УДК 004.056.5(076) DOI:10.31854/1813-324X-2020-6-3-66-74

О сравнении систем защиты информации при асимптотическом управлении информационной безопасностью КИИ

С.Д. Ерохин[1], **А.Н. Петухов**[1, 2*], **П.Л. Пилюгин**[1, 3]

[1]Московский технический университет связи и информатики,
Москва, 111024, Российская Федерация
[2]Московский институт электронной техники,
Москва, 124498, Российская Федерация
[3]Московский государственный университет им. М.В. Ломоносова
Москва, 119991, Российская Федерация
[*]Адрес для переписки: anpetukhov@yandex.ru

Информация о статье
Поступила в редакцию 19.08.2020
Принята к публикации 08.09.2020

Ссылка для цитирования: Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. О сравнении систем защиты информации при асимптотическом управлении информационной безопасностью КИИ // Труды учебных заведений связи. 2020. Т. 6. № 3. С. 66–74. DOI:10.31854/1813-324X-2020-6-3-66-74

Аннотация: *В статье рассматриваются возможности управления безопасностью критических информационных инфраструктур. Предлагаются подходы к построению политики, неориентированной на оценку остаточного риска и фиксированный список угроз. Обосновывается возможность построения управления информационной безопасностью на основе мониторинга событий безопасности. Предлагается формальное описание событий безопасности, механизмов защиты. Вводится отношение порядка для сравнения систем защиты информации и осуществления асимптотического управления информационной безопасностью критических информационных инфраструктур.*

Ключевые слова: *информационная безопасность, политика безопасности, события безопасности, мониторинг событий безопасности, асимптотическое управление, характеристики сетевых событий, критические информационные инфраструктуры.*

Введение

Защищенность в традиционном смысле характеризует эффективность усилий, направленных на противостояние некоторому установленному потенциалу агрессивности среды и выражает достаточность реагирования на возможные воздействия, нарушающее нормальное функционирование защищаемого объекта. Метризация защищенности в рамках рискориентированного подхода строится на основе модели с полным перекрытием Клементса [1], которая рассматривает степень защищенности как априорную характеристику отношений угрозы, актива и защитной меры, а высокоуровневые сущности «Общих критериев» [2, 3, 4] включают параметр «риска» как интегрального остатка от неполной защищенности.

В идеале спецификация агрессии должна включать описание всей причинно-следственной цепочки проявления вредоносного воздействия, а именно «направление вредоносного намерения или потенциала (угроза) – организационно-технический дефект или несовершенство (уязвимость) – последовательность шагов по реализации (атака) – характер ущерба от снижения или утраты информационными активами своей ценности или функциональности (инцидент)». Если предположить гипотетическую возможность исчерпывающего (предельно детального) такого описания, не допускающего вариативности и интерпретации в своих частях, то можно попытаться решить задачу противопоставления специфицированной таким образом агрессии некоторой защитной мерой, обеспечивающей полную защищенность от этой агрессии.

Однако гарантированно исчерпывающе перечислить такие «точечные» описания пока не представляется возможным, поэтому для спецификации агрессии используются обобщающие категории, включающие возможность вариативной интерпретации (в основном, в реализационной части). Таким образом, спецификация вида агрессии объединяет множество различных интерпретаций причинно-следственных цепочек, и нет никаких оснований

утверждать (несмотря на заверения производителя), что противопоставляемые ей защитные меры охватывают и прерывают все интерпретации. Чем больше доля такого охвата, тем выше уровень защищенности. Это полностью соответствует определению защищенности как способности противостоять агрессивному вредоносному воздействию на защищаемый объект.

Для оценки защищенности предлагается использовать вероятность возникновения угрозы и вероятность ее реализации (как правило, без спецификации сценария атаки и других деталей). Эти характеристики носят исключительно экспертный характер (кроме характеристик, связанных с криптостойкостью), и они позволяют рассматривать защищенность как характеристику обратную остаточному риску.

Подход на основе асимптотического управления информационной безопасностью [5] критических информационных инфраструктур (КИИ) предполагает отказ от оценки допустимого (остаточного) риска для измерения эффективности применяемых средств защиты. В связи с этим возникает естественный вопрос о соотношении (хотя бы качественном) достигаемого уровня безопасности при использовании тех или иных защитных мер. При этом для любого суждения о *степени* защищенности (оценка или сопоставление) всегда постулируется «принцип монотонности»: защищенность объекта при совокупном использовании двух любых защитных мер не ниже защищенности при использовании любой из них в отдельности.

В процедуре оценки рисков информационной безопасности ISO 27005 рассматриваются два подхода к оценке риска: качественный и количественный. «Как правило, вначале применяют качественный анализ для выделения высокоприоритетных рисков, а затем уже для выявленных рисков применяют количественный анализ, который является более трудоемким и дает более точные результаты» [6, 7].

Для КИИ асимптотический подход к управлению информационной безопасности (ИБ) использует последовательное улучшение качества системы защиты. Поскольку оценка качества, базирующаяся на измерении в количественных шкалах остаточного риска, в рамках рассматриваемого подхода не применяется, следует использовать качественные (порядковые) шкалы для определения улучшения (направления развития) свойств систем защиты, а это, в свою очередь, требует ввести отношение порядка на множестве всевозможных систем защиты.

Традиционные количественные оценки ущерба также могут быть использованы для определения отношения порядка на множестве всевозможных систем защиты в рассматриваемом асимптотическом подходе к управлению ИБ КИИ. В настоящей работе для устранения описанных выше недостатков традиционной оценки ущерба предлагается альтернативный подход к сравнению качества защиты, основанный на субъектно-объектной модели системы защиты.

