DOI 10.37882/2223-2966.2024.03.10

ОБ ИСПОЛЬЗОВАНИИ МЕТОДОВ ФОРСАЙТА В ЦЕЛЯХ ПРОГНОЗИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СРЕДНЕСРОЧНЫЙ ПЕРИОД[1]

ON THE USE OF FORESIGHT METHODS IN ORDER TO PREDICT THREATS TO INFORMATION SECURITY IN THE MEDIUM TERM

V. Elin
A. Tsaregorodtsev

Summary. The article reveals the features of constructing medium-term and long-term forecasts, the formation of risks and threats to information security based on the use of the foresight method based on the combination of expert knowledge using feedback and validation, followed by discussion, study and evaluation by experts. During implementation, threat identification at medium-term stages occurs in priority areas that carry out the transfer of content; consideration of the situation from the point of view of the viability of threats and vulnerabilities. The highest-rated schemes are presented in this article.

Keywords: information security, risks and threats to information security, computer attacks, cyber threats.

Елин Владимир Михайлович
Кандидат педагогических наук, доцент, Финансовый университет при Правительстве Российской Федерации; Москва
Доцент, Московский университет МВД России имени В.Я. Кикотя, Москва
elin_vm@mail.ru
Царегородцев Анатолий Валерьевич
Доктор технических наук, профессор, главный научный сотрудник, Финансовый университет при Правительстве Российской Федерации, Москва
academic_tsar@mail.ru

Аннотация. В статье раскрываются особенности построения среднесрочных и долгосрочных прогнозов формирования высокорейтинговых сценариев рисков и угроз информационной безопасности на основе применения методов форсайта в результате объединения экспертных знаний с использованием обратной связи и валидации с последующим обсуждением, изучением и оценкой экспертами. По итогам исследования осуществляется выявление угроз на среднесрочных этапах на основе сценариев по приоритетным направлениям, которые выступают средством передачи содержания; рассмотрение ситуации с точки зрения состоятельности угроз и уязвимостей.

Ключевые слова: информационная безопасность, риски и угрозы информационной безопасности, компьютерные атаки, киберугрозы.

Введение

В настоящей статье анализируется зарубежный опыт построения среднесрочных прогнозов в области информационной безопасности на основании форсайтных методов выявления угроз информационной безопасности и возможность применения представленного опыта в современных российских реалиях.

Вопрос выявления угроз информационной безопасности приобретает особенную актуальность с началом практической деятельности по обеспечению безопасности критической информационной инфраструктуры Российской Федерации[1]. Ряд российских ученых неоднократно высказывался о взаимосвязи атак, угроз, уязвимостей и инцидентов, и их опасности для защищаемых информационных технологий[2]. При этом под угрозой безопасности информации (Infirmation security threat) следует понимать совокупность условий м факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации[3].

[1] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_220885/

[2] Жарова, А. К. Правовое обеспечение атрибуции компьютерных атак / А. К. Жарова // Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности : Сборник докладов участников XVII международного форума, Москва, 18–20 сентября 2023 года. — Москва: Национальная Ассоциация международной информационной безопасности, 2023. — С. 74–78; Другаль, А. О. Обоснование необходимости разработки экспертной системы оценки угроз информационной безопасности / А. О. Другаль, А. В. Царегородцев // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2023. — № 6-2. — С. 68–73. — DOI 10.37882/2223-2982.2023.6-2.13.

[3] ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения / ГОСТ Р № 53114-2008.

[1] Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

Документами стратегического планирования Российской Федерации установлено, что государственная политика обеспечения информационной безопасности формируется в интересах построения безопасной среды достоверной информации, защищенной системы функционирования информационной инфраструктуры в результате развития системы прогнозирования, выявления и предупреждения угроз информационной безопасности, определения источников угроз и оперативной ликвидации последствий угроз[4].

