УДК 004.7

Модель процесса функционирования сети передачи данных в условиях нарушений безопасности информации

Model of the data transmission network's functioning process in the event of information security violations

Липатников / Lipatnikov V.
Валерий Алексеевич
(lipatnikovanl@mail.ru)
доктор технических наук, профессор,
заслуженныйдеятель науки РФ, заслуженный изобретатель РФ, почетный работник ВПО РФ,
член-корреспондент РАЕН.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ (ВАС им. С. М. Буденного),
старший научный сотрудник.
г. Санкт-Петербург

Макаренко / Makarenko D.
Денис Владимирович
(nsdivdeni@yandex.ru)
ВАС им. С. М. Буденного,
адъюнкт научно-исследовательского центра.
г. Санкт-Петербург

Шевченко / Shevchenko A.
Александр Александрович
(alex_pavel1991@mail.ru)
ВАС им. С. М. Буденного,
старший научный сотрудник.
г. Санкт-Петербург

Ключевые слова: способ повышения безопасности – a way to increase security; сеть передачи данных – a data transmission network; нарушения безопасности информации – information security breaches; угрозы вторжений – intrusion threats.

В современном информационном пространстве одним из важнейших вопросов является безопасность сети передачи данных. Цель исследования: модель должна предусматривать порядок и содержание действий по анализу угроз безопасности в сетях передачи данных. Результаты: определена возможность оценки зависимости вероятности безопасности сети передачи данных от параметров процесса реагирования системы защиты информации на вредоносные воздействия. Предложена модель на основе Марковских процессов. Практическая значимость: модель позволит оценить значения вероятности безопасности в условиях нарушений и обеспечивает теоретическое обоснование построения средств контроля инцидентов нарушения безопасности.

In the information field one of the most prominent questions is the security of the data transmission network. The purpose of the study: the model should provide for the procedure and content of actions for analyzing security threats in data transmission networks. Results: the possibility of assessing the dependence of the probability of data transmission network security on the parameters of the information protection system's response to malicious influences has been determined. A model based on Markov processes is proposed. When developing the model, data was used reflecting the parameters of the data transmission network, as well as a system of distributed network agents monitoring security threats. Practical significance: the model will allow estimating the values of the probability of security in conditions of information security breaches. The model provides a theoretical justification for building security incident controls.

Введение

В настоящее время сеть Интернет является неотъемлемой частью жизни людей и государства, а также важнейшим средством функционирования предприятий и коммерческих компаний. Информация является наиболее важным ресурсом, который стремятся использовать как добросовестные пользователи сети, государство и рекламодатели, так и недоброжелатели, которые реализуют хищение данных для совершения мошеннических действий и дестабилизации ситуации в стране. На современном этапе одним из важнейших средств информационного взаимодействия являются сети передачи данных (СПД) и, как следствие, они же являются наиболее интересным объектом для совершения вредоносных воздействий. Нарушители направляют свои усилия на хищение информации, проведение атак, фишинга и массовую рассылку спама в целях своей выгоды. Имеющиеся средства защиты информации (СЗИ) являются эффективными, но в связи с тенденцией создания новых методов воздействия требуют модернизации и реорганизации системы защиты информации, которые позволят оперативно реагировать на угрозы безопасности (УБ).

Анализ релевантных работ показал необходимость моделирования процесса обеспечения безопасности сети передачи данных в условиях атак. Например, в [1] рассматривалась модель, в которой применялась система виртуальных контейнеров. Модель не учитывает возможности противника по проведению многоэтапных атак и одновременных разноплановых вредоносных воздействий.

Проблема анализа несвоевременного реагирования на нарушения безопасности информации (НБИ) рассматривалась в [2], где предложена модель, в которой применялась система обнаружения геолокации нарушителя. Модель позволяла исследовать точку входа в сеть, через которую осуществлялось воздействие. Однако модель не учитывает изменяющуюся обстановку, что требует доработки процессов защиты информации в части, касающейся противостояния УБ.