В качестве универсальной модели механизма защиты для формализации описания в асимптотическом управлении ИБ используется монитор событий безопасности [8]. В этом случае система защиты рассматривается, как совокупность механизмов защиты из множества $\boldsymbol{M}$, где механизм защиты выполняет две основных функции: обнаружение и противодействие. Для эффективности механизма необходимым является обнаружение, так как необнаруженным событиям нельзя противодействовать. Это позволяет рассматривать множество доступных для наблюдения монитором событий безопасности (из всего пространства таких событий), как основную характеристику механизма защиты [8].

Свойства инцидентов и событий безопасности, используемые в рассматриваемой модели

Событие безопасности в соответствии с ГОСТ РИСО/МЭК ТО 18044-2007 рассматривается как обнаруживаемое монитором (через набор признаков) состояние наблюдаемой системы, которое может привести к возникновению инцидента или просто индицирует возможность его возникновения. В обоих случаях формально это описывалось через корреляционную связь события с инцидентом: «вероятности возникновения события при условии инцидента $\eta = P$ (событие/инцидент есть) и при его отсутствии $\mu = P$ (события/инцидента нет) различны» [9]. Далее будем обозначать $\boldsymbol{A} = \{a_i\}$ множество событий безопасности, обнаруживаемых соответствующими механизмами безопасности из $\boldsymbol{M}$ конкретной системы защиты. Для дальнейшего изложения следует учитывать, что неважно, есть или нет точной оценки этих вероятностей, важно, только, как отмечено выше, чтобы они не были равны, иначе событие не будет информативным.

При этом важно, чтобы события безопасности были независимыми или «почти» независимыми, т. е. слабо корреляционно связаны между собой. Действительно нет никакого смысла наблюдать два события безопасности, если они возникают всегда совместно. Таким образом, события безопасности из группы событий, индицирующих конкретный инцидент, будем считать независимыми или «почти» независимыми. Тогда, исходя из правила добавления только независимых событий, можно считать, что будут независимы и все события из $\boldsymbol{A}$.

Кроме того, события из $\boldsymbol{A}$ будут совместными, так как возможно наблюдение нескольких независимых признаков одновременно или в период наблюдения.

Вместе с тем следует иметь в виду, что событие может индицировать несколько инцидентов. Однако значимость (ценность) такого события для

индикации тем меньше, чем большее число инцидентов им индицируется. Это объясняется тем, что факт наблюдения такого события не дает возможность точно индицировать конкретный инцидент и, соответственно, запускать процедуру конкретного реагирования. Такое событие может использоваться, как правило, для подтверждения опасности и повышения уверенности при наблюдении других событий безопасности. В принципе возможен вариант, когда несколько таких «неоднозначных» событий указывают на один конкретный инцидент (множества индицируемых ими инцидентов в качестве пересечения имеют один элемент). Однако при дальнейшем рассмотрении, будем предполагать (предположение П-1), что таких «неоднозначных» событий безопасности нет.

Под инцидентом $\boldsymbol{I_k}$ будем понимать событие, связанное с нарушением некоторого критического процесса системы, приводящее к прекращению (полному или частичному) функционирования КИИ. В отношении таких инцидентов предполагается:

– во-первых, что сам инцидент также наблюдаем средствами мониторинга (что далеко не всегда возможно, но допустимо для мониторинга ИТКС и сетей электросвязи);

– во-вторых, инцидент в данном случае рассматривается как критическое нарушение функционирования КИИ (или нарушение критического процесса КИИ [10]), это позволяет уточнить общее определение инцидента в ГОСТ РИСО/МЭК ТО 18044-2007, как «нежелательного или неожиданного события(й) ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ [11]»;

– в-третьих, инциденты рассматриваются, как независимые или «почти» независимые события (т. е. слабо корреляционно связанные), так как даже, когда они наступают совместно, структурно они могут соответствовать разным компонентам системы; можно предположить, что в этом случае у них есть общая причина, которая и должна рассматриваться как инцидент;

– в-четвертых, предполагается, что состав инцидентов фиксирован (предположение П-2): для рассматриваемой задачи управления ИБ предполагается, что все критические процессы (возможные инциденты) были идентифицированы ранее в соответствии с инвентаризацией КИИ при категорировании [10]; изменение состава инцидентов возможно на основе получения дополнительной информации, и новому составу инцидентов будет соответствовать новая система защиты информации (СЗИ), улучшать свойства которой можно на основе мониторинга в процессе асимптотического управления.

Последнее обстоятельство подчеркивает кусочно-непрерывный характер процесса асимптотического управления. Текущее функционирование адаптивной составляющей в процессе «непрерывного» периода асимптотического управления накапливает некоторую «критическую массу» оценки прогностической составляющей и может инициировать качественный скачок, связанный с изменением состава инцидентов. Кроме того, изменение номенклатуры (состава и описания) инцидентов может осуществляться извне, например, по каналам взаимодействия с ГосСОПКА.

Сравнение систем защиты информации на основе наблюдаемых событий безопасности

Сравнение СЗИ строится на основе модели системы защиты с полным перекрытием. Однако в предлагаемом подходе происходит ее трансформация этой модели от структуры «угроза – механизм защиты – объект защиты» к структуре «угроза – событие безопасности – механизм защиты – инцидент безопасности – объект защиты». Т. е. вместо тройки (t_i, m_j, o_k) рассматривается тройка (a_i, m_j, I_k), где $\{t_i\}$ – угрозы; $\{m_j\}$ – механизмы; $\{o_k\}$ – объекты; $\{a_i\}$ – события; $\{I_k\}$ – инциденты (рисунок 1).

