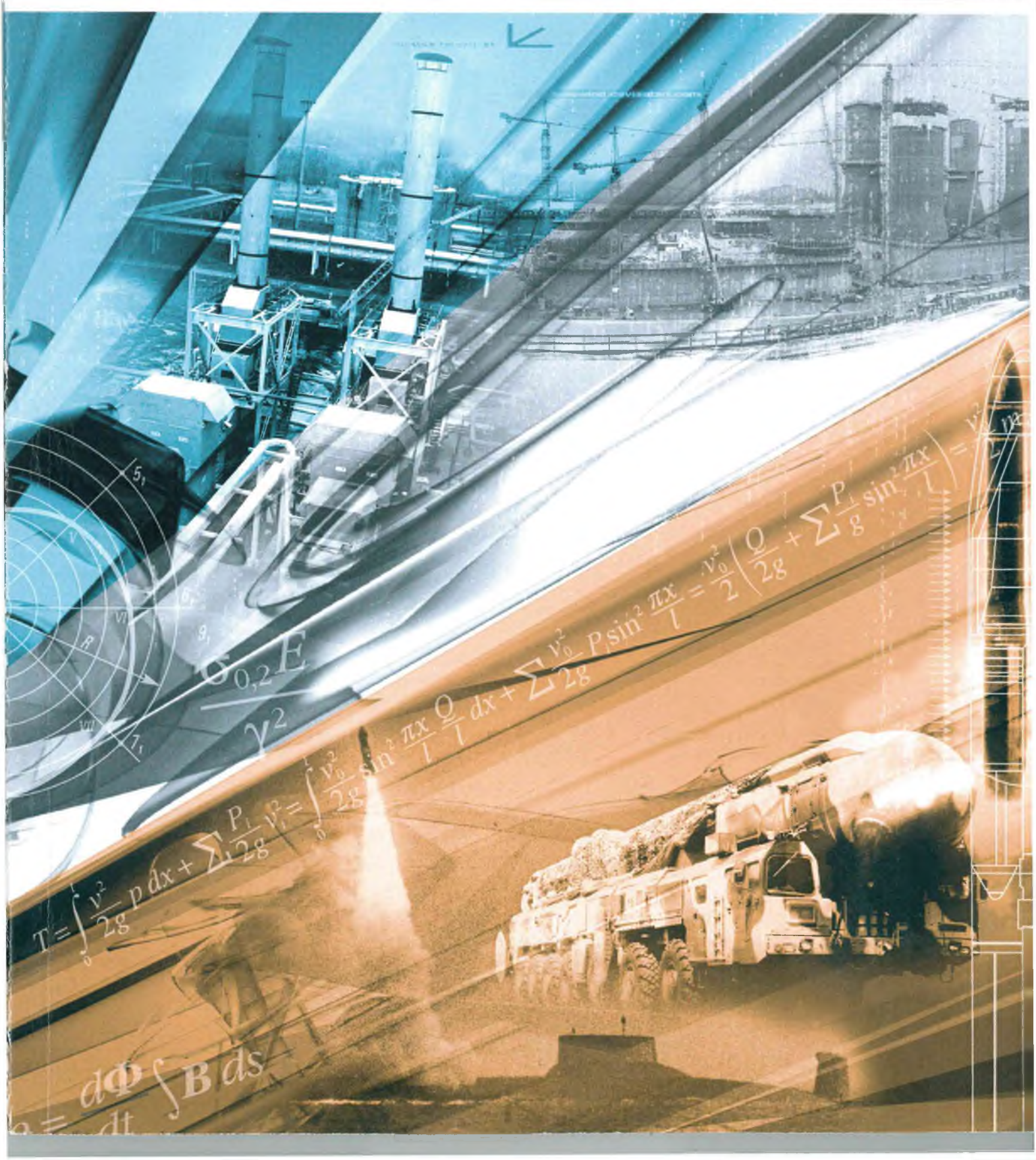
ВОЕННО-ИНЖЕНЕРНАЯ КОРПОРАЦИЯ
РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
Секция «Инженерные проблемы стабильности и конверсии»

ISSN 1680-2780

Двойные технологии

№ 2
2020



ДВОЙНЫЕ ТЕХНОЛОГИИ №2 (91) 2020

Научно-технический журнал
Наукоемкие технологии, проекты двойного использования комплексов вооружений, техногенная и другие виды безопасностей эксплуатации военных систем, экологический мониторинг.

