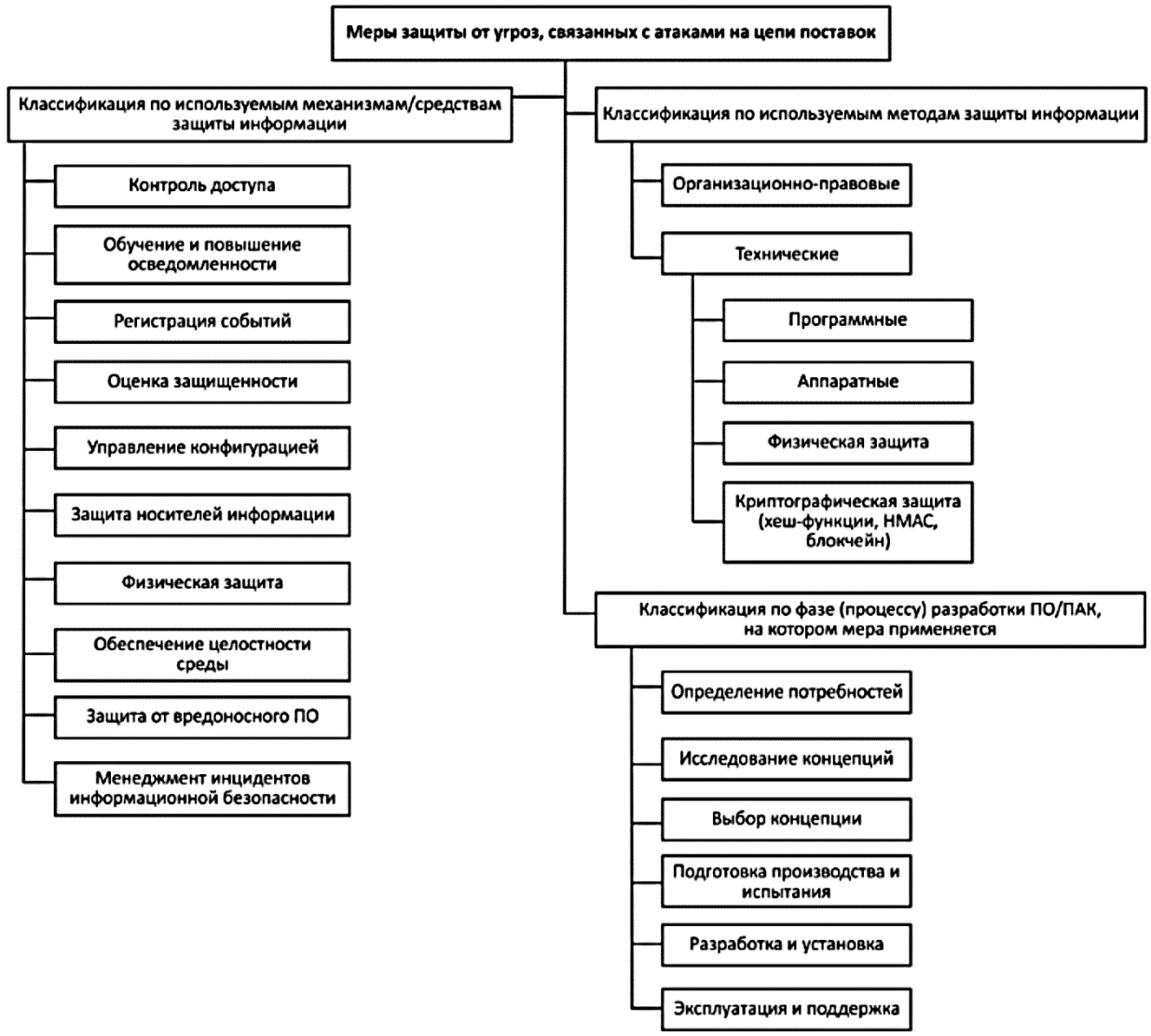

Рис. 2. Результаты систематизации мер защиты информации от угроз, связанных с атаками на цепи поставок
(Fig. 2. Results of systematization of information protection measures against threats related to supply chain attacks)

Заключение

Повсеместное использование цепей поставок ПО и рост инцидентов информационной безопасности, связанных с атаками на них, диктуют необходимость разработки (адаптации существующих) нормативных и методических документов, подходов к защите цепей поставок ПО.

