УДК 004.056:621.39

Имитационная модель процесса реализации атаки на систему управления сетью синхронизации

The simulation model of the process of implementing an attack on the system for managing the synchronization network

Канаев / Kanaev A.
Андрей Константинович
(kanaev@itain.ru)
доктор технических наук, профессор.
ЗАО «Институт телекоммуникаций»,
заместитель генерального директора по спецпроектам.
г. Санкт-Петербург

Опарин / Oparin E.
Евгений Валерьевич
(Oparin@itain.ru)
кандидат технических наук.
ЗАО «Институт телекоммуникаций»,
ведущий специалист отдела разработки систем связи.
г. Санкт-Петербург

Опарина / Oparina E.
Екатерина Владимировна
(syrayaekaterina@mail.ru)
кандидат технических наук.
ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I»,
доцент кафедры «Механика и прочность материалов и конструкций».
г. Санкт-Петербург

Сахарова / Sakharova M.
Мария Александровна
(saharova@itain.ru)
кандидат технических наук.
ЗАО «Институт телекоммуникаций»,
начальник отдела разработки средств связи.
г. Санкт-Петербург

Ключевые слова: телекоммуникационная система – telecommunication system; система управления – control system; сеть синхронизации – synchronization network; уязвимость – vulnerability; атака – attack; злоумышленник – attacker; система информационной безопасности – information security system.

В работе приведена имитационная модель, в которой отражены все этапы борьбы между организованным злоумышленником и системой информационной безопасности при атаке на системы управления сетями синхронизации. Построенная модель позволяет получить вероятностно-временные характеристики процесса, отражающего взаимодействие организованного злоумышленника и системы информационной безопасности, произвести оценку данных характеристик в зависимости от состава ресурсов, имеющихся в наличии у злоумышленника и системы информационной безопасности. Полученные результаты могут быть применены администраторами систем информационной безопасности для учета при построении и проектировании средств защиты систем управления сетей синхронизации.

The work provides an imitation model that reflects all stages of the struggle between an organized attacker and an information security system when attacking synchronization networks control systems. The built model allows you to obtain probabilistic-temporal characteristics of the process that reflects the interaction of an organized attacker and information security system, assess these characteristics, depending on the composition of the resources available in the presence of the attacker and the information security system. The results can be applied by the administrators of information security systems for accounting for the construction and design of the protection systems for the control systems of synchronization networks.

Введение

Сеть синхронизации (СС) является ключевой подсистемой телекоммуникационной системы (ТКС). Сети синхронизации выполняют функции формирования, передачи и распределения сигналов синхронизации до цифровой аппаратуры ТКС, обеспечивая таким образом процесс её функционирования. Сеть синхронизации тесно взаимодействует со смежными подсистемами, существенно влияет на их функционирование. Качество услуг связи тесно связано с показателями качества процесса функционирования СС, а сигналы синхронизации и информационные сигналы потребителей передаются, как правило, в одних и

тех же цифровых потоках, используя при этом одни и те же направляющие системы. Отказы, возникающие в сетях синхронизации, способны значительно снизить качество предоставления услуг связи вплоть до полного их прекращения. [1, 2].

Таким образом, сети синхронизации представляют собой потенциальное место проникновения в телекоммуникационную систему со стороны организованного злоумышленника, намеревающегося оказать разрушающее и деструктивное воздействие. Отметим, что воздействие на сеть синхронизации как правило носит косвенный характер, при котором отказы в сетях синхронизации приводят в дальнейшем к возникновению отказов в телекоммуникационной системе. В данном случае устранение отказов значительно затруднено, так как зачастую отсутствует возможность достоверно определить причину их возникновения [1, 3].

Анализ проведения различных атак на сети синхронизации показал, что наибольшую опасность представляет собой атака на системы управления (СУ) сетей синхронизации. При получении злоумышленником контроля над СУ сети синхронизации возможно возникновение отказов значительного масштаба вплоть до полной приостановки процесса функционирования СС [3, 4].