В работе [3] предлагается способ расчета вероятности потери пакетов, основанный на использовании фундаментальных выражений, полученных для систем массового обслуживания M/M/1 с учетом категорийности потока и дисциплины обслуживания заявок с введением поправочных коэффициентов, учитывающих вариативность трафика [4], индекс Херста [5] и связанных с ним параметров [6]. В исследовании [11–20] отмечается, что для использования методов машинного обучения в системы обнаружения атак (COA, IDS) обычно требуется преобразование данных

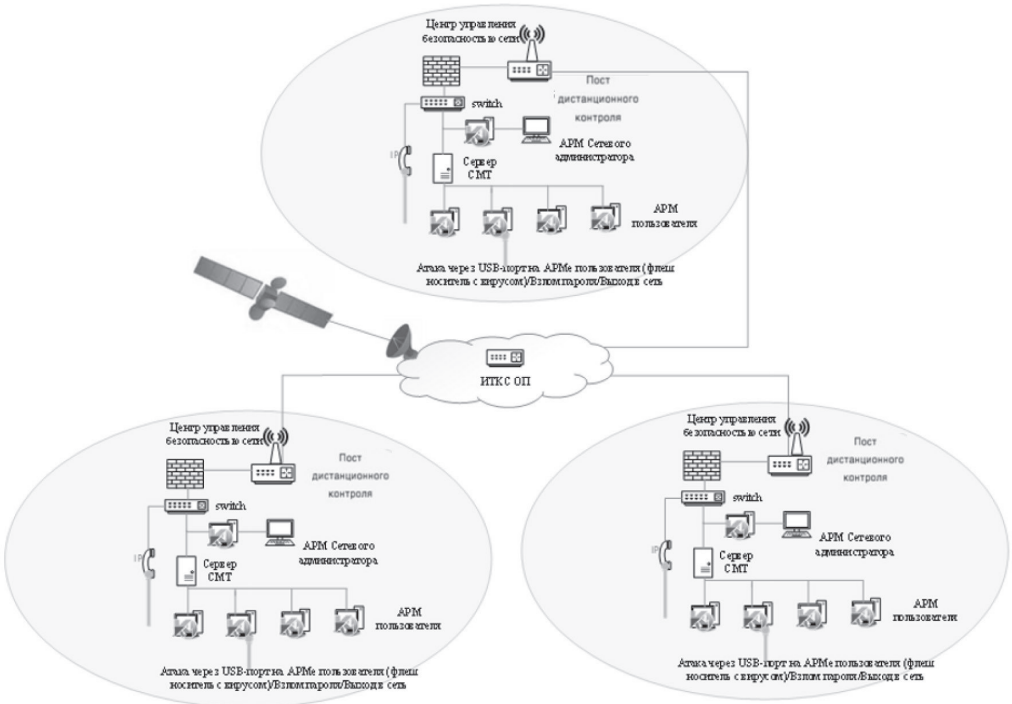

Рис. 1. Структурная схема СПД предприятия

в набор признаков, то есть формирование признакового пространства, и подчеркивается важность отбора подходящих признаков для точности данных методов. Для оценки применимости методов глубокого обучения для обнаружения вторжений описаны в исследовании нейронная сеть CNN-BiLSTM [12] и представлены результаты её сравнения с разработанной ранее моделью [13–17], основанной на использовании классификатора типа «случайный лес» (Random Forest), на публичном наборе данных обучения CICIDS2017 [14–15]. Данные работы, безусловно, вносят значительный вклад в развитие методов моделирования, однако не учитывают влияние результатов реализации нарушителем атак. Следовательно, задача моделирования процесса функционирования СПД в условиях НБИ является актуальной.

Предполагаемым решением проблемы является разработка модели, которая должна учитывать организацию сетевого контроля и оперативное принятие мер по пресечению нарушений безопасности.

Целью исследования является оценка вероятности безопасности СПД в условиях многоэтапных атак.

Задачей является разработка модели процесса функционирования СПД в условиях НБИ на основе Марковских процессов.

Решение. В качестве объекта исследования рассмотрена СПД, представленная на рис. 1.

СПД предприятия представляет собой сегментарные области сети, центральную и подчиненную. В обоих сегментах реализовано обнаружение вредоносного воздействия, проводится мониторинг сети. В центральном сегменте реализуется обобщение и обработка информации об обнаруженной УБ. Между подчиненной и центральной областями организуется взаимодействие, позволяющее реализовать эффективную систему защиты информации (ЗИ) за счет оперативности реагирования на НБИ.