В нашей стране нормативной документацией установлено, что актуальные угрозы безопасности информации оцениваются для функционирующих систем и сетей с заданной архитектурой в целях выявления негативных последствий от реализации угроз; инвентаризации систем и сетей и определения возможных объектов подвергающихся воздействию; оценки способов реализации (возникновения) угроз безопасности и сценариев реализации угроз безопасности информации в системах и сетях[5].

Методологическая база прогнозирования вызовов и угроз информационной безопасности ENISA

В странах Евросоюза применяемая методологическая база прогнозирования вызовов и угроз информационной безопасности ENISA[6] разработана в 2021 году на основании форсайтных исследований, в результате взаимодействия футурологов, социологов, промышленников и предпринимателей, а также специалистов в сфере информационной безопасности. Методика планируется к использованию для построения среднесрочных прогнозов на период до 2030 года. Методика включает в себя 4 этапа исследований: сбор информации (объединение экспертных знаний с использованием обратной связи и валидации), обсуждение, изучение и оценка экспертами («семинары по групповому прогнозированию»), выявление угроз на среднесрочных (до 10 лет) этапах на основе сценариев по приоритетным направлениям, которые выступают средством передачи содержания; рассмотрение ситуации с точки зрения состоятельности угроз и уязвимостей.

Исследование предлагает к рассмотрению 4 категории нарушителей: субъекты, спонсируемые другими государствами, киберпреступники, хакеры по найму и хактивисты. Указанный подход в целом соответствует российской методике, подразделяющей нарушителей на лиц, обладающих базовыми, базовыми повышенными, средними и высокими возможностями.

Использовавшиеся сценарии предполагали акцентировать внимание на наиболее вцысокорейтинговые (по мнению ENISA) угрозы[7]: физическая атака (преднамеренная); непреднамеренный ущерб/потеря информации или ИТ-активов; стихийное бедствие; сбои/неисправности в работе; перебои в работе; подслушивание/перехват; вредоносная деятельность/злоупотребление. В свою очередь, для определения источника угрозы, производилась имплементация каждой угроз с одним или несколькими сценариями, что позволило определить взаимосвязь между сценарием и тенденциями, представленную в таблице 1.

В результате проведенного исследования представлен ряд потенциальных угроз, информационной безопасности, которые рассмотрим далее.

Нарушение цепочки поставок вследствие дефектов программного обеспечения, связанное с использованием библиотек программ с открытым исходным кодом, что приведет к появлению новых и непредвиденных уязвимостей, создавая больше возможностей для злоумышленников скомпрометировать цепочку поставок со стороны поставщика и заказчика. При этом осуществляется реализация 2 и 4 сценариев, в качестве злоумышленников могут выступать спонсируемые государствами группы, а также преступные лица и организации с целями саботажа функционирования информационных систем и хищения значимой компьютерной информации. В качестве примера предлагается сценарий, когда спонсируемые государством субъекты внедряют бэкдор в хорошо известное и популярное онлайн-хранилище кода библиотеки с открытым исходным кодом в целях проникновения в информацию большинства крупных европейских корпораций и используют эту информацию для шантажа лидеров, шпионажа или иного инициирования сбоев в работе по всему ЕС.

Расширенные операции по дезинформации (операции по внедрению (Influence Operations (IO), включающие в себя расширенные (с возможным использованием технологий искусственного интеллекта) возможности преступных группировок, хакеров и правительственных структур с целью манипулирования сообществами с использованием поддельных идентификационных данных на геополитическом уровне. Инструментами таких воздействий, возможно, будут выступать: мошенничество, несанкционированный доступ, перехват сеанса, кража личных данных, идентификации подделок, злоупотребление личными данными.

[4] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»// https://www.consultant.ru/document/cons_doc_LAW_389271/

[5] Методика оценки угроз безопасности информации: Методический документ .Утвержден ФСТЭК России 5 февраля 2021 г.// https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

[6] Foresight on Emerging and Future Cybersecurity Challenges,// ENISA, Ad-Hoc Working Group on Foresight On Emerging And Future Cybersecurity Challenges, 2021.