Описание процесса взаимодействия организованного злоумышленника и системы информационной безопасности

На основе анализа различных сценариев атак и стратегий проведения защиты от них была сформирована модель взаимодействия организованного злоумышленника и системы информационной безопасности. Основой данной модели служит граф конфликтно обусловленных состояний (рис. 1).

Злоумышленник в общем случае проводит атаку в несколько этапов, основными из которых являются [5–7]:

- сбор и анализ исходных данных об объекте атаки;
- сканирование технологической сети передачи данных системы управления СС;
- определение структуры технологической сети передачи данных системы управления СС;
- вычисление точек входа в технологическую сеть передачи данных системы управления СС;
- анализ обнаруженных уязвимостей и подбор инструментария по их реализации;
- обход систем обнаружения вторжений с последующей реализацией атаки.

Каждый этап проведения атаки характеризуется тем, что, либо злоумышленник завершит данный этап и перейдет к следующему, либо система информационной безопасности зафиксирует атаку, нейтрализует злоумышленника и восстановит функционирование сети синхронизации в соответствии с нормативными значениями [8, 9].

Таким образом, модель противоборства организованного злоумышленника и системы информационной безопасности включает следующие состояния:

- S_1 – исходное состояние, при котором сеть синхронизации функционирует в соответствии с нормативными значениями параметров;
- S_2 – состояние, которое характеризуется тем, что злоумышленнику удалось получить необходимые исходные данные для проведения атаки;
- S_3 – состояние, при котором при котором система информационной безопасности нейтрализовала злоумышленника на этапе сбора исходных данных;
- S_4 – в данном состоянии злоумышленнику удалось просканировать технологическую сеть передачи данных системы управления СС;

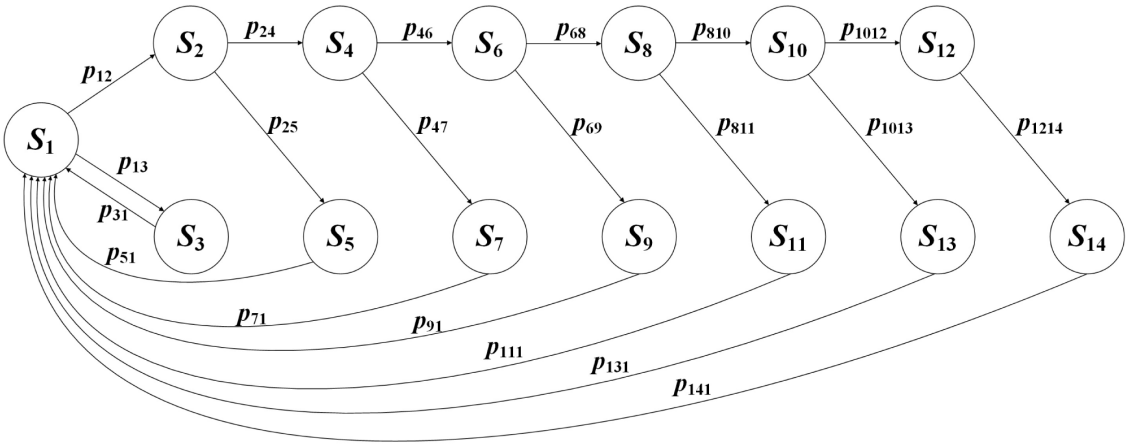

Рис. 1. Процесс взаимодействия организованного злоумышленника и системы информационной безопасности

· S_5 – в данном состоянии система информационной безопасности нейтрализовала злоумышленника на этапе сканирования технологической сети передачи данных системы управления СС;

· S_6 – состояние, которое характеризуется тем, что злоумышленник на основе добытых исходных данных построил структуру технологической сети передачи данных системы управления СС;

· S_7 – в данном состоянии система информационной безопасности нейтрализовала злоумышленника на этапе определения структуры технологической сети передачи данных системы управления СС;