Представленный на рис. 2 алгоритм процесса функционирования СПД в условиях воздействий является основой модели и поясняется следующим образом. Постоянно проводится сканирование сетевого трафика сети на предмет УБ (подозрительных действий пользователя, аномального изменения загруженности трафика сети, просроченных паролей, несанкционированных подключений носителей к автоматизированным рабочим местам, сканирования трафика на предмет задержек и утери пакетов). При обнаружении несоответствия состояния сетевого потока пределам нормы организуется изменение штатного режима функционирования СПД. Затем происходит инициализация уязвимости и выявление ее особенностей, которые сравниваются с имеющейся базой данных уязвимостей. При нахождении источника угрозы организуется ее анализ и сравнение параметров с имеющейся базой данных угроз. Если параметры угрозы известны, то происходит устранение по известному методу, иначе на основе предыдущих нарушений составляется план противодействия новой угрозе и предлагается решение по ее устранению. После принятия решения сетевым администратором

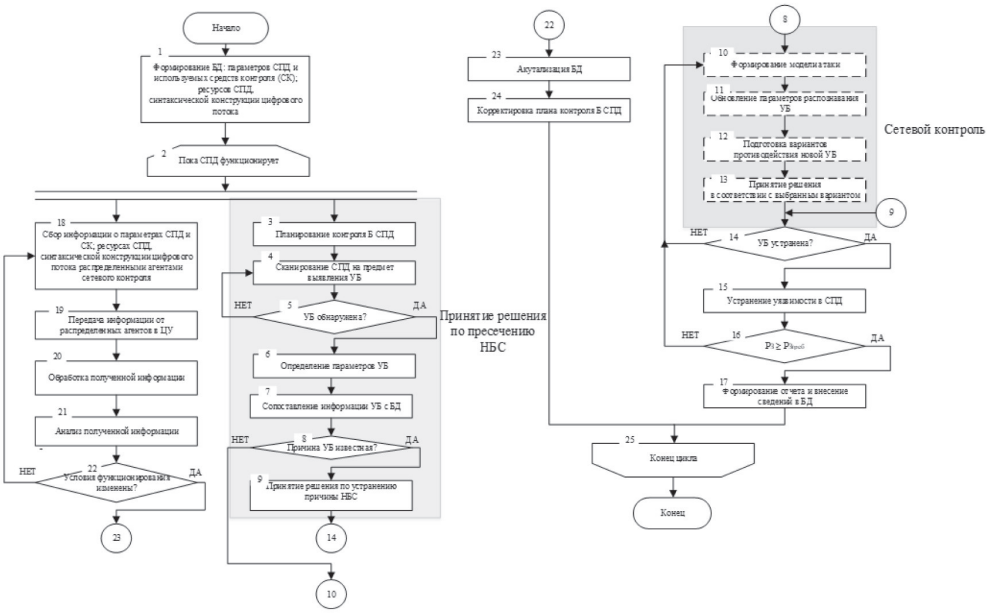

Рис. 2. Блок-схема алгоритма процесса функционирования СПД в условиях НБИ

оценивается вероятность безопасности СПД, если она удовлетворяет требуемому значению, то угроза устраняется и сведения о ней записываются в базу данных (БД).

На основе блок-схемы алгоритма составлен граф состояний системы ЗИ при реализации процесса обеспечения безопасности СПД в условиях НБИ, представленный на рис. 3.

Состояние «0» соответствует состоянию покоя системы ЗИ. Вероятность того, что система ЗИ находится в этом состоянии, обозначим через P_0. Система переходит в состояние «1» с вероятностью P_{01} за время $t_{ож}$.

Состояние «1» соответствует состоянию системы ЗИ, в котором осуществляется планирование контроля безопасности СПД. Система переходит в состояние «2» с вероятностью P_{12} за время $t_{п}$.

Состояние «2» соответствует состоянию системы ЗИ, в котором производится сканирование СПД на предмет выявления УБ. Система переходит в состояние «3» с вероятностью P_{23} за время $t_{с}$.

Состояние «3» соответствует состоянию системы ЗИ, в котором осуществляется определение параметров УБ. Система переходит в состояние «4» с вероятностью P_{34} за время $t_{оп}$.

Состояние «4» соответствует состоянию системы ЗИ, в котором происходит сопоставление информации УБ с БД и уясняется, известна ли причина УБ. Если она известна, то система переходит в состояние «5» с вероятностью P_{45} за время $t_{ип}$, иначе система переходит в состояние «6» с вероятностью P_{46} за время $t_{нп}$.

Состояние «5» соответствует состоянию системы ЗИ, в котором принимается решение по устранению причины УБ. Система переходит в состояние «10» с вероятностью P_{510} за время $t_{пр}$.

Состояние «6» соответствует состоянию системы ЗИ, в котором формируется модель атаки. Система переходит в состояние «7» с вероятностью P_{67} за время $t_{фма}$.

Состояние «7» соответствует состоянию системы ЗИ, в котором осуществляется обновление параметров распознавания УБ. Система переходит в состояние «8» с вероятностью P_{78} за время $t_{опр}$.