Среди возможных направлений совершенствования в международной сфере можно выделить следующие:

- унификацию законодательства в вопросах борьбы с киберкриминалом, создающим риски, связанные с атаками на цепи поставок;
- формирование этичных норм для использования атак на цепочки поставок в военных целях;
- формирование протоколов обмена информации о подобных угрозах между

странами в рамках военно-политических союзов, таможенных союзов и пр.;

- развитие системы международной сертификации согласно требованиям безопасности: унификации методик проведения сертификационных испытаний, взаимному признанию сертификатов, правилам раскрытия кода и т.п.;
- разработку международного стандарта по управлению рисками информационной безопасности, связанными с атаками на цепочку поставок.

В национальной сфере с учетом высокого уровня зависимости отечественной промышленности от зарубежных информационных технологий можно выделить следующие направления:

- определение на государственном уровне (например, в «Доктрине информационной безопасности») в качестве стратегической цели защиту цепей поставок ПО, предназначенных для функционирования в информационных системах, обрабатывающих сведения, содержащие государственную тайну, критической информационной инфраструктуре, государственных информационных системах;
- формирование рабочей группы с привлечением представителей коммерческих организаций, осуществляющей координацию действий в области обеспечения безопасности цепей поставок;
- формирование и поддержание в актуальном состоянии перечня угроз связанных с атаками на цепи поставок (может быть выполнено в форме национального стандарта по аналогии с угрозами при разработке ПО – ГОСТ Р 58412 или в форме элементов Банка данных угроз ФСТЭК России);
- создание научно обоснованных методов и методик защиты цепей поставок от угроз;
- разработку руководящих указаний по защите цепей поставок ПО для организаций, осуществляющих проектирование информационных систем ГИС, КИИ и пр.;
- разработку руководящих указаний по защите цепей поставок ПО (работа с субподрядчиками) для организаций-разработчиков ПО (может быть выполнено в форме национального стандарта – расширения линейки национальных стандартов в области разработки безопасного ПО) [16, 22];
- формирование протоколов обмена информацией о недобросовестных поставщиках ПО, атаках на цепи поставок и создание национального центра обмена этой информацией и мерах защиты от этих угроз;
- создание и ведение единого хранилища данных о добросовестных поставщиках ПО;
- проведение мероприятий, направленных на повышение осведомлённости организаций в области угроз для цепей поставок (проведение тематических конференций, создание информационных ресурсов).

СПИСОК ЛИТЕРАТУРЫ:

1. Буряк Ю.И., Амирханян В.Г., Калинин В.Л. Обеспечение безопасности цепей поставок промышленной продукции на базе использования современных информационных технологий // Вестник компьютерных и информационных технологий. 2012. № 9 (99). С. 26−33.
2. Погодина В.В., Аристов А.М., Аристов В.М. Проблема обеспечения информационной безопасности логистических процессов на предприятии // Журнал правовых и экономических исследований. 2016. № 3. С. 162−168.
3. Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science. V. 149, 2019. P. 65-70. DOI: 10.1016/j.procs.2019.01.108.
4. Петренко С.А. Управление киберустойчивостью: постановка задачи // Защита информации. Инсайд. 2019. № 3 (87). С. 16−24.
5. Харрис Ш. Кибер войн@. Пятый театр военных действий/Пер. с англ. - М.: Альпина нон-фикшн, 2016. –390 с.