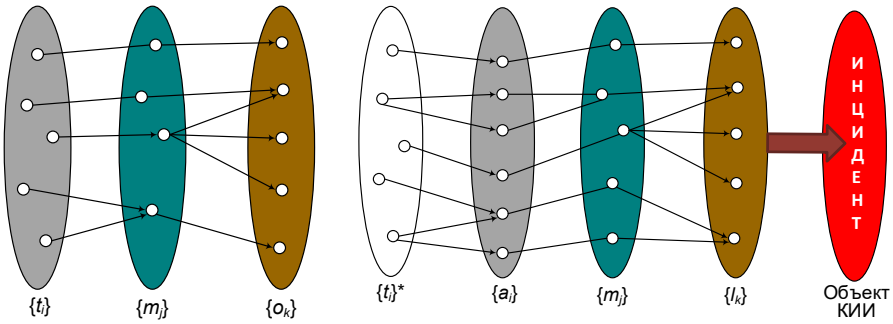

Рис. 1. Трансформация модели с полным перекрытием

Fig. 1. Transformation of the Model with Full Overlap

Для сетевых механизмов защиты (МЭ, IDS, IPS, SIEM и т. д.) в процессе мониторинга индицируются события на основе сигнатур и обнаружения аномалий [12]. Отметим, что понятие сигнатуры событий безопасности рассматривается здесь несколько шире, чем аналогичное понятие, например, в практике антивирусной деятельности (фрагмент программного кода, характерный для вредоносного

ПО). Сигнатура события безопасности (шаблон, паттерн, комплекс признаков и др.) предназначена для обнаружения факта, свидетельствующего, что соответствующее событие или группа событий произошли. Сигнатура может определяться источниками информации о событии (например, сенсоры первичных измерений) и структурой формирования из этой информации более сложных агрегатов, которые соответствуют комплексным событиям, коррелированным с инцидентом безопасности (схема агрегации).

В первом случае можно рассматривать набор (вектор) из n параметров последовательных состояний системы $s_i = (p_1, ... p_n)$, как представление события безопасности (или набора таких событий), описываемых сигнатурой некоторого инцидента I_m. Здесь $(p_1, ... p_n)$, это наборы параметров состояний системы наблюдаемых в различные моменты времени интервала наблюдений, что соответствует приведенным выше определениям события безопасности и инцидента.

Таким образом, мы можем далее рассматривать соответствие наблюдаемых параметров системы сигнатуре как выявление (наблюдение) соответствующих событий безопасности. Т. е. если $\boldsymbol{S} = \{s_i\}$ множество всех возможных сигнатур, то в соответствии с этим уточнением положим $\theta(s_i) \subseteq \boldsymbol{A}$, где θ: $\boldsymbol{S} \rightarrow \boldsymbol{A}$ отображение множества сигнатур на множество событий безопасности. Это отображение может быть не взаимно-однозначным, в этом случае θ^{-1} может рассматриваться как метод агрегирования событий безопасности $\{\theta^{-1}(a_1, ... a_r)\} = \{s_i\}$, а $\{s_i / \theta(s_i) \subseteq \boldsymbol{A}\} \subseteq \boldsymbol{S}$ – как новый набор независимых событий безопасности, описываемых сигнатурами.

Во втором случае монитор позволяет обнаруживать некоторые отклонения от ожидаемого «поведения» системы. При этом следует иметь в виду, что аномалии сетевого трафика могут являться вполне безопасным явлением [13]. Поэтому идентификация аномалий как событий безопасности, соответствующих инцидентам, требует дополнительной фильтрации и обработки получаемых данных [14], причем для этого привлекаются не только вероятностные методы [15]. Такие аномалии, идентифицированные как события безопасности, также отслеживаются монитором на основе соответствующих сигнатур (например, превышение попыток ввода пароля или одновременное открытие большого числа TCP-соединений и т. п.).

Так как далее мониторинг на основе сигнатурного обнаружения событий полагается общей моделью используемых механизмов защиты, то в дальнейшем будем исходить из того, что $\boldsymbol{M} = \{s_i / \theta(s_i) \subseteq \boldsymbol{A}\}$, т. е. все механизмы защиты описываются множеством наблюдаемых ими событий безопасности, что соответствует множеству сигнатур инцидентов. Используя эти утверждения, покажем возможность сравнивать системы защиты, использующие мониторинг на основе сигнатурного обнаружения событий.

Основой для сравнительной оценки эффективности различных СЗИ могут быть множества используемых ими сигнатур событий безопасности $\boldsymbol{S}_k \subseteq \boldsymbol{S}$ (эксплуатационные и архитектурные параметры здесь не рассматриваются). Для того, чтобы сравнить СЗИ, можем сопоставить множества всех событий безопасности СЗИ, устанавливая тем самым на множестве СЗИ отношение частичного порядка. Исходя из этого, далее будут рассмотрены условия введения отношения порядка $\succcurlyeq_S$ на основе сравнения множеств сигнатур СЗИ для группы событий безопасности.

Отношение частичного порядка на множествах сигнатур событий безопасности

Пусть множество инцидентов содержит только один инцидент (предположение П-3) и пусть, как это описано выше, $СЗИ_1$ и $СЗИ_2$ полностью характеризуются их множествами сигнатур: S_1 и S_2, тогда при сравнении множеств сигнатур возможны следующие случаи:

1) $\boldsymbol{S}_1 \supseteq \boldsymbol{S}_2$ или $\boldsymbol{S}_1 \subseteq \boldsymbol{S}_2$ – отношения включения множеств устанавливает для СЗИ (и соответствующих им множеств событий безопасности) отношение предпочтения: $\boldsymbol{S}_1 \succcurlyeq_S \boldsymbol{S}_2$ или $\boldsymbol{S}_1 \preccurlyeq_S \boldsymbol{S}_2$;

2) $\boldsymbol{S}_1 \cap \boldsymbol{S}_2 = \emptyset$ – сравнение на основе включения множеств не применимо;

3) $\boldsymbol{S}_1 \cap \boldsymbol{S}_2 \neq \emptyset$, но $\boldsymbol{S}_1 \not\supseteq \boldsymbol{S}_2$ или $\boldsymbol{S}_1 \not\subseteq \boldsymbol{S}_2$ – сравнение на основе включения множеств также не применимо.