Состояние «8» соответствует состоянию системы ЗИ, в котором вырабатывается подготовка вариантов противодействия новой УБ. Система переходит в состояние «9» с вероятностью P_{89} за время $t_{подг}$.

Состояние «9» соответствует состоянию системы ЗИ, в котором осуществляется принятие решения в соответствии с выбранным вариантом. Если угроза устранена, то система переходит в состояние «10» с вероятностью P_{910} за время $t_{уу}$, иначе система переходит в состояние «6» с вероятностью P_{610} за время $t_{уну}$.

Состояние «10» соответствует состоянию системы ЗИ, в котором реализуется устранение уязвимости в СПД. Если уязвимость устранена, то система переходит в состояние «11» с вероятностью P_{1011} за время $t_{ууяз}$, иначе система переходит в состояние «6» с вероятностью P_{106} за время $t_{нуяз}$.

Состояние «11» соответствует состоянию системы ЗИ, в котором формируется отчет и осуществляется внесение сведений в БД. Система переходит в состояние «1» с вероятностью P_{121} за время $t_{фо}$.

В процессе моделирования будем использовать показатель «вероятность безопасности СПД» ($P_{Б}$) и параметры: время формирования параметров СПД ($t_{ож}$), время планирования контроля безопасности СПД ($t_{п}$), время сканирования СПД на предмет выявления УБ ($t_{с}$), время определения параметров УБ($t_{оп}$), время сопоставления информации УБ с БД ($t_{ип}$), время принятия решения по устранению причины УБ ($t_{пр}$), время формирования модели атаки ($t_{фма}$), время обновления параметров распознавания УБ ($t_{опр}$), время подготовки вариантов противодействия новой УБ ($t_{подг}$), время принятия решения ($t_{уу}$), время устранения уязвимости ($t_{ууяз}$), время формирования отчета ($t_{фо}$).

Для построения модели воспользуемся аппаратом Марковских случайных процессов [4], то есть составим систему дифференциальных уравнений (1), в которой неизвестными функциями являются вероятности нахождения системы в различных состояниях P_1, P_2, ... P_{11}. Переменными δ, ε, α, β, σ, φ обозначаются состояния перехода. Решением системы (1) является выражение (2).

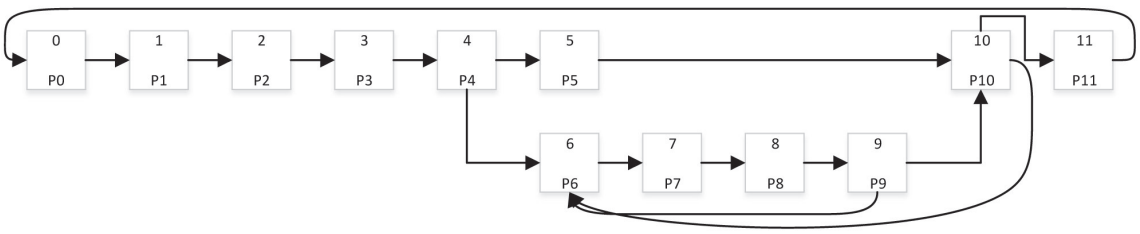

Рис. 3. Граф состояний системы ЗИ при реализации процесса обеспечения безопасности СПД в условиях НБИ

$$
\begin{cases}
\dfrac{dP_0(t)}{dt} = \mu_0 P_{11}(t) - \lambda_0 P_0(t); \\
\dfrac{dP_1(t)}{dt} = \lambda_0 P_0(t) - \lambda_{12} P_1(t); \\
\dfrac{dP_2(t)}{dt} = \lambda_{12} P_1(t) - \lambda_{23} P_2(t); \\
\dfrac{dP_3(t)}{dt} = \lambda_{23} P_2(t) - \lambda_{34} P_3(t); \\
\dfrac{dP_4(t)}{dt} = \lambda_{34} P_3(t) - \alpha P_4(t) - \beta P_4(t); \\
\dfrac{dP_5(t)}{dt} = \alpha P_4(t) - \lambda_{510} P_5(t) \\
\dfrac{dP_6(t)}{dt} = \beta P_4(t) - \lambda_{67} P_6(t) + \delta P_9(t) + \phi P_{10} \\
\dfrac{dP_7(t)}{dt} = \lambda_{67} P_6(t) - \lambda_{78} P_7(t) \\
\dfrac{dP_8(t)}{dt} = \lambda_{78} P_7(t) - \lambda_{89} P_8(t) \\
\dfrac{dP_9(t)}{dt} = \lambda_{89} P_8(t) - \delta P_9(t) - \sigma P_9(t) \\
\dfrac{dP_{10}(t)}{dt} = \sigma P_9(t) - \phi P_{10}(t) - \varepsilon P_{10}(t) + \lambda_{510} P_5(t) \\
\dfrac{dP_{11}(t)}{dt} = \varepsilon P_{10}(t) - \mu_0 P_{11}(t)
\end{cases} \quad (1)
$$