Группы специальностей: авиационная и ракетно-космическая техника (05.07.00); радиотехника и связь (05.12.00); информатика, вычислительная техника и управление (05.13.00) (технические, физико-математические науки).

СОДЕРЖАНИЕ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

Военно-Инженерная Корпорация

АКЦИОНЕРНОЕ ОБЩЕСТВО
«ВОЕННО–ИНЖЕНЕРНАЯ КОРПОРАЦИЯ»

Издается с сентября 1997 г.
Свидетельство о регистрации ПИ №77-3609 от 05.06.2000 г.
ISSN 1680-2780

Выходит 4 раза в год

Журнал включен в «Перечень ведущих периодических изданий» ВАК и систему РИНЦ

УДК 004.056

© Сидак А.А., Василенко В.В., Лыков В.В., Крайнов М.С.
© Sidak A., Vasilenko V., Lykov V., Kraynov M.

АПРОБАЦИЯ МЕТОДИКИ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ. ОПРЕДЕЛЕНИЕ СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ

THE INFORMATION SECURITY THREATS MODELLING METHODOLOGY APPROBATION IN INFORMATION SYSTEMS. IDENTIFICATION OF THREAT SCENARIOS

Аннотация. *В статье проанализированы подходы проекта нового методического документа Федеральной службы по техническому и экспортному контролю «Методика моделирования угроз безопасности информации» к определению сценариев реализации угроз безопасности информации в информационных системах. Проанализированы ограничения существующих практических подходов к описанию сценариев реализации угроз безопасности информации, связанные с неопределенностью учитываемых факторов. Предложены направления их решения с использованием результатов научных исследований и инструментальных средств. Неопределенность при определении сценариев предложено снижать за счет использования проактивного подхода к формированию структуры информационной системы, а также за счет представления сценария как последовательности техник нарушителя в виде цепочки стандартизированных событий безопасности.*

Abstract. *The article analyzes the approaches of the draft new methodological document of the Federal Service for Technical and Export Control «Methodology for Modeling Information Security Threats» to identify scenarios for the implementation of information security threats in information systems. The limitations of existing practical approaches to the description of scenarios for the implementation of information security threats associated with the uncertainty of the factors considered are analyzed. The directions of their solution using the results of scientific research and tools are proposed. It is proposed to reduce the uncertainty in determining scenarios by using a proactive approach to the formation of the information system structure, as well as by presenting the scenario as a sequence of attacker techniques in the form of a chain of standardized security events.*

Ключевые слова. *Угроза безопасности информации, моделирование угроз, сценарий, техника, тактика, цепочка событий безопасности, структуризация, проактивный подход, вид информации, подобие.*

Key words. *Information security threat, threat modeling, scenario, technique, tactic, chain of security events, structuring, proactive approach, type of information, similarity.*

1. Введение

Целевой характер защиты информации (ЗИ) в информационных системах (ИС) предполагает учет и блокирование угроз безопасности информации (БИ) [1, 2].

Ограничения применявшихся до настоящего времени подходов к моделированию угроз БИ были связаны с тем, что последовательность действий нарушителя в информационной инфраструктуре (ИИ) практически не учитывалась, а значит нельзя было в полной мере говорить об эффективности принимаемых мер по ЗИ.

С целью преодоления указанных проблем ФСТЭК России при участии экспертов Центра безопасности информации и других ведущих российских организаций в области информационной безопасности в 2020 г. был подготовлен проект нового методического документа «Методика моделирования угроз безопасности информации» (далее – проект Методики) [3], основанного на современном сценарном подходе к моделированию угроз БИ в ИС [4].

Таким образом, центральной задачей при моделировании угроз БИ стала задача выявления сценариев

Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя ООО «Центр безопасности информации», e-mail: sidak@cbi-info.ru;*
Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации», e-mail: v.vasilenko@cbi-info.ru;*
Лыков Владимир Викторович *– директор департамента, ООО «Центр безопасности информации», e-mail: likov@cbi-info.ru.*
Крайнов Михаил Сергеевич *– ведущий инженер, ООО «Центр безопасности информации», e-mail: kraynov@cbi-info.ru.*

Sidak Aleksey *– candidate of technical science, senior researcher, deputy Chairman, Information Security Center, e-mail: sidak@cbi-info.ru.*
Vasilenko Vladimir *– doctor of technical science, professor, deputy chairman, Information Security Center, e-mail: v.vasilenko@cbi-info.ru;*
Lykov Vladimir *– director of department, Information Security Center, e-mail: likov@cbi-info.ru;*
Kraynov Mikhail *– leading engineer, Information Security Center, e-mail: kraynov@cbi-info.ru.*

реализации угроз БИ в ИИ.