6. Астье Ж.И.; Жуков И.Ю.; Мурашов О.Н. Системы управления «умный дом» и интернет вещей. Безопасность информационных технологий, [S.L.], v. 24, n. 3. P. 18−29, July 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/260 (дата обращения: 01.12.2017). DOI: http://dx.doi.org/10.26583/bit.2017.3.02.
7. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1 (1). С. 28−36. DOI: 10.21681/2311-3456-2013-1-28-36.
8. Brown C., Dog S., Franklin J.M. and etc. Assessing Threats to Mobile Devices & Infrastructure. The Mobile Threat Catalogue. NISTIR 8144 (draft). NIST, 2016. 50 p. DOI: 10.6028/NIST.IR.8144.
9. Miller, J.F. Supply Chain Attack Framework and Attack Patterns. MTR 14-0228. MITRE, 2013. P. 86. URL: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf.
10. Reed M., Miller J.F., Popick P. Supply Chain Attack Patterns: Framework and Catalog. Office of the Deputy Assistant Secretary of Defense, 2014. 88 p. URL: https://www.acq.osd.mil/se/docs/Supply-Chain-WP.pdf (дата обращения: 21.07.2019).
11. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. №2 (3). С. 60−65.
12. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 2. Рабочее место оператора // Вопросы кибербезопасности. 2014. №4 (7). С. 60−68.
13. Yuan X., Nuakoh E.B., Beal J.S., Yu H. Retrieving relevant CAPEC attack patterns for secure software development. In Proceeding of CISR '14 Proceedings of the 9th Annual Cyber and Information Security Research Conference (Oak Ridge, Tennessee, USA, April 08 - 10, 2014). ACM New York, NY, USA, 2014. P. 33−36. DOI: 10.1145/2602087.2602092.
14. Blank R.M. (ed.), Gallagher P.D. (ed.) Guide for Conducting Risk Assessments. NIST SP 800-30, NIST, 2012, Rev.1. 95 p. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата обращения: 21.07.2019).
15. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30−33.
16. Barabanov A., Grishin M., Markov A., Tsirlov V. Current Taxonomy of Information Security Threats in Software Development Life Cycle. In: 2018 IEEE 12th International Conference Application of Information and Communication Technologies (AICT). IEEE (17-19 Oct 2018, Almaty, Kazakhstan). 2018. P. 356−361. DOI: 10.1109/icaict.2018.8747065.
17. Boyens J., Paulsen C., Moorthy R., Bartol N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST SP 800-161. NIST, 2015, 282 p. DOI: 10.6028/NIST.SP.800-161.
18. Sigler K., Shoemaker D., Kohnke A. Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product. Auerbach Publications, 2017. – 278 p.
19. Alzahrani N., Bulusu N. Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 30−35. DOI: 10.1145/3211933.3211939.
20. Hepp T., Wortner P., Schönhals A., Gipp B. Securing Physical Assets on the Blockchain: Linking a novel Object Identification Concept with Distributed Ledgers. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 60−65. DOI: 10.1145/3211933.3211944.
21. Ray S., Chen W., Cammarota R. Protecting the supply chain for automotives and IoTs. In Proceedings of the 55th Annual Design Automation Conference (DAC '18). ACM, New York, NY, USA, 2018. Article 89. P. 1−4. DOI: 10.1145/3195970.3199851.
22. Марков А.С., Цирлов В.Л., Барабанов А.В. Методический аппарат анализа и синтеза комплекса мер разработки безопасного программного обеспечения // Программные продукты и системы. 2015. № 4. С. 166−174. DOI: 10.15827/0236-235X.112.166-174.

REFERENCES:

[1] Buryak YU.I., Amirhanyan V.G., Kalinin V.L. Obespechenie bezopasnosti cepej postavok promyshlennoj produkcii na baze ispol'zovaniya sovremennyh informacionnyh tekhnologij, Vestnik komp'yuternyh i informacionnyh tekhnologij. 2012, n. 9 (99). S. 26−33 (in Russian).
[2] Pogodina V.V., Aristov A.M., Aristov V.M. Problema obespecheniya informacionnoj bezopasnosti logisticheskih processov na predpriyatii, ZHurnal pravovyh i ekonomicheskih issledovanij. 2016, n. 3. S. 162−168 (in Russian).
[3] Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science. V. 149, 2019. P. 65−70. DOI: 10.1016/j.procs.2019.01.108.