$$
\begin{cases}
P_1 = \dfrac{\lambda_{12}}{\lambda_0} P_0; \\
P_2 = \dfrac{\lambda_{12}^2}{\lambda_0 \lambda_{23}} P_0; \\
P_3 = \dfrac{\lambda_{12}^2}{\lambda_{34} \lambda_0} P_0; \\
P_4 = \dfrac{\lambda_{12}^2}{\lambda_0 (\alpha(t) + \beta)} P_0; \\
P_5 = \dfrac{\alpha(t) \lambda_{12}^2}{\lambda_{510} \lambda_0 (\alpha(t) + \beta)} P_0; \\
P_6 = \dfrac{\sigma\varepsilon\beta\lambda_{12}^2 - \delta(\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}\alpha(t)) - \lambda_0^2(\alpha(t)+\beta)\sigma\phi}{\varepsilon\lambda_0(\alpha(t)+\beta)\lambda_{67}} P_0; \\
P_7 = \dfrac{\sigma\varepsilon\beta\lambda_{12}^2 - \delta(\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}\alpha(t)) - \lambda_0^2(\alpha(t)+\beta)\sigma\phi}{\varepsilon\lambda_0(\alpha(t)+\beta)\lambda_{78}} P_0; \\
P_8 = \dfrac{\sigma\varepsilon\beta\lambda_{12}^2 - \delta(\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}\alpha(t)) - \lambda_0^2(\alpha(t)+\beta)\sigma\phi}{\varepsilon\lambda_0(\alpha(t)+\beta)\lambda_{89}} P_0; \\
P_9 = \dfrac{\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}^2\alpha(t)}{\varepsilon\lambda_0(\alpha(t)+\beta)\sigma} P_0; \\
P_{10} = \dfrac{\lambda_0}{\varepsilon} P_0; \\
P_{11} = \dfrac{\lambda_0}{\mu_0} P_0.
\end{cases} \quad (2)
$$

где

$$
P_0 = \frac{1}{1 + \frac{\lambda_{12}}{\lambda_0} + \frac{\lambda_{12}^2}{\lambda_0 \lambda_{23}} + \frac{\lambda_{12}^2}{\lambda_{34} \lambda_0} + \frac{\lambda_{12}^2}{\lambda_0 (\alpha(t) + \beta)} + \frac{\alpha(t) \lambda_{12}^2}{\lambda_{510} \lambda_0 (\alpha(t) + \beta)}}
$$

$$
\frac{1}{\frac{\sigma\varepsilon\beta\lambda_{12}^2 - \delta(\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}\alpha(t)) - \lambda_0^2(\alpha(t)+\beta)\sigma\phi}{\varepsilon\lambda_0(\alpha(t)+\beta)\lambda_{67}}}
$$

$$
\frac{1}{\frac{\sigma\varepsilon\beta\lambda_{12}^2 - \delta(\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}\alpha(t)) - \lambda_0^2(\alpha(t)+\beta)\sigma\phi}{\varepsilon\lambda_0(\alpha(t)+\beta)\lambda_{78}}}
$$

$$
\frac{1}{\frac{\sigma\varepsilon\beta\lambda_{12}^2 - \delta(\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}\alpha(t)) - \lambda_0^2(\alpha(t)+\beta)\sigma\phi}{\varepsilon\lambda_0(\alpha(t)+\beta)\lambda_{89}}}
$$

$$
\frac{1}{\frac{\lambda_0^2(\alpha(t)+\beta)(\phi+\varepsilon) - \varepsilon\lambda_{12}^2\alpha(t)}{\varepsilon\lambda_0(\alpha(t)+\beta)\sigma} + \frac{\lambda_0}{\varepsilon} + \frac{\lambda_0}{\mu_0}}.
$$

В качестве вероятности безопасности СПД можно использовать вероятность нахождения системы ЗИ в состоянии, когда осуществляется формирование отчета и внесение сведений в БД (P_{11}), а после этого система продолжает штатно функционировать, то есть продолжает сканирование СПД на предмет выявления УБ. Таким образом, вероятность состояния безопасности СПД $P_Б = P_0 + P_{11}$ и с учетом выражения (2) примет вид (3):

$$
P_Б = P_0 + \frac{\lambda_0}{\mu_0} P_0 \ . \quad (3)
$$

Контрольное решение

Для исследования модели процесса обеспечения безопасности СПД в условиях НБИ, выраженной зависимостью [3], возьмем временные характеристики процесса обеспечения безопасности СПД, указанные в таблице 1. Используемые значения данных временных характеристик являются экспертными оценками.