Указанная деятельность предполагает высокоинтеллектуальный труд, направленный на познание процессов в информационной системе, связанных с активностью внутренних и внешних нарушителей.

Таким образом, подходы, положенные в основу проекта Методики, делают актуальной научную проблему сценарного моделирования угроз БИ.

В теоретическом аспекте актуальность материалов настоящей статьи связана с поиском рациональных подходов и технологий, позволяющих наиболее эффективно достигать целей указанной деятельности.

В прикладном аспекте актуальность материалов настоящей статьи связана с необходимостью развития методического обеспечения разработки моделей угроз безопасности информации для информационных систем в соответствии с требованиями нормативных правовых актов и методических документов.

2. Апробация применения проекта Методики при описании сценария реализации угрозы БИ

Проиллюстрируем, как работает сценарный подход в соответствии с проектом методики.

Сценарий реализации угрозы БИ может быть описан на основе тактик и техник, реализуемых нарушителем, список основных из которых приведен в проекте Методики [3] (см. рис. 1).

В качестве примера описания сценария реализации угроз БИ на основе тактик и техник, определенных проектом Методики, приведем описание сценария реализации угрозы фишинговой атаки, направленной на несанкционированную выгрузку защищаемой информации из ИС (см. рис. 2).

На первом этапе реализации угрозы БИ нарушитель передает фишинговое сообщение электронной почты с прикрепленным вредоносным вложением (например, файлом формата PDF, содержащим вредоносный код, запускаемый при открытии файла) на почтовый ящик пользователя ИС. Текст таких сообщений обычно содержит информацию, которая нацелена на то, чтобы пользователь открыл файл, содержащий вредоносный код. Например, в письме может быть написано, что к электронному письму приложен важный файл от конкретного государственного органа (например, требование о погашении налоговой задолженности). Для введения пользователя в заблуждение в поле адреса отправителя может быть подставлен адрес отправителя, который похож на электронный адрес соответствующего государственного органа. Если пользователь откроет приложенный к письму файл, то это неизбежно приведет к запуску вредоносного кода с правами пользователя, который его открыл. Кроме того, по замыслу нарушителя для скрытности вредоносные процессы могут выполняться не сразу, а через значительный промежуток времени, например, через неделю.

В соответствии с проектом Методики описанные действия нарушителя можно отнести к технике (способу) Т2.2. «Использование методов социальной инженерии», которая относится к тактике Т2 «Получение первоначального доступа к компонентам систем и сетей» (см. рис. 2).

На втором этапе реализации угрозы БИ после получения доступа к системе нарушитель может запустить вредоносный процесс, который осуществляет копирование и отправку по собственным протоколам на сервер, принадлежащий нарушителю, защищаемой информации, содержащейся в объектах доступа, права на которые имеет пользователь, открывший файл, прикрепленный к письму, отправленному нарушителем.

В соответствии с проектом Методики описанные действия нарушителя можно отнести к технике (способу) Т9.3. «Отправка данных по собственным протоколам», которая относится к тактике Т9 «Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз» (см. рис. 2).

Как показывают результаты апробации проекта Методики представление угрозы БИ в виде целенаправленного сценария с использованием стандартизированных описаний техник и тактик нарушителя значительно повышает эффективность ЗИ в ИС за счет целенаправленного применения мер и средств ЗИ на различных уровнях (эшелонах) защиты [5].