[7] Threat Landscape Report//ENISA, Threat Landscape Report, 2022

Таблица 1.

Диаграмма взаимосвязи сценария и тенденции

Сценарий 1	Сценарий 2	Сценарий 3	Сценарий 4	Сценарий 5
Более широкое использование новых технологий при дистанционном обслуживании	Снижение количества пресной воды	Усложнение доступа правоохранительных органов к данным, хранящимся в (зашифрованных) сетях, и использовании собранных данных	Растущая зависимость от автоматизации и подключения для устойчивого производства энергии	Растущее внедрение (технического) законодательства в Европе
Использование технологий распределенных реестров	Растущее геополитическое влияние провайдеров связи	Растет число устройств, которые не подвергаются (или не могут подвергаться) регулярному исправлению	Популярность нетрадиционных форм работы, таких как фриланс («gig economy»)	Инфраструктура спутникового управления становится все более важной
Развитие технологии глубокой фальсификации	Возросшая политическая власть негосударственных субъектов	Принятие решений все чаще основывается на автоматизированном анализе данных	Растет популярность спроса и предложения «все как услуга» (XaaS)	Системы на основе искусственного интеллекта все чаще внедряются с предвзятостью или проблемами, влияющими на инклюзивность, безопасность, этику, конфиденциальность, надежность и объяснимость
Возрастает значимость кибербезопасности на выборах	Растет сбор и анализ данных для оценки поведения пользователей, особенно в частном секторе	Проблемы общественного здравоохранения, возникающие из-за проблем с психическим здоровьем жертв кибербезопасности	Автоматизация сельскохозяйственных навыков и рабочей силы	Рост цифрового авторитаризма
Расширение и усовершенствование возможностей подключения нелегального бизнеса	Развитие умных городов	Способность контролировать данные о себе (отдельном лице, компании или государстве) становится все более желательной и технически сложной	Промышленный переход с ископаемого топлива на водород или электричество (спрос)	Массовое вымирание и утрата биоразнообразия продолжаются

Рост авторитаризма в области цифрового наблюдения (потеря конфиденциальности) следует связать с возможностями информационных технологий в сборе персональных данных, таких как сведения о геоданных, потоки данных с камер наблюдения и технологий по распознаванию лиц. Аналитики полагаю, что в дальнейшем свободы личности в Европе могут быть ограничены в целях обеспечения безопасности вследствие усиления цифровой слежки на интернет-платформах или внедрения цифровых удостоверений личности. Центры обработки указанной категории данных могут послужить мишенью для атаки преступных групп, также в связи с тем, что частные корпорации не обеспечивают требования защиты данных и безопасности. Представленная угроза имеет особую значимость для правительственных и частных организаций (включая правоохранительные органы) в рамках государственно-частного партнерства, обрабатывающие биометрические данные, и влечет за собой злоупотребление собранными данными правоохранительными органами или сообществами онлайн-линчевателей для отслеживания потенциальных преступников.

Человеческие ошибки в процессе эксплуатации устаревших элементов в киберфизических системах следует связывать с тем, что с 2030 года Интернет вещей проникнет в значительную часть транспортной, энергетической и водопроводной сетей, а также промышленной инфраструктуры[8] в целях повышения эффективности и совершенствования процесса принятия решений, что повлечет увеличение значимости смарт-устройств, а также систем управления и контроля интернета вещей. Быстрое внедрение Интернета вещей и продолжающаяся нехватка квалифицированных кадров приведут к недостатку знаний, подготовки и понимания киберфизической экосистемы к 2030 году, что приведет к проблемам с обеспечением безопасности, возникающим вследствие неправильной настройки, несвоевременного обслуживания и неадекватной поддержки по окончании срока службы снятого с производства программного обеспечения Интернета вещей. В дополнение к этим проблемам субъекты угроз могут осуществлять интеллектуальные атаки с использованием таких

[8] Указанные категории народного хозяйства в странах Евросоюза формируют элементы критической информационной инфраструктуры согласно положениям "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high general level of security for network and information systems in the Union territory." Euro Lex. July 19, 2016. Retrieved April 26, 2018.