Для повышения безопасности КИИ на основе асимптотического управления [16] первый случай показывает, как последовательное «улучшение» эффективности защиты связано с добавлением новых сигнатур в системы мониторинга. Однако возможно возникновение различных ситуаций, соответствующих случаю 2. Например, при агрегировании нескольких сигнатур в одну (построение сигнатуры-шаблона) или при выявлении (и удалении) «неэффективных» или менее эффективных сигнатур и замены их другими, что особенно важно в случае ограниченности ресурсов. В этом случае рассматриваются не множества сигнатур, а соответствующие им события безопасности (т. е. сигнатура рассматривается как результат агрегирования событий безопасности). Далее сравнение производится, если это возможно, как сравнение множеств. Например, пусть $\boldsymbol{A}_i$ множество событий безопасности, соответствующее множеству сигнатур $\boldsymbol{S}_i$: $\boldsymbol{A}_i = \theta(\boldsymbol{S}_i)$. Если справедливо, что: $\boldsymbol{A}_1 \supset \boldsymbol{A}_2$ или $\boldsymbol{A}_1 \subset \subset \boldsymbol{A}_2$, тогда отношения включения множеств устанавливает для СЗИ (и соответствующих им множеств сигнатур и событий безопасности) отношение предпочтения $\boldsymbol{S}_1 \succcurlyeq_S \boldsymbol{S}_2$ или $\boldsymbol{S}_1 \preccurlyeq_S \boldsymbol{S}_2$.

В других ситуациях возможны различные варианты проведения сравнений, которые не столь очевидны. Если $\boldsymbol{S}_1 \cap \boldsymbol{S}_2 = \emptyset$, то для исключения возможных неточностей также рассматриваем множества соответствующих им событий безопасности. В этом случае также имеем, что $\boldsymbol{A}_1 \cap \boldsymbol{A}_2 = \emptyset$, и для проведения «грубой оценки» множеств сигнатур в качестве метрики множества событий безопасности используем мощность соответствующего множества $\|\boldsymbol{A}_i\| = |\boldsymbol{A}_i|$.

Такой линейной метрике соответствует сложение вероятностей событий безопасности, которое здесь не применимо, так как события хотя и независимы, но совместны. Однако в качестве обоснования такой на первый взгляд тривиальной метрики рассмотрим вероятность $P_I(\boldsymbol{A})$ индицирования инцидента группой $\boldsymbol{A}$ соответствующих ему совместных событий безопасности. Будем предполагать, что все события безопасности одинаково значимы для обнаружения инцидента (предположение П-4), и что вероятности таких событий примерно совпадают. Инцидент индицируется, если происходит обнаружение хотя бы одного события безопасности и, соответственно, $P_I(\boldsymbol{A}) = 1 - P(\bar{\boldsymbol{A}})$, где $P(\bar{\boldsymbol{A}})$ – вероятность того, что не произойдет ни одного события безопасности из $\boldsymbol{A} = (a_1, a_2, \ldots, a_n)$. Тогда $\bar{\boldsymbol{A}} == (\bar{a}_1 \cup \bar{a}_2 \cup \bar{a}_2 \ldots \cup \bar{a}_n)$ – произведение независимых событий и $P(\bar{\boldsymbol{A}}) = \prod_1^n (1 - p(a_i)) = (1-p)^n$, где $p \approx p(a_i)$ вероятности событий a_i, если они равны (или это среднее значение этих вероятностей). Отсюда видно, что $P_I(\boldsymbol{A}) = 1 - (1-p)^n$ при росте n монотонно возрастает.

Очевидно, что при больших количествах событий безопасности n изменения $P_I(\boldsymbol{A})$ будут невелики, и при традиционной оценке остаточных рисков ими можно пренебречь, однако в случае КИИ любое улучшение будет значимым. При этом отметим, что возможно уменьшение показателя степени в функции $P_I(\boldsymbol{A}) = 1 - (1-p)^{n-r}$, где r обозначает минимальное число событий безопасности необходимое для обеспечения нужного качества индикации инцидента в соответствии со схемой последовательных испытаний Бернулли (рисунок 2).

Для определения $\|\boldsymbol{A}_1\| \geqq \|\boldsymbol{A}_2\|$ или $\|\boldsymbol{A}_1\| \leqq \|\boldsymbol{A}_2\|$ можно просто провести сравнение по количеству событий безопасности и, соответственно, получим: $\boldsymbol{S}_1 \succcurlyeq_S \boldsymbol{S}_2$ или $\boldsymbol{S}_1 \preccurlyeq_S \boldsymbol{S}_2$. В случае, если $\boldsymbol{A}_1 \cap \boldsymbol{A}_2 \neq \emptyset$, можно проводить сравнение множеств $\boldsymbol{B}_1 = \boldsymbol{A}_1 \setminus (\boldsymbol{A}_1 \cap \boldsymbol{A}_2)$ и $\boldsymbol{B}_2 = \boldsymbol{A}_2 \setminus (\boldsymbol{A}_1 \cap \boldsymbol{A}_2)$, тогда $\boldsymbol{B}_1 \cap \boldsymbol{B}_2 = \emptyset$ и $\|\boldsymbol{B}_1\| \geqq \|\boldsymbol{B}_2\|$ или $\|\boldsymbol{B}_1\| \leqq \|\boldsymbol{B}_2\|$, и, соответственно, $\boldsymbol{S}_1 \succcurlyeq_S \boldsymbol{S}_2$ или $\boldsymbol{S}_1 \preccurlyeq_S \boldsymbol{S}_2$ (рисунок 3).