3. Проблемы существующих подходов к описанию сценариев реализации угрозы БИ

Результаты отечественных исследователей, например, изложенные в работе [6], фактически повторяют зарубежный опыт моделирования сценариев реализации угроз БИ в виде графов атак, узлами которых являются компоненты ИС, а дугами – применение отдельных техник. Проблема такого подхода заключается в отношении «многие-ко-многим» между реализацией угроз БИ (как наступление негативных последствий) и сценариями атак (как совокупности действий нарушителей (тактик)). При этом виды информации (ВИ), являющиеся главным объектом защиты и воздействия в ИС, предметно не рассматриваются в сценарии. Техники, описанные, например, на ресурсе attack.mitre.org, являются лишь примерами, возможными к реализации только в конкретных специфичных условиях определенными группами нарушителей. Таким образом, они не подходят на роль элементов сценариев, которые можно было бы каталогизировать, а впоследствии уточнять для использования в составлении сценариев реализации угроз БИ.

Существуют также международные материалы [7], посвященные использованию известного метода «дерева событий» и построения сценариев, основанных на «дереве событий». Проблема данного подхода – в отношении «одно-ко-многим» между инициирующим сценарий событием и событиями, свидетельствующими о наступлении негативных последствий (то есть реализацией нескольких угроз БИ одновременно).

Таким образом, ограничения и противоречия существующих подходов и результатов исследований не позволяют их эффективно использовать для составления сценариев реализации угроз БИ, когда одной угрозе может соответствовать один или более сценариев («одна-к-одному» или «одна-ко-многим»).