[4] Petrenko S.A. Upravlenie kiberustojchivost'yu: postanovka zadachi, Zashchita informacii. Insajd. 2019, n. 3 (87). S. 16−24 (in Russian).
[5] Harris SH. Kiber vojn@. Pyatyj teatr voennyh dejstvij/Per. s angl. -M.: Al'pina non-fikshn, 2016. – 390 s. (in Russia).
[6] Astier J.Y.; Zhukov, I.Y.; Murashov O. N. Smart Building Management Systems and Internet of Things. IT Security, [S.l.], v. 24, n. 3. P. 18−29, july 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/260 (accessed: 01.12.2017). DOI: http://dx.doi.org/10.26583/bit.2017.3.02.
[7] Markov A.S., Fadin A.A. Organizacionno-tekhnicheskie problemy zashchity ot celevyh vredonosnyh programm tipa Stuxnet, Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2013, n. 1 (1). P. 28−36. DOI: 10.21681/2311-3456-2013-1-28-36.
[8] Brown C., Dog S., Franklin J.M. and etc. Assessing Threats to Mobile Devices & Infrastructure. The Mobile Threat Catalogue. NISTIR 8144 (draft). NIST, 2016. 50 p. DOI: 10.6028/NIST.IR.8144.
[9] Miller, J.F. Supply Chain Attack Framework and Attack Patterns. MTR 14-0228. MITRE, 2013. P. 86. URL: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf.
[10] Reed M., Miller J.F., Popick P. Supply Chain Attack Patterns: Framework and Catalog. Office of the Deputy Assistant Secretary of Defense, 2014. 88 p. URL: https://www.acq.osd.mil/se/docs/Supply-Chain-WP.pdf (accessed: 21.07.2019).
[11] Klyanchin A.I. Katalog zakladok ANB (Spigel). CHast' 1. Infrastruktura, Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2014, n. 2 (3). S. 60−65 (in Russian).
[12] Klyanchin A.I. Katalog zakladok ANB (Spigel). CHast' 2. Rabochee mesto operatora, Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2014, N4 (7). S. 60−68 (in Russian).
[13] Yuan X., Nuakoh E.B., Beal J.S., Yu H. Retrieving relevant CAPEC attack patterns for secure software development. In Proceeding of CISR '14 Proceedings of the 9th Annual Cyber and Information Security Research Conference (Oak Ridge, Tennessee, USA, April 08 - 10, 2014). ACM New York, NY, USA, 2014. P. 33−36. DOI: 10.1145/2602087.2602092.
[14] Blank R.M. (ed.), Gallagher P.D. (ed.) Guide for Conducting Risk Assessments. NIST SP 800-30, NIST, 2012, Rev.1. 95 p. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed: 21.07.2019).
[15] Barabanov A.V., Markov A.S., Cirlov V.L. Mezhdunarodnaya sertifikaciya v oblasti informacionnoj bezopasnosti, Standarty i kachestvo *[Standards and Quality]*. 2016, n. 7. S. 30−33 (in Russian).
[16] Barabanov A., Grishin M., Markov A., Tsirlov V. Current Taxonomy of Information Security Threats in Software Development Life Cycle. In: 2018 IEEE 12th International Conference Application of Information and Communication Technologies (AICT). IEEE (17-19 Oct 2018, Almaty, Kazakhstan). 2018. P. 356−361. DOI: 10.1109/icaict.2018.8747065.
[17] Boyens J., Paulsen C., Moorthy R., Bartol N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST SP 800-161. NIST, 2015, 282 p. DOI: 10.6028/NIST.SP.800-161.
[18] Sigler K., Shoemaker D., Kohnke A. Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product. Auerbach Publications, 2017. – 278 p.
[19] Alzahrani N., Bulusu N. Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 30−35. DOI: 10.1145/3211933.3211939.
[20] Hepp T., Wortner P., Schönhals A., Gipp B. Securing Physical Assets on the Blockchain: Linking a novel Object Identification Concept with Distributed Ledgers. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 60−65. DOI: 10.1145/3211933.3211944.
[21] Ray S., Chen W., Cammarota R. Protecting the supply chain for automotives and IoTs. In Proceedings of the 55th Annual Design Automation Conference (DAC '18). ACM, New York, NY, USA, 2018. Article 89. P. 1−4. DOI: 10.1145/3195970.3199851.
[22] Markov A.S., Cirlov V.L., Barabanov A.V. Metodicheskij apparat analiza i sinteza kompleksa mer razrabotki bezopasnogo programmnogo obespecheniya, Programmnye produkty i sistemy *[Software & Systems]*. 2015, n. 4. 166−174. DOI: 10.15827/0236-235X.112.166-174 (in Russian).

Поступила в редакцию – 03 сентября 2019 г. Окончательный вариант – 10 сентября 2019 г.
Received – September 03, 2019. The final version – September 10, 2019.