С учетом установленных предположений и ограничений для введенного отношения предпочтения $\succcurlyeq_S$ можно утверждать, что:

$$\text{СЗИ}_1 \succcurlyeq_S \text{СЗИ}_2, \text{ если } \boldsymbol{S}_1 \succcurlyeq_S \boldsymbol{S}_2;$$

$$\text{СЗИ}_1 \preccurlyeq_S \text{СЗИ}_2, \text{ если } \boldsymbol{S}_1 \preccurlyeq_S \boldsymbol{S}_2;$$

$$\text{СЗИ}_1 =_S \text{СЗИ}_2, \text{ если } \boldsymbol{S}_1 \succcurlyeq_S \boldsymbol{S}_2 \text{ и } \boldsymbol{S}_1 \preccurlyeq_S \boldsymbol{S}_2.$$

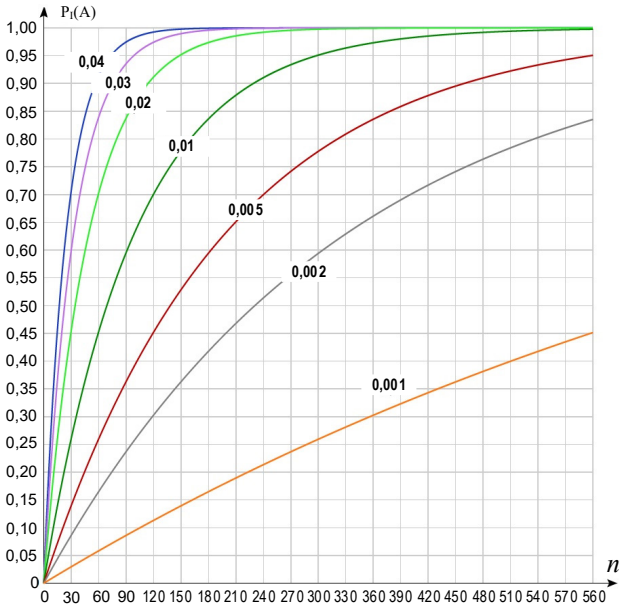

Рис. 2. Изменение характера зависимости $P_I(A)$ вероятности индицирования инцидента от числа наблюдаемых событий безопасности n при различных вероятностях p(0,001 → 0,04) возникновения этих событий

Fig. 2. The Changing of Dependence P_I (A) Probability of Incident Recognition as a Function of the Number of Observed Security Events n for Various Probabilities p (0,001 → 0,04) of These Events Occurring

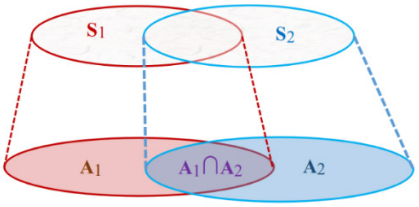

Рис. 3. Общий случай соотношения множества событий безопасности

Fig. 3. The General Case of the Relation of a Set of Security Events

Несмотря на невысокую точность оценок, описанный выше подход обладает примечательным свойством – все СЗИ сравнимы между собой. Однако допущение того (П-4), что значимость всех сигнатур одинакова для индицирования инцидента, является слишком сильным и далеко не всегда корректна, кроме того, введенное отношение позволяет сравнить СЗИ только для одного инцидента.

Отношение частичного порядка на множествах сигнатур событий безопасности для сравнения СЗИ с учетом значимости сигнатур

Более универсальным, более точным (снимающим ограничения предположения (П-4) о равной значимости событий безопасности), однако, трудоемким и, возможно, не всегда технически реализуемым (так как требуется набрать значительный объем статистики) методом является использование корреляционного анализа, применяемого в методах прикладной статистики [17]. Парные или частные коэффициенты корреляции можно рассматривать как коэффициенты значимости в процессе аддитивной свертки критериев, в отличие от

описанной выше свертки с одинаковыми коэффициентами значимости, равными 1. Использование этих коэффициентов возможно в качестве метрики для оценки связи между различными событиями безопасности, а также коэффициента множественной корреляции для оценки связи событий безопасности и инцидента. Т. е. в качестве оценки «степени связности» события безопасности и инцидента, в соответствии с их определением как зависимых событий, можно рассматривать корреляцию между ними. Тогда в общем случае связность события безопасности и инцидента определяется их парным коэффициентом корреляции.

Если происходит несколько событий безопасности (a_1, ..., a_n), индицирующих инцидент I_s, то показателем связности (тесноты) между этими событиями и инцидентом выступает коэффициент множественной корреляции $\boldsymbol{\rho}_{I\cdot a1,\ldots,an}$ [18]:

$$\boldsymbol{\rho}_{I\cdot a1,\ldots,an} = 1 - \frac{|R|}{R_{00}},$$

где R – корреляционная матрица $R = \{\boldsymbol{\rho}_{i,i}\}$; $|R|$ – определитель этой матрицы; R_{00} – алгебраическое дополнение для $\boldsymbol{\rho}_{0,0}$.

Сама корреляционная матрица определяется как:

$$R = \begin{pmatrix} \boldsymbol{\rho}_{0,0} & \cdots & \boldsymbol{\rho}_{0,an} \\ \vdots & \ddots & \vdots \\ \boldsymbol{\rho}_{an,0} & \cdots & \boldsymbol{\rho} \end{pmatrix},$$

где $\boldsymbol{\rho}_{i,j} = \boldsymbol{\rho}_{ai,aj}$ – парные коэффициенты корреляции при $i, j = 1, \ldots, n$, а $\boldsymbol{\rho}_{0,0} = \boldsymbol{\rho}_{I,I}$ и все $\boldsymbol{\rho}_{i,i} = 1$.

Так как события безопасности независимы, то мультиколлериальность отсутствует (строки линейно-независимы): $\boldsymbol{\rho}_{i,j} = 0$ при $i \neq j$.

Множественный коэффициент корреляции можно использовать как метрику для оценки эффективности набора сигнатур $\boldsymbol{S}_k$:

$$\|\theta(\boldsymbol{S}_k)\| = \|\boldsymbol{A}_k\| = \boldsymbol{\rho}_{I\cdot\boldsymbol{A}_k} = \boldsymbol{\rho}_{I\cdot a1,\ldots,an}.$$

Часто, как показатель близости, также используется коэффициент детерминации:

$$D = (\boldsymbol{\rho}_{I\cdot\boldsymbol{A}_k})^2.$$

Необходимым условием корреляционного анализа является линейная регрессионная связь между объясняемым параметром и объясняющими факторами. Для рассматриваемой задачи объясняемым параметром является инцидент I, а объясняющими факторами – сигнатуры (агрегированные события безопасности). Как это предлагалось в [12], будем рассматривать все переменные этой линейной регрессии как дихотомические (бинарные), принимающие значения: 1 – если событие (инцидент) произошло; 0 – в противном случае.