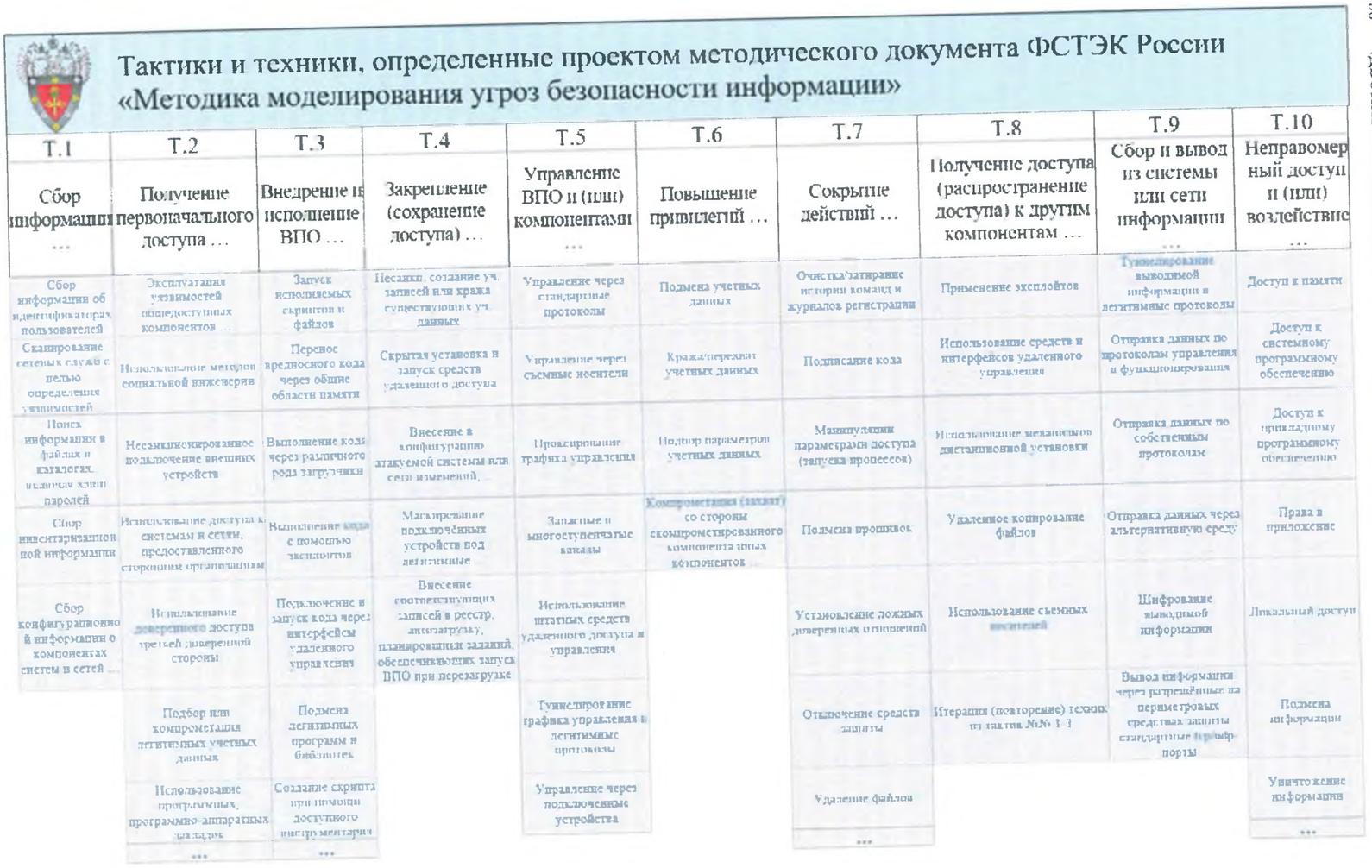


Рис. 1. Тактики и техники нарушителя, определенные проектом Методики

Рис. 2. Сценарий реализации угрозы фишинговой атаки, описанный в терминах тактик и техник

В целях моделирования угроз очень важным является достигнуть именно такого рассмотрения, когда можно четко выделить сценарий реализации конкретной угрозы БИ, абстрагировавшись от иных сценариев и других угроз БИ.

4. Гипотеза решения проблемы описания сценариев реализации угроз БИ

Ограничения и противоречия существующих подходов к описанию сценариев реализации угроз БИ связаны, прежде всего, с неопределенностью следующих факторов:

- структуры ИС;
- информационных активов, подверженных угрозам БИ;
- техник реализации угроз БИ.

Вследствие чего описание сценария реализации угрозы БИ будет обладать большой энтропией, определяемой выражением

$$H=\log\Omega, \quad (1)$$

где Ω – число сочетаний значений указанных выше факторов описания сценария реализации угрозы БИ, приводящих разработчика к выводу об адекватности описания сценария.

Очевидно, что разработка методов снижения неопределенности указанных факторов во многом позволит решить проблему формирования сценариев реализации угроз БИ.

Указанная задача может быть решена на основе гипотезы, что неопределенность факторов формирования сценариев может быть решена путем проактивного формирования структуры ИС [5, 8], а также представления сценария угрозы БИ в виде набора упорядоченных по времени событий безопасности, вызванных действиями нарушителя [4].

Обследование ИС, созданной произвольным образом без достаточного научного обоснования под задачи ЗИ, может не дать точных результатов, а следовательно, и достоверных исходных данных для разработки сценариев реализации угроз БИ. Описания сценариев для похожих ИС могут быть абсолютно бесполезны (практически не осуществимы) для создаваемой ИС.

Формирование структуры ИС на основе научно обоснованной декомпозиции видов информации (методы описаны в работах [5, 8]) позволит иметь четкие исходные данные по распределению информационных активов в ИС и логических точках доступа к ним. Четкая структуризация ИС позволит правильно установить и настроить средства мониторинга информационной безопасности (ИБ) типа NeuroDAT [9], от которых можно будет получить дополнительную инвентаризационную информацию.

Представление сценария как совокупности (цепочки) событий безопасности [4], определенных в соответствии с национальным стандартом ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации», позволит использовать опыт других подобных систем в части определения актуальных угроз БИ (см. работы [8, 10]), а информация об инцидентах в этих системах [9] может стать исходными данными для фрагментов сценариев реализации угроз БИ.

5. Определение сценариев реализации угроз БИ на стадии эксплуатации ИС

Многие сценарии реализации угроз БИ проще определить именно на стадии эксплуатации, так как в ИС применяются различные средства ЗИ, которые могут служить источниками дополнительных исходных данных для сценариев.

Например, для описанного выше сценария реализации угрозы БИ источниками таких данных могут выступать система мониторинга типа NeuroDAT SIEM, средство обнаружения целевых атак типа Kaspersky Anti Targeted Attack и межсетевой экран (МЭ), установленный на границе ИС (см. рис. 3).

Kaspersky Anti Targeted Attack может зарегистрировать события, связанные с попытками передачи на почтовые ящики пользователей ИС писем с прикрепленным вредоносным вложением. Такие события могут стать основанием для того, чтобы учитывать при разработке описания сценария технику нарушителя Т2.2. «Использование методов социальной инженерии».