· S_8 – состояние, в соответствии с которым злоумышленник обозначил точки входа в технологическую сеть передачи данных системы управления СС;

· S_9 – в данном состоянии система информационной безопасности нейтрализовала злоумышленника на этапе вычисления точек входа в технологическую сеть передачи данных системы управления СС;

· S_{10} – в данном состоянии злоумышленник на основе анализа найденных уязвимостей подобрал необходимый инструментарий по их реализации;

· S_{11} – в данном состоянии система информационной безопасности нейтрализовала злоумышленника на этапе анализа уязвимостей;

· S_{12} – состояние, которое характеризуется тем, что злоумышленник обходит систему обнаружения вторжений и реализует атаку;

· S_{13} – в данном состоянии система информационной безопасности нейтрализует злоумышленника на этапе обхода системы обнаружения вторжений;

· S_{14} – в данном состоянии злоумышленник нейтрализуется после реализованной атаки.

Переход процесса (рис. 1) в состояние S_{12} соответствует победе злоумышленника, а переход в состояния S_3, S_5, S_7, S_9, S_{11}, S_{13} соответствует победе системы информационной безопасности.

Моделирование процесса реализации атаки на систему управления сетью синхронизации

Исследование процесса взаимодействия организованного злоумышленника и системы информационной безопасности проведено в среде AnyLogic путем построения имитационной модели (рис. 2) [10, 11].

Исходными данными для проведения имитационного моделирования являются:

· матрица переходных вероятностей из одного состояния в смежное $P=(p_{ij})$;

· функции распределения случайных времен пребывания рассматриваемого процесса атаки в каждом из S_i состояний $F_i(t)$.

Переходные вероятности и функции распределения случайных времен, пребывая в каждом состоянии, характеризуют собой степень оснащенности и квалификации сторон противоборства. Повышенные значения переходных вероятностей для одной из сторон указывают на степень её превосходства в квалификации, оснащенности и имеющихся в наличии ресурсах на каждом этапе проведения атаки. Как правило, число наиболее опытных злоумышленников незначительно на фоне общего числа злоумышленников, а системы информационной безопасности настраиваются на выявление типовых уже известных сценариев атак. Время пребывания процесса проведения атаки в каждом состоянии отражает длительность этапа локализации злоумышленника или преодоления рубежа защиты. Наиболее оснащенные и квалифицированные злоумышленники преодолевают рубежи защиты значительно быстрее рядовых злоумышленников, а наиболее сложная и многоэлементная система безопасности локализует злоумышленника интенсивнее типовой системы.

Учитывая статистику отраженных и реализованных атак, а также опыт технической эксплуатации сетей синхронизации в качестве переходных вероятностей были приняты следующие значения (1):

$$P=\begin{pmatrix} 0 & 0.9 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.7 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.6 & 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0.7 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.05 & 0.95 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (1)$$

Состояния S_2, S_4, S_6, S_8, S_{10}, S_{12} характеризуют действия организованного злоумышленника. Учитывая, что организационно-технические возможности злоумышленника заранее не известны, в качестве распределения времени пребывания в данных состояниях было взято непрерывное равномерное распределение со следующей плотностью вероятности (2):

$$f_i(t)=\begin{cases} \dfrac{1}{b-a}, & t\in[a,b] \\ 0, & t\notin[a,b] \end{cases} \quad (2)$$

Генерирование непрерывного равномерного распределения в среде *AnyLogic* осуществляется с помощью функции *uniform*(*a*,*b*) (таблица 1).

Состояния S_1, S_3, S_5, S_7, S_9, S_{11}, S_{13}, S_{14} характеризуют действия системы информационной безопасности. В данных состояниях система технической эксплуатации сети синхронизации восстанавливает и поддерживает

нормативный режим функционирования, поэтому в качестве распределения времени пребывания в данных состояниях было взято нормальное распределение со следующей плотностью вероятности (3):

$$f_i(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} \quad (3)$$

где μ – математическое ожидание, σ – среднеквадратическое отклонение.