Используя исходные данные из таблицы 1 и выражение (3), получаем зависимости вероятности безопасности СПД от времени устранения уязвимости в СПД ($t_{устр}$) при различном времени формирования модели атаки ($t_{фма}$) и времени сканирования СПД на предмет выявления УБ ($t_с$), представленные на рис. 4–5.

Проведя анализ состояний системы, можно выявить зависимость между временными параметрами и вероятностью безопасности СПД. Имеются ключевые временные параметры, изменения которых будут влиять на вероятность безопасности СПД. Такими параметрами являются время обнаружения УБ, время сопоставления информации УБ с БД, время сканирования СПД и время формирования модели

атаки. Исходя из полученных графиков возможно сделать вывод, что значение вероятности безопасности будет понижаться тем сильнее, чем больше потребуется времени на обнаружение угрозы и на формирование модели атаки, что позволяет определить модель как достоверную. Сделан вывод, что системному администратору необходимо своевременно реагировать и принимать решение по устранению уязвимостей и угроз безопасности СПД, для этого необходимо обеспечить СЗИ мощным аппаратом системы поддержки принятия решений для соответствия временным рамкам по устранению угроз безопасности, а также дальнейшему сокращению временных параметров, представленных на графиках.

Предложенная модель показала хорошее согласование получаемых результатов с данными, приведенными в ранее опубликованных работах [7–10].

Выводы

Применение модели позволяет оценить зависимость между вероятностью безопасности и временными параметрами функционирования СПД и определить наилучшие показатели времени обнаружения угрозы вторжения и формирования модели атак для принятия решения администратором СПД по устранению уязвимостей и угроз СПД, вследствие чего показатель вероятности безопасности СПД повысит свое значение.

Новизна предложенного способа моделирования заключается в учете распределенных агентов контроля СПД и оптимизации методов устранения угроз безопасности для системы поддержки принятия решений. Это позволяет определить пути повышения безопасности за счет оперативности поиска угроз, оптимизации принятия решений и адаптивности к вредоносным воздействиям. Имеется перечень релевантных работ, применимых к данному направлению исследований.

Практическая значимость заключается в том, что модель позволяет анализировать и вырабатывать направления по повышению качества функционирования СПД в условиях деструктивного информационного воздействия нарушителя. Она обеспечивает возможность выработать оптимальные решения, минимизирующие потенциальные негативные последствия в случае реализации угроз злоумышленниками. Это достигается за счет анализа зависимостей между показателями безопасности и характеристиками подпроцессов защиты. Использование распределенных агентов и оптимизированных методов повы-

Таблица 1

Исходные данные модели СПД в условиях НБИ

№ п/п	Состояние системы	Параметр	Значение в минутах
1	Формирование БД: параметров и используемых средств контроля (СК); ресурсов СПД, синтаксической конструкции цифрового потока	$t_{ож}$	0,3
2	Планирование контроля Б СПД	$t_{п}$	0,5
3	Сканирование СПД на предмет выявления УБ	$t_{с}$	0.1 0.5 1
4	Определение параметров УБ	$t_{о}$	1 2 10
5	Сопоставление информации УБ с БД. Определение, известна ли причина УБ	$t_{ип}$ $t_{нп}$	0,3
6	Принятие решения по устранению причины НБС	$t_{пр}$	1
7	Формирование модели атаки	$t_{фма}$	1 5 10
8	Обновление параметров распознавания УБ	$t_{опр}$	0,5
10	Подготовка вариантов противодействия новой УБ	$t_{подг}$	1
11	Принятие решения в соответствии с выбранным вариантом	$t_{уу}$ $t_{уну}$	1
12	Устранение уязвимости в СПД	$t_{ууяз}$ $t_{нуяз}$	1
13	Формирование отчета и внесение сведений в БД	$t_{фо}$	0,5