Агенты NeuroDAT SIEM могут контролировать состав программного обеспечения (ПО) на средствах вычислительной техники, что позволяет выявлять функционирование нештатного ПО, которое предназначено для отправки информации на сервер нарушителя. В свою очередь МЭ, установленный на границе ИС, может зарегистрировать событие отправки этим ПО больших объемов информации. Такая информация может являться основанием для того, чтобы при разработке описания сценария учитывать технику нарушителя Т9.3. «Отправка данных по собственным протоколам».

Кроме того, в связи с тем, что NeuroDAT SIEM имеет возможность интеграции с Kaspersky Anti Targeted Attack и МЭ, в ИС могут быть созданы правила автоматической регистрации инцидентов ИБ, которые при эксплуатации ИС позволят выявлять попытки выполнения таких сценариев реализации угроз БИ и оперативно на них реагировать.

6. Использование общедоступных источников для определения сценариев реализации угроз БИ

Для описания сценариев реализации угроз БИ в соответствии с проектом Методики могут использоваться опубликованные в общедоступных источниках данные о техниках и тактиках нарушителей.

В качестве примера такого источника можно привести базу знаний об известных тактиках и приемах нарушителей безопасности MITRE ATT&CKTM (подробнее см. http://www.cbi-info.ru/groups/page-1306.htm). На рис. 4 проиллюстрирован сценарий реализации угрозы фишинговой атаки в терминах техник и тактик из этой базы знаний.

Наряду с другими, приведенные в настоящей статье примеры моделирования сценариев реализации угроз БИ докладывались экспертами Центра безопасности информации на Конференции «ЦБИ & Kaspersky. Вместе надежней» (г. Москва, 25 февраля 2020 г.).