Генерирование нормального распределения в среде *AnyLogic* осуществляется с помощью функции *normal*(σ,μ) (таблица 1).

Исходные данные для построения имитационной модели получены путем анализа статистики технической эксплуатации сетей синхронизации, анализа результатов проведения атак, а также мероприятий по нейтрализации злоумышленников со стороны систем информационной безопасности.

Таким образом, получены следующие результаты (рис. 3–6).

На основе построенной модели можно оценивать вероятностно-временные характеристики процесса взаимодействия организованного злоумышленника и системы информационной безопасности. Необходимо подчеркнуть, что оценивание вероятностно-временных характеристик возможно для каждого из этапов процесса противоборства. Получены результаты по оценке среднего времени атаки, среднего времени нейтрализации злоумышленника, а также вероятностей реализации атаки и её отражения.

По результатам моделирования видно, что среднее время атаки, включая также подбор злоумышленником необходимых исходных данных составляет 836 часов, минимальное время – 700 часов, а максимальное – 957 часов. Среднее время нейтрализации злоумышленника равно 673 часа, при этом данное время колеблется от 600 до 1000 часов. Также по гистограмме времени нейтрализации атаки видно, что значительное число атак локализуется на ранних стадиях.

Следует подчеркнуть, что противоборствующие стороны намерены достичь желаемых целей максимально быстро. Ресурсы, материальные, технические и финансовые, как правило ограничены, поэтому противоборствующие стороны нацелены на достижение целей оптимальным образом. При помощи построенной

Таблица 1

Исходные данные для проведения имитационного моделирования

№	Условное обозначение состояния		Значение	Ед. изм.	№	Условное обозначение состояния		Значение	Ед. изм.
1	S_1	S1	normal(6,168)	час	8	S_8	S8	uniform(21,27)	час
2	S_2	S2	uniform(600,840)	час	9	S_9	S9	normal(0.4,6)	час
3	S_3	S3	normal(0.2,1)	час	10	S_{10}	S10	uniform(36,60)	час
4	S_4	S4	uniform(21,27)	час	11	S_{11}	S11	normal(0.4,10)	час
5	S_5	S5	normal(0.4,2)	час	12	S_{12}	S12	uniform(1,3)	час
6	S_6	S6	uniform(9,15)	час	13	S_{13}	S13	normal(0.4,12)	час
7	S_7	S7	normal(0.4,4)	час	14	S_{14}	S14	normal(1,24)	час