При сравнении бинарных переменных, измеренных в дихотомической шкале, мерой корреляционной связи служит коэффициент ассоциации Пирсона φ. Величина коэффициента $\boldsymbol{\rho}_{i,j} = \boldsymbol{\rho}_{ai,aj} = \varphi$ лежит в интервале +1 и –1.

В общем виде формула эмпирического вычисления коэффициента корреляции дихотомических переменных $x = a_i$ и $y = a_j$ [19]:

$$\varphi = \frac{p_{xy} - p_x p_y}{\sqrt{p_x(1-p_x)p_y(1-p_y)}},$$

где p_x – оценка вероятности появления события $x = a_i$; p_y – оценка вероятности появления события $y = a_j$; p_{xy} – оценка вероятности появления событий x и y одновременно.

Более наглядно вычисление φ производится на основе таблицы 1 по результатам наблюдения, но с тем же результатом [19]:

$$\varphi = \frac{ad - bc}{\sqrt{(a+b)(b+d)(a+c)(c+d)}}.$$

ТАБЛИЦА 1. Таблица сопряжения

TABLE 1. Conjugacy Table

Событие a_i	Событие a_j		Σ
	Да	Нет	
Да	a	b	$a + b$
Нет	c	d	$c + d$
Σ	$a + c$	$b + d$	$n = a + b + c + d$

Известны также другие показатели связи, вычисляемые по этой таблице. Например, коэффициент ассоциации Юла [19]:

$$q = \frac{ad - bc}{ad + bc}.$$

В рассматриваемом случае асимптотического управления предполагается постепенное изменение СЗИ, в результате последовательного изменения множества контролируемых событий безопасности. Для оценки влияния отдельных факторов (в нашем случае событий безопасности) используются частные коэффициенты корреляции, когда значения всех остальных факторов фиксируются [19]. Метод последовательного включения (или исключения) событий безопасности позволяет выбрать из возможного набора событий именно те, которые повысят качество СЗИ. Например, это происходит, когда вводится новое событие безопасности a_i, имеющее наибольшее по абсолютной величине значение частного коэффициента корреляции с инцидентом при фиксированном влиянии ранее введенных событий безопасности:

$$\boldsymbol{\rho}_{I\cdot ai|a1,..,ai-1,ai+1,\ldots,an}.$$

В общем случае можно рассматривать включение (или исключения) группы событий безопасности, a_{i+1}, ..., a_{i+l} ($l < n$), тогда используется частный коэффициент корреляции l-го порядка.

При введении дополнительных событий безопасности коэффициент детерминации (множественной корреляции) должен возрастать (чем больше, тем лучше), а остаточная дисперсия уменьшаться. Следовательно, можем вести отношения предпочтения $\succcurlyeq_R$, сравнения сигнатур $\boldsymbol{S}_i$ на основе введенной метрики $\|\theta(\boldsymbol{S}_k)\| = \boldsymbol{\rho}_{I\cdot\boldsymbol{A}_k}$ и, соответственно, $\succcurlyeq_R$ для сравнения СЗИ:

$$\text{СЗИ}_1 \succcurlyeq_R \text{СЗИ}_2, \text{ если } \boldsymbol{S}_1 \succcurlyeq_R \boldsymbol{S}_2;$$

$$\text{СЗИ}_1 \preccurlyeq_R \text{СЗИ}_2, \text{ если } \boldsymbol{S}_1 \preccurlyeq_R \boldsymbol{S}_2;$$

$$\text{СЗИ}_1 =_R \text{СЗИ}_2, \text{ если } \boldsymbol{S}_1 =_R \boldsymbol{S}_2.$$

Вместо заключения

Рассмотренные варианты отношения порядка позволяют сравнивать между собой СЗИ и тем самым оценивать улучшение свойств СЗИ в процессе асимптотического управления. И если использование отношения $\succcurlyeq_R$ представляется более точным, то для $\succcurlyeq_S$ можно отметить его простоту и универсальность.

Использование метрики $||\theta(\boldsymbol{S}_r)||=||\boldsymbol{A}_r||$ (введенной для $\succcurlyeq_S$ или $\succcurlyeq_R$) в качестве универсальной ограничивает то, что описанные выше варианты отношения порядка вполне корректны только для случая одного инцидента.

В случае множества инцидентов можно рассматривать инцидент $\boldsymbol{I} = \{\boldsymbol{I}_1, \boldsymbol{I}_2, ..., \boldsymbol{I}_m\}$ как набор инцидентов одинаковой значимости, обнаруживаемых СЗИ, и сравнение СЗИ должно учитывать эффективность обнаружения каждого. Т. е. мы можем рассматривать это как задачу многокритериального выбора, где отдельным критерием выступает эффективность обнаружения каждого $\boldsymbol{I}_r$ (т. е. снимаются ограничения предположения П-1 и П-3). Для сравнения СЗИ по множествам сигнатур соответственно будет использоваться векторный критерий $(\boldsymbol{S}_1, \boldsymbol{S}_2, ..., \boldsymbol{S}_m)$.