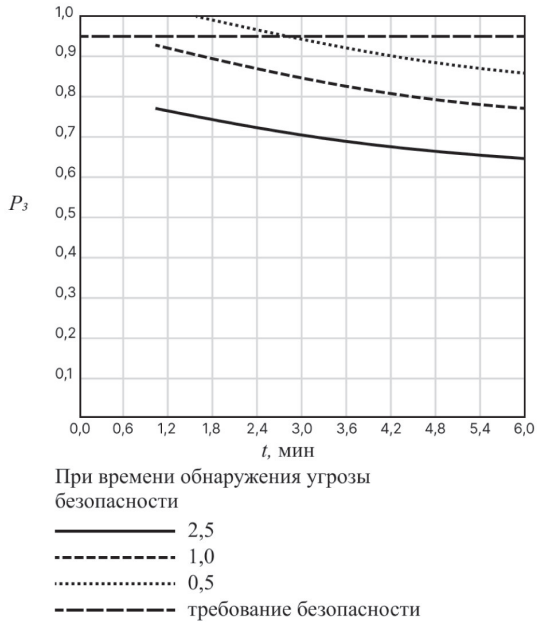

Рис. 4. График зависимости вероятности безопасности от времени обнаружения угрозы вторжения

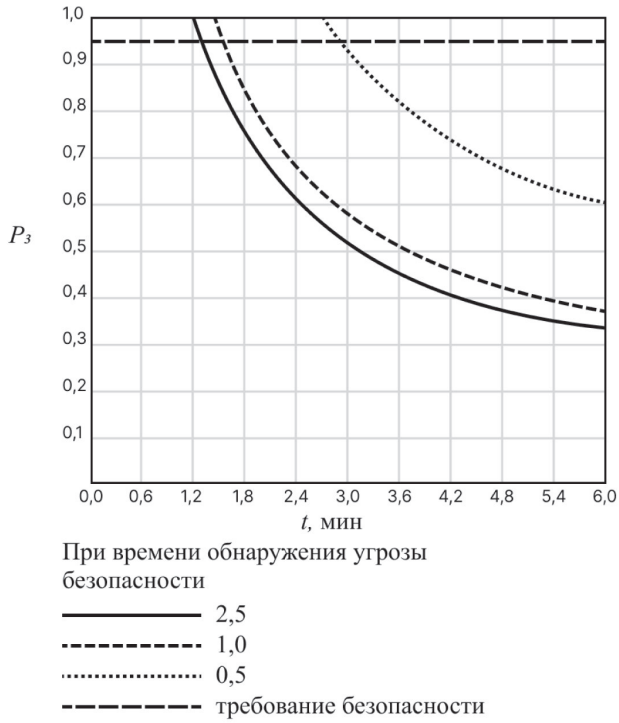

Рис. 5. График зависимости вероятности безопасности от времени формирования модели атаки

шает эффективность защиты СПД, снижая время реакции на угрозы.

В дальнейших исследованиях имеется необходимость применения технологии машинного обучения при совершенствовании средств сетевого контроля, для повышения вероятности безопасности СПД.

Литература

1. Шевченко, А. А. Математическая модель информационного противоборства двух систем в информационно-телекоммуникационном пространстве / А.А. Шевченко // Инновационная деятельность в Вооруженных Силах Российской Федерации : труды всеармейской научно-практической конференции (Санкт-Петербург, 14–15 октября 2020). – Санкт-Петербург : ВАС им. С.М. Буденного, 2020. – С. 237–241.

2. Задбоев, В. А. Способ защиты информационной сети с использованием метода определения местоположения злоумышленника / В.А. Задбоев, В.А. Липатников, К.В. Мелехов // Технологии. Инновации. Связь : материалы научно-практической конференции (Санкт-Петербург, 12 апреля 2023). – Санкт-Петербург : ВАС им. С.М. Буденного, 2023. – С. 138–143.

3. Липатников, В. А. Структурно-параметрический метод защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта / В.А. Липатников, В.А. Парфиров // Системы управления, связи и безопасности – 2023. – № 4. – С. 105–156.

4. Горохов, А. В. Модель процесса управления безопасностью информационных ресурсов в информационно-вычислительной сети / А.В. Горохов, В.А. Липатников, К.Д. Грабовый // Интернаука. – 2021. – № 39-1 (215). – С. 15–17.

5. Анализ уязвимостей и сетевых атак на ресурсы сетей передачи данных / В.А. Липатников, К.В. Мелехов, В.А. Робак, А.А. Шевченко // Перспективы безопасности-2024 : сборник материалов II научно-технической конференции, посвященной информационной безопасности (Санкт-Петербург, 19–20 июня 2024). – Санкт-Петербург : Специальный Технологический Центр, 2024. – С. 29–37.