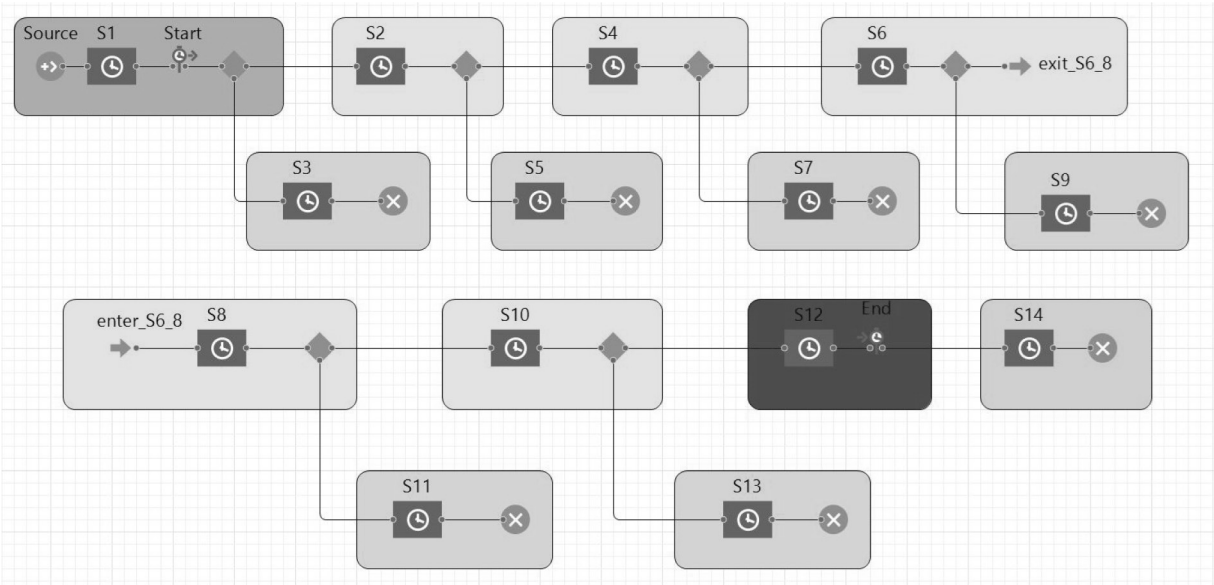

Рис. 2. Имитационная модель процесса взаимодействия организованного злоумышленника и системы информационной безопасности