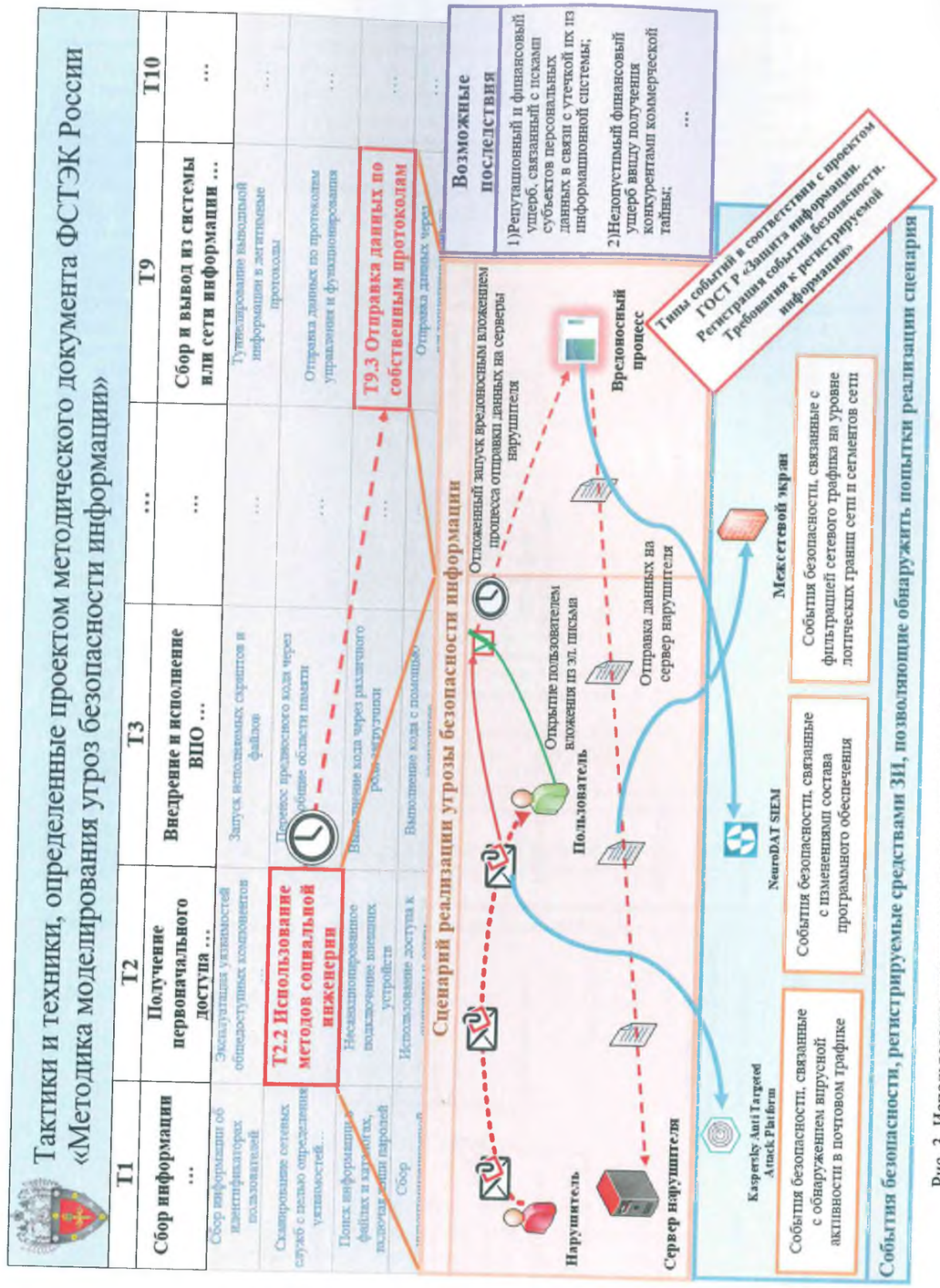


Рис. 3. Использование результатов регистрации событий безопасности для определения сценариев реализации угроз БИ