Для векторных критериев возможны разные подходы, в частности можно использовать свертки (агрегирование) исходных данных [20]. Так, введенное отношение $\succcurlyeq^S$ или $\succcurlyeq^R$ можно распространить на общий случай для множества инцидентов индицируемых в СЗИ, если в качестве единого инцидента $\boldsymbol{I}$ рассматривать возникновение любого инцидента. В общем случае сравнение производится только как сравнение векторов одинаковой размерности $(\boldsymbol{S}_1^i, \boldsymbol{S}_2^i, ..., \boldsymbol{S}_m^i)$ и $(\boldsymbol{S}_1^j, \boldsymbol{S}_2^j, ..., \boldsymbol{S}_m^j)$, и $(\boldsymbol{S}_1^i, \boldsymbol{S}_2^i, ..., \boldsymbol{S}_m^i) \succcurlyeq (\boldsymbol{S}_1^j, \boldsymbol{S}_2^j, ..., \boldsymbol{S}_m^j)$ если $\boldsymbol{S}_r^i \succcurlyeq_S \boldsymbol{S}_r^j$ для любого r (или $\boldsymbol{S}_r^i \succcurlyeq_R \boldsymbol{S}_r^j$), в противном случае вектора несравнимы.

Однако следует учесть, что при асимптотическом управлении мы улучшаем качество СЗИ постепенно, последовательно внося изменения и, следовательно, можно предположить, что в большинстве случаев это будет связано с одним вполне конкретным инцидентом.

В заключение следует отметить, что, учитывая возможность динамики развития состава индицируемых инцидентов, следует одновременно предполагать неизменность защищаемого объекта и среды (так как их изменение может сокращать множество инцидентов). В частности, следует допускать, что переход от одной модели угроз к другой, основанный на изменении состава инцидентов, происходит при неизменном составе механизмов защиты.

Список используемых источников

1. Хоффман Л. Современные методы защиты информации. Пер. с англ. М.: Сов. радио, 1980. 262 с.
2. ГОСТ Р ИСО/МЭК 15408-1-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М.: Стандартинформ, 2014.
3. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61. DOI:10.24411/2409-5419-2018-10041
4. Mikhalevich I.F., Trapeznikov V.A. Critical Infrastructure Security: Alignment of Views // Systems of Signals Generating and Processing in the Field of on Board Communications (Moscow, Russia, 20–21 March 2019). IEEE, 2019. DOI:10.1109/SOSG.2019.8706821
5. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Принципы и задачи асимптотического управления безопасностью критических информационных инфраструктур // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 12. С. 29–35. DOI:10.24411/2072-8735-2018-10330
6. ISO/IEC 27005:2018(en) Information technology. Security techniques. Information security risk management // Online Browsing Platform. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en (дата обращения 07.09.2020)
7. Гавдан Г.П., Иваненко В.Г., Салкуцан А.А. Обеспечение безопасности значимых объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 69–82. DOI:10.26583/bit.2019.4.05
8. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Событийно-ориентированная политика безопасности и формальная модель механизма защиты критических информационных инфраструктур // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 99–105. DOI:10.31854/1813-324X-2019-5-4-99-105
9. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Эффективность активного мониторинга событий сетевой безопасности // Электросвязь. 2020. № 2. С. 46–51. DOI:10.34832/ELSV.2020.3.2.007
10. Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи. АДЭ, 26.06.2019. URL: http://www.rans.ru/images/metrecKII.pdf (дата обращения 07.09.2020)

11. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М.: Стандартинформ, 2009.
12. Масич Г.Ф. Системы обнаружения вторжений. Intrusion Detection System – IDS // ИМССУрОРАН. 2016. URL: https://www.icmm.ru/uchebnaya-deyatelnost/lektsii/514-ids (дата обращения 07.09.2020)
13. Ложковский А.Г., Каптур В.А., Вербанов О.В., Колчар В.М. Математическая модель пакетного трафика // Вестник Нац. техн. ун-та «ХПИ». 2011. № 9. С. 113–119. URL: http://repository.kpi.kharkov.ua/handle/KhPI-Press/10831 (дата обращения 07.09.2020)
14. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. Москва: Горячая линия–Телеком, 2019. 448 с.
15. Новикова Е.С., Бекенева Я.А., Шоров А.В., Федотов Е.С. Обзор алгоритмов корреляции событий безопасности для обеспечения безопасности облачных вычислительных сред // Информационно управляющие системы. 2017. № 5(90). С. 95–104. DOI:10.15217/issn1684-8853.2017.5.95
16. Петухов А.Н., Пилюгин П.Л. Методы и инструменты моделирования безопасности критических информационных инфраструктур // Вторая всероссийская конференция «Современные технологии обработки сигналов» (СТОС-2019, Москва, Россия, 11–12 декабря 2019). Москва: Московское НТО радиотехники, электроники и связи им. А.С. Попова, 2019.
17. Фёрстер Э., Рёнц Б. Методы корреляционного и регрессионного анализа. Руководство для экономистов. Пер. с нем. М.: Финансы и статистика, 1983. 304 с.
18. Крамер Г. Математические методы статистики. Пер. с англ. М.: Мир, 1975. 648 с.
19. Ермолаев О.Ю. Математическая статистика для психологов. М.: Московский психолого-социальный институт, Флинта, 2003. 336 с.
20. Подиновский В.В. Идеи и методы теории важности критериев. М: Наука, 2019. 103 с.

* * *

About the Comparison of Information Security Systems for Asymptotic Information Security Management of Critical Information Infrastructures

S. Erokhin[1], **A. Petukhov**[1, 2*], **P. Pilyugin**[1, 3]

[1]Moscow Technical University of Communications and Informatics,
Moscow, 111024, Russian Federation
[2]National Research University of Electronic Technology (MIET),
Moscow, 124498, Russian Federation
[3]Lomonosov Moscow State University
Moscow, 119991, Russian Federation

Article info
DOI:10.31854/1813-324X-2020-6-3-66-74
Received 19th August 2020
Accepted 8th September 2020

For citation: Erokhin S., Petukhov A., Pilyugin P. About the Comparison of Information Security Systems for Asymptotic Information Security Management of Critical Information Infrastructures. *Proc. of Telecom. Universities.* 2020;6(3):66–74. (in Russ.) DOI:10.31854/1813-324X-2020-6-3-66-74