методов, как генеративные состязательные сети (GAN), выражающиеся в использовании уязвимостей серверов с целью срыва запланированных обновлений. Особое значение следует уделять тому обстоятельству, что со стороны конечного пользователя устройствами Интернета вещей часто управляют мобильные устройства с установленными ОС iOS или Android. Конечные пользователи общаются через свои мобильные приложения с интеллектуальных устройств, выступающих частью жилого помещения или транспорта, что дает возможность злоумышленникам получить первоначальный доступ к мобильным устройствам.

Целевые атаки с использованием данных интеллектуальных устройств — при составлении прогноза постулируется возрастание объема данных, характеризующих поведенческие реакции субъектов с использованием интеллектуальных устройств, будут собираться различные категории данных, что позволит составить точный и уникальный поведенческий профиль каждого пользователя. Собранные с применением онлайн платформ данные могут содержать данные о состоянии здоровья, поступающие от носимых устройств и медицинского оборудования или устройств Интернета вещей в умных домах (информацию о поведении дома, данные о передвижении или поведении).

Незаконный доступ к массивам данных позволяет адаптировать атаки социальной инженерии с учетом профиля поведения пользователя. Уровень сложности таких атак социальной инженерии потребует находить новые способы противодействия методам социальной инженерии и улучшения аутентификации.

Недостаточный анализ и контроль инфраструктуры и объектов космического базирования. При построении модели следует исходить из того, что в будущем космический сектор преобразится еще больше благодаря увеличению инвестиций частных субъектов, партнерским отношениям между частными компаниями и правительствами и усилению геополитической и коммерческой конкуренции в космосе. Рынки стимулируют частные компании быстрее внедрять инновации и снижать затраты за счет кибербезопасности. Частные компании могут попытаться использовать это для саботажа конкурентов; правительства могут попытаться использовать уязвимости для создания конкурентного геополитического преимущества в космосе; а преступные группы будут использовать уязвимости для вымогательства у компаний финансовых выгод и создания хаоса. Поскольку правительства и общества в значительной степени зависят от спутников (например, GPS), спонсируемые государством злоумышленники и хакеры по найму будут пытаться получить доступ и к оборудованию наземных узлов, включая базовые станции (т.е. приемопередатчики, которые соединяют спутники и наземные станции в единую сеть) с использованием атак типа «отказ в поддержании обслуживания». Злоумышленники будут использовать доступные методы для обхода механизмов защиты и обнаружения, но останутся бездействующими до тех пор, пока не осуществят свой эксплойт стратегически, например, во время конфликта как средство ведения гибридной войны. Внедрение оружия космического базирования может изменить геополитическую парадигму.

Рост числа продвинутых гибридных угроз. К 2030 году кибератаки станут более изощренными и будут сочетаться с физическими атаками. Методы проведения атак постоянно развиваются и часто комбинируются. При новом способе работы инструментам обнаружения потребуются более широкие возможности корреляции, включая соединение, казалось бы, несвязанных событий. Поэтому они представляют собой растущую проблему как для правительств, компаний, так и для граждан. В прошлом гибридные атаки в основном осуществлялись государственными субъектами как комбинация традиционной и кибервойны. При осуществлении гибридных атак применяются новые технологии и различные типы эксплойтов, чтобы обойти существующие системы реагирования (в т.ч. искусственный интеллект). Злоумышленники будут использовать одновременную комбинацию методов для получения первоначального доступа, включая сбор больших данных для адаптации своих фишинговых кампаний, машинное обучение для интерпретации данных, разработку новых инструментов для обхода защитных механизмов и сочетание физического и виртуального доступа для выполнения своих атак. С ростом числа интеллектуальных устройств, использованием облачных технологий, увеличением количества онлайн-идентификаций и социальных платформ, а также цифровых удостоверений личности, выдаваемых правительствами, у злоумышленников появится множество новых сфер для использования и комбинирования для создания креативных векторов атак.