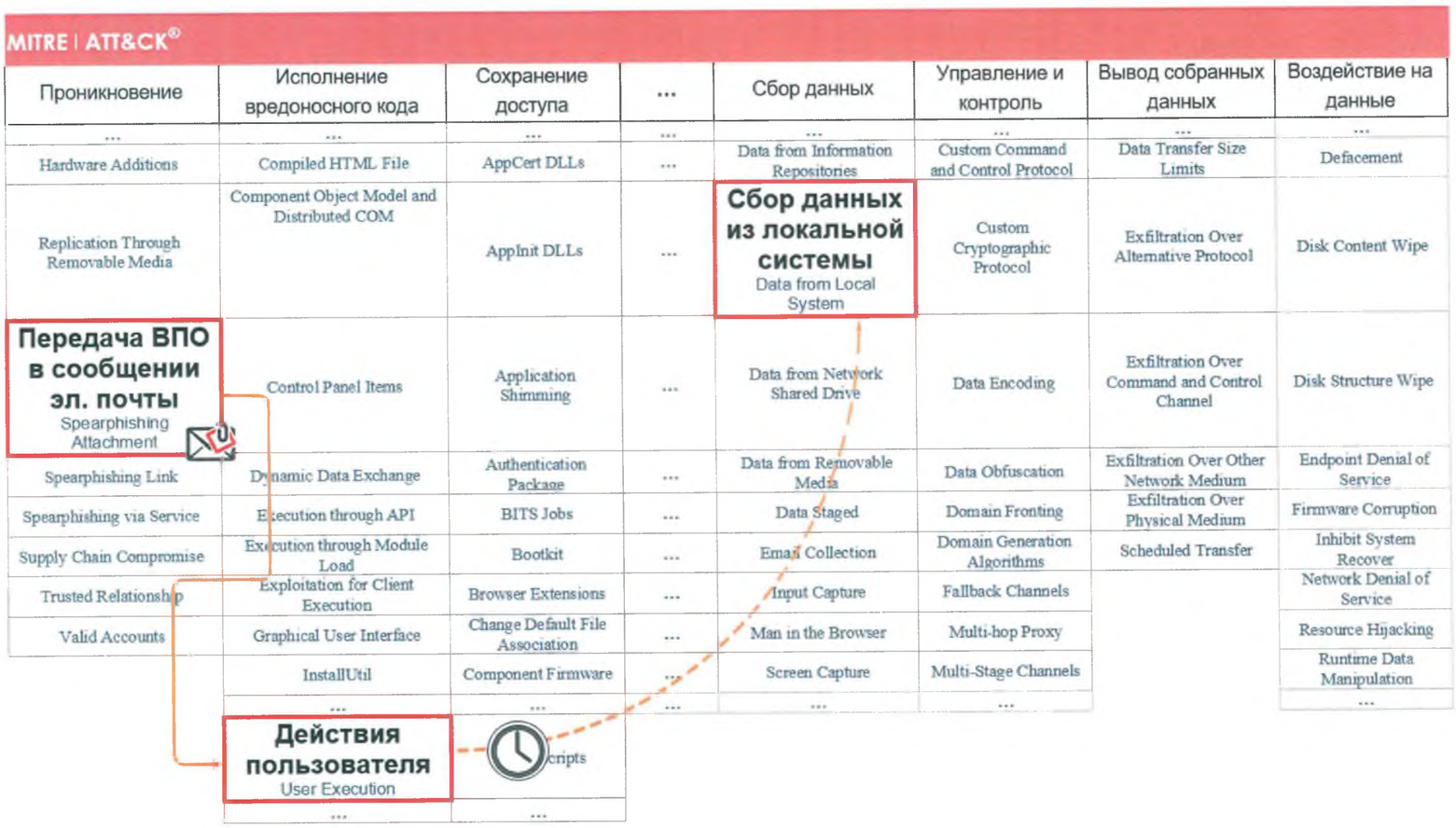


Рис. 4. Сценарий реализации угрозы БИ в терминах ATT&CK MITRE

7. Заключение

Проведенные научные исследования, результаты которых изложены в настоящей статье, были направлены на совершенствование методического обеспечения описания сценариев реализации угроз БИ в целях реализации положений проекта Методики.

Результаты проведенных исследований показали справедливость исходной гипотезы решения проблемы неопределенности факторов при описании сценариев реализации угроз БИ.

По результатам апробации проекта Методики разработаны следующие рекомендации по развитию ее подходов:

- осуществление проактивного формирования структуры ИС, основанного на декомпозиции защищаемых информационных активов (видах информации), с целью априорного получения исходных данных, важных для описания сценария угрозы БИ;
- использование средств мониторинга с целью уточнения инвентаризационной информации, необходимой для описания сценария угрозы;
- использование цепочек событий безопасности (на основе ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации») в качестве основы для описания сценария;
- применение метода подобия для использования результатов описания сценариев реализации угроз БИ для иных (подобных) ИС.

Указанные рекомендации могут быть использованы как непосредственно при моделировании угроз БИ для конкретных ИС, так и при разработке отраслевых (ведомственных, корпоративных) методик моделирования угроз БИ.

На стадии эксплуатации ИС инструментальные средства типа NeuroDAT [9] могут быть использованы для выявления (по регистрируемым и контролируемым событиям безопасности) фрагментов цепочек техник нарушителя для определения новых сценариев реализации угроз БИ, а также (по результатам отработки инцидентов ИБ) для подтверждения актуальности ранее разработанных сценариев реализации угроз БИ.

Литература

1. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», зарегистрирован в Минюсте России 31.05.2013 № 28608 // СПС КонсультантПлюс.

2. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», зарегистрирован в Минюсте России 26.03.2018 № 50524 // СПС КонсультантПлюс.

3. Методический документ ФСТЭК России «Методика моделирования угроз безопасности информации» (проект)// ФСТЭК России: [сайт]. URL: https://fstec.ru/component/attachments/download/2727 (дата обращения: 16.04.2020).

4. Сидак А.А. Решение проблем эквифинальности автоматизированных систем при сценарном подходе моделирования угроз безопасности информации // Двойные технологии. – 2020. – № 1. – С. 89-94.

5. Сидак А.А. Вопросы структуризации автоматизированных систем при организации защиты информации // Информационные войны. – 2018. – № 1. – С. 88-90.

6. Кузнецов Д. Моделирование угроз на основе сценариев или Как Cyber Kill Chain и ATT&CK помогают анализировать угрозы ИБ// Безопасность пользователей в сети Интернет Safe-surf [сайт]. URL: https://safe-surf.ru/specialists/article/5247/626649/ (дата обращения 3.05.2020).

7. IEC 62502:2010 Analysis techniques for dependability – Event tree analysis (ETA).

8. Сидак А.А. Обоснование требований по защите информации в автоматизированных системах // Стратегическая стабильность. – 2009. – № 4 – С. 7–9.

9. Аксенко Ю.И., Васильенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности // Стратегическая стабильность. – 2018. – № 1. – С. 64–67.

10. Сидак А.А. Применение метода подобия при моделировании угроз безопасности информации в автоматизированных системах // Стратегическая стабильность. – 2019. – № 4. – С. 17–20.

Материал поступил в редакцию 23.04. 2020 г.