6. Липатников, В. А. Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации / В.А. Липатников, К.В. Мелехов // Актуальные проблемы защиты и безопасности : труды XXVII Всероссийской научно-практической конференции (Санкт-Петербург, 01–04 апреля 2024). – Санкт-Петербург : Российская академия ракетных и артиллерийских наук, 2024. – С. 306–310.

7. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства / В.А. Липатников, В.А. Парфиров, А.А. Шевченко, К.В. Мелехов // Актуальные проблемы защиты и безопасности : труды XXVI Всероссийской научно-практической конференции (Санкт-Петербург, 03–06 апреля 2023). – Санкт-Петербург : Типография Любавич, 2023. – Т. 1.– С. 569–572.

8. Липатников, В. А. Модель компьютерной атаки типа «ZEROLOGON» на сеть передачи данных / В.А. Липатников, К.В. Мелехов, М.М. Рябов // Современные тенденции инженерного образования : сборник материалов Научно-практической конференции (Санкт-Петербург, 26 апреля 2023). – Санкт-Петербург : ВАС им. С.М. Буденного, 2023. – С. 196–201.

9. Котенко, И. В. Моделирование атак на компоненты машинного обучения систем обнаружения вторжений / И.В. Котенко, Е.А. Ичетовкин // Информатизация и связь. – 2025. – № 2. – С. 118–128.

10. Привалов, А. А. Модель процесса функционирования узла коммутации технологической сети передачи данных в условиях DDoS атак нарушителя / А.А. Привалов, В.Л. Лукичева, Д.Д. Титов // Информация и Космос. – 2021. – № 2. – С. 66–75.

11. Mohammadi, S. Anomaly-based Web Attack Detection: The Application of Deep Neural Network Seq2Seq With Attention Mechanism / S. Mohammadi, A. Namadchian // The ISC International Journal of Information Security. – 2020. – Vol. 12, Iss. 1. – P. 44–54.

12. Deep Learning based DDoS Attack Detection in Internet of Things: An Opti-mized CNN-BiLSTM Architecture with Transfer Learning and Regularization Tech-niques / I. Jebril, M. Premkumar, G.M. Abdulsaheb [et al.] // ResearchGate. – URL : https://www.researchgate.net/publication/380422963_Deep_learning_based_DDoS_Attack_Detection_in_Internet_of_Things_An_Optimized_CNN-BiLSTM_Architecture_with_Transfer_Learning_and_Regularization_Techniques (дата обращения: 04.01.2024).

13. Горюнов, М. Н. Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 / М.Н. Горюнов, А.Г. Мацкевич, Д.А. Рыболовлев // Труды ИСП РАН. – 2020. – Т. 32, № 5. – С. 81–94.

14. Intrusion Detection Evaluation Dataset (CICIDS2017) // UNB. – URL : https://www.unb.ca/cic/datasets/ids-2017.html (дата обращения: 04.10.2023).

15. Патент № RU 2705773 C1. Способ защиты информационно-вычислительной сети от вторжений : № 2019100252 : заявл. 09.01.2019 : опубл. 11.11.2019 / В.А. Липатников, К.В. Чепелев, А.А. Шевченко ; патентообладатель ВАС им. С.М. Буденного.

16. Костарев, С. В. Технологии защиты информации в условиях кибернетиче-ского противоборства / С.В. Костарев, В.В. Карганов, В.А. Липатников. – Санкт-Петербург : ВАС им. С.М. Буденного, 2020. – 716 с.

17. Korshunov, G. A. Decision support systems for information protection in the management of the information network / G.A. Korshunov, V.A. Lipatnikov, A.A. Shevchenko // Fuzzy Technologies in the Industry – FTI 2018 : proceedings of the II International Scientific and Practical Conference (Ulyanovsk, October 23–25, 2018). – Ulyanovsk : Ulyanovsk State Technical University, 2018. – P. 418–426.

18. Липатников, В. А. Способ обнаружения и классификации многоэтапной атаки на основе долгой краткосрочной памяти / В.А. Липатников, А.А. Ломанов // Технологии. Инновации. Связь : сборник материалов научно-практической конференции (Санкт-Петербург, 19 апреля 2021). – Санкт-Петербург : ВАС им. С.М. Буденного, 2022. – С. 104–108.

19. Военная доктрина Российской Федерации. Утверждена Указом Президента Российской Федерации от 25.12.2014г. № Пр-2976.

20. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).