Нехватка навыков связана с тем, что уже в настоящее время недостаток соответствующих компетенций способствует большинству нарушений информационной безопасности, нанося серьезный урон предприятиям, правительствам и гражданам. К 2030 году проблема нехватки квалифицированных кадров не будет решена. В то время как рост числа незаполненных рабочих мест в сфере кибербезопасности будет по-прежнему представлять значительный риск для общества и правительств. Этот риск будет усугубляться взаимодействием между новыми и устаревшими технологиями, для которых рабочая сила не была подготовлена, поскольку знания об устаревших технологиях передаются недостаточно быстро, чтобы управлять рисками в 2030 году. Преступные группы будут нацеливаться на организации, учреждения и компании, которые имеют большое коли-

чество незаполненных рабочих мест в области информационной безопасности, чтобы находить уязвимости и использовать их для получения финансовой выгоды. Публичные объявления о вакансиях часто содержат подробную информацию о том, каких навыков в настоящее время не хватает в компании или государственном учреждении, что дает злоумышленникам представление о возможных направлениях для атак.

Функционирование трансграничных поставщиков услуг ИКТ, как основание формирования единой точки отказа, следует связывать с тем, что по мере развития информационных технологий граница между физическими процессами и их представлением в киберпространстве будет размыта, поскольку инфраструктурные секторы, такие как транспорт, здравоохранение, электросети и промышленность, все больше полагаются на поставщиков услуг ИКТ для подключения к Интернету и управления коммуникациями между устройствами. Поставщики услуг ИКТ и их инфраструктура — включая спутниковые технологии — являются основой общества и поэтому могут стать единственной точкой отказа. Следовательно, эти поставщики услуг станут мишенью правительств, террористов и преступных группировок. Использование уязвимостей в их инфраструктура, использующая гибридные атаки для получения доступа к их сетям, конечным точкам, центрам обработки данных или другим физическим компонентам инфраструктуры ИКТ, может нанести ущерб городам и целым регионам.

Злоупотребление искусственным интеллектом. Искусственным интеллектом можно манипулировать с момента его создания и на протяжении всего жизненного цикла.

Заключение

Таким образом можно сделать вывод о том, что используемая в странах Евросоюза методика ENISA по применению методов форсайта для выявления потенциальных угроз информационной безопасности с горизонтом планирования около 10 лет является вполне работоспособной и может получить применение при осуществлении практической деятельности в части разработки методического инструментария обеспечения безопасности информационных технологий в России.

ЛИТЕРАТУРА

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_220885/
2. Жарова, А.К. Правовое обеспечение атрибуции компьютерных атак / А.К. Жарова // Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности: Сборник докладов участников XVII международного форума, Москва, 18–20 сентября 2023 года. — Москва: Национальная Ассоциация международной информационной безопасности, 2023. — С. 74–78.
3. Другаль, А.О. Обоснование необходимости разработки экспертной системы оценки угроз информационной безопасности / А.О. Другаль, А.В. Царегородцев // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2023. — № 6-2. — С. 68–73. — DOI 10.37882/2223-2982.2023.6-2.13.
4. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения / ГОСТ Р № 53114-2008.
5. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»// https://www.consultant.ru/document/cons_doc_LAW_389271/
6. Методика оценки угроз безопасности информации: Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.// https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g
7. Foresight on Emerging and Future Cybersecurity Challenges // ENISA, Ad-Hoc Working Group on Foresight On Emerging And Future Cybersecurity Challenges, 2021.
8. Threat Landscape Report//ENISA, Threat Landscape Report, 2022.

© Елин Владимир Михайлович (elin_vm@mail.ru); Царегородцев Анатолий Валерьевич (academic_tsar@mail.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»