Abstract: *The article discusses the security management capabilities of critical information infrastructures. It discusses approaches to developing security policies that don't lean on assessing residual risks and identifying a fixed list of threats. We examine the possibility of building information security management systems based on monitoring of security events. A formal description of security events as well as relevant protection methods is proposed. The paper introduces an order relation for information security systems comparison and asymptotic CII security control implementation.*

Keywords: *information security, information security policy, information security events, information security events monitoring, asymptotic management, network events characteristics, critical information infrastructures.*

References

1. Khoffman L. *Modern Methods of Information Protection*. Moscow: Sov. radio Publ; 1980. 262 p. (in Russ.)
2. GOST R ISO/MEK 15408-1-2013 I*nformation technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components.* Moscow: Standartinform Publ.; 2014. (in Russ.)
3. Zakharchenko R.I., Korolev I.D. Methods of Estimation of Stability of Functioning of Objects of Critical Information Infrastructure Operating in Cyberspace. *H&ES RESEARCH*. 2018;10(2):52–61. (in Russ.) DOI:10.24411/2409-5419-2018-10041
4. Mikhalevich I.F., Trapeznikov V.A. Critical Infrastructure Security: Alignment of Views. *Proceedings of the Conference on Systems of Signals Generating and Processing in the Field of on Board Communications, 20–21 March 2019, Moscow, Russia*. IEEE; 2019. DOI:10.1109/SOSG.2019.8706821
5. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Principles and Tasks of Asymptotic Security Management of Critical Information Infrastructures. *T-Comm*. 2019;13(12):29–35. (in Russ.) DOI:10.24411/2072-8735-2018-10330
6. *Online Browsing Platform*. ISO/IEC 27005:2018(en) Information technology. Security techniques. Information security risk management. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en [Accessed 7th September 2020]
7. Gavdan G.P., Ivanenko V.G., Salkutsan A.A. Security of Significant Objects of Critical Information Infrastructure. *IT Security*. 2019;26(4):69–82. (in Russ.) DOI:10.26583/bit.2019.4.05
8. Erokhin S., Petukhov A., Pilyugin P. Event-based Security Policy and Formal Model of Critical Information Infrastructures Protecting Mechanism. *Proc. of Telecom. Universities.* 2019;5(4):99–105. (in Russ.) DOI:10.31854/1813-324X-2019-5-4-99-105
9. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Effectiveness of Active Monitoring of Network Security Events. *Elektrosviaz*. 2020;2:46–51. (in Russ.) DOI:10.34832/ELSV.2020.3.2.007
10. *Methodical Recommendations for Categorizing Critical Information Infrastructure Objects Belonging to Subjects of Critical Information Infrastructure Operating in the Field of Communications*. Documentary Telecommunication Association, 26th June 2019. (in Russ.) Available from: http://www.rans.ru/images/metrecKII.pdf [Accessed 7th September 2020]
11. GOST R ISO MEK/TO 18044-2007 *Information technology. Security techniques. Information security incident management*. Moscow: Standartinform Publ.; 2014. (in Russ.)
12. Masich G.F. Intrusion Detection System – IDS. *Institute of Continuous Media Mechanics of the Ural Branch of Russian Academy of Science*. 2016. (in Russ.) Available from: https://www.icmm.ru/uchebnaya-deyatelnost/lektsii/514-ids [Accessed 7th September 2020]
13. Lozhkovskii A.G., Kaptur V.A., Verbanov O.V., Kolchar V.M. Mathematical Model of Packet Traffic. *Vestnik Nat. tech. university "KhPI"*. 2011;9:113–119. (in Russ.) Available from: http://repository.kpi.kharkov.ua/handle/KhPI-Press/10831 [Accessed 7th September 2020]
14. Shelukhin O.I. *Network Anomalies. Detection, Localization, Forecasting*. Moscow: Goriachaia liniia–Telekom Publ.; 2019. 448 p. (in Russ.)
15. Novikova E.S., Bekeneva Ya.A., Shorov A.V., Fedotov E.S. A Survey of Security Event Correlation Techniques for Cloud Computing Environment Security. *Information and Control Systems*. 2017;5(90):95–104. (in Russ.) DOI:10.15217/issn1684-8853.2017.5.95
16. Petukhov A.N., Pilyugin P.L. Methods and Tools for Modeling the Security of Critical Information Infrastructures. *Proceedings of 2nd All-Russian Conference on Modern Signal Processing Technologies, 11–12 December 2019, Moscow, Russia*. Moscow: Moscow Scientific and Technical Society Radio Engineering, Electronics and Communications named after A.S. Popov Publ.; 2019. (in Russ.)
17. Förster E., Rönz B. *Methods of Correlation and Regression Analysis*. Moscow: Finansi i statistika Publ.; 1983. 304 p. (in Russ.)
18. Kramer G. *Mathematical Methods of Statistics*. Moscow: Mir Publ.; 1975. 648 p. (in Russ.)
19. Ermolaev O.Yu. *Mathematical Statistics for Psychologists*. Moscow: Moscow Psychological and Social Institute Publ., Flinta Publ.; 2003. 336 p. (in Russ.)
20. Podinovskiy V.V. *Ideas and Methods of the Theory of the Importance of Criteria*. Moscow: Nauka Publ.; 2019. 103 p. (in Russ.)

Сведения об авторах:

ЕРОХИН Сергей Дмитриевич — кандидат технических наук, доцент, ректор Московского технического университета связи и информатики, esd@mtuci.ru
https://orcid.org/0000-0001-8449-3612

ПЕТУХОВ Андрей Николаевич — кандидат технических наук, начальник отдела НИЧ Московского технического университета связи и информатики, anpetukhov@yandex.ru
https://orcid.org/0000-0002-1427-2440

ПИЛЮГИН Павел Львович — кандидат технических наук, старший научный сотрудник НИЧ Московского технического университета связи и информатики, ppl@mail.ru
https://orcid.org/0000-0003-0011-7180