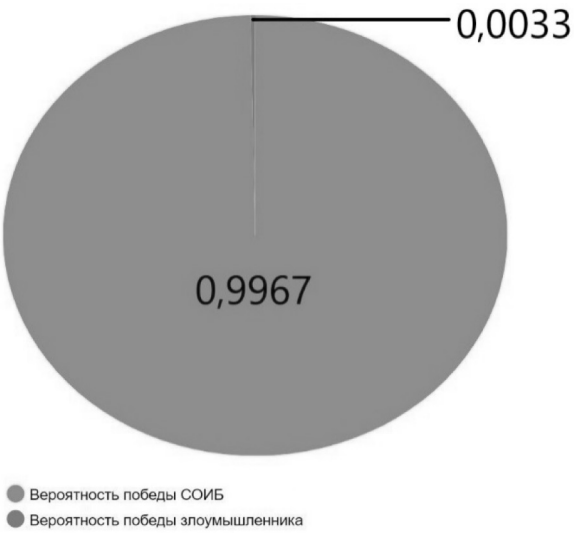

Рис. 3. Вероятность победы злоумышленника и системы информационной безопасности

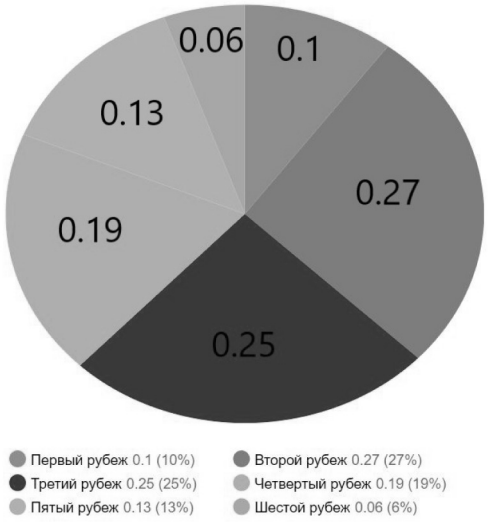

Рис. 4. Доля отраженных атак на различных стадиях нейтрализации злоумышленника

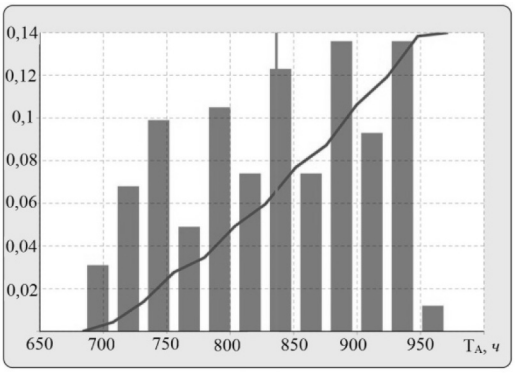

Рис. 5. Гистограмма времени осуществления атаки

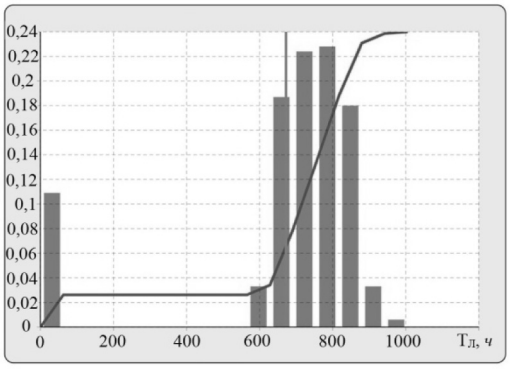

Рис. 6. Гистограмма времени нейтрализации злоумышленника

имитационной модели возможно оценивать среднее время атаки в зависимости от времени нахождения в различных состояниях. В итоге противоборствующие стороны могут обоснованно распределять имеющиеся в наличии ресурсы для решения различных задач по каждому состоянию в соответствии с выбранным планом противоборства. При уменьшении времени нахождения в отдельном состоянии, как правило, имеющиеся в наличии ресурсы расходуются более интенсивно.

Значительное влияние на время нейтрализации злоумышленника оказывают параметры самого злоумышленника и параметры системы информационной безопасности, а также их соотношение на разных этапах взаимодействия. Указанное влияние можно выразить через значения переходных вероятностей между состояниями.

Значительное число ресурсов и уровень компетентности сторон, как правило, соответствуют повышенным значениям переходных вероятностей. При помощи построенной имитационной модели возможно отследить взаимосвязь между переходными вероятностями и временем нейтрализации злоумышленника. Моделирование показывает, что с ростом оснащения системы информационной безопасности среднее время нейтрализации злоумышленника падает. В противном случае, когда злоумышленник способен навязать борьбу, среднее время его нейтрализации возрастает. Производя модернизацию и совершенствование отдельных частей системы информационной безопасности на конкретных рубежах защиты можно достичь изменения значений переходных вероятностей, а значит, достичь вероятности отражения атаки и длительности нейтрализации злоумышленника согласно нормативным значениям.

Заключение

В данной статье получена имитационная модель взаимодействия организованного злоумышленника и системы информационной безопасности при реализации атаки на систему управления сетью синхронизации. Полученная модель может служить основой для оценки администраторами безопасности степени защищенности СУ СС, причем как комплексно, так и для каждого отдельного рубежа защиты.

Имея в наличии статистику отраженных и завершенных атак, а также нормативные значения показателей защищенности, на основе полученных результатов можно адекватно оценить средства защиты, их ресурсный потенциал, сделать вывод об их модернизации или распределения имеющихся мощностей по отдельным рубежам защиты.

При оперативном определении характера атаки, применяемых злоумышленником технических средствах, приведенная модель может служить основой для прогнозирования результатов атаки, времени её завершения или отражения.

Следует отметить, что построенная имитационная модель универсальна и не зависит от исходных данных. При анализе проектируемых или находящихся в эксплуатации сетей синхронизации и систем информационной безопасности возможно получить конкретную реализацию модели с реальными свойствами.

Литература

1. Давыдкин, П. Н. Тактовая сетевая синхронизация / П.Н. Давыдкин, М.Н. Колтунов, А.В. Рыжков. – Москва : Эко-Трендз, 2004. – 205 с.

2. Канаев, А. К. Предложения по построению интеллектуальной системы поддержки принятия решений по управлению сетью тактовой сетевой синхронизации / А.К. Канаев, Е.В. Опарин // Труды учебных заведений связи. – 2017. – Т. 3, № 4. – С. 43–53.

3. Буренин, А. Н. Теоретические основы управления современными телекоммуникационными сетями : монография / А.Н. Буренин, В.И. Курносов. – Москва : Наука, 2011. – 464 с.

4. Канаев, А. К. Полумарковская модель действий злоумышленника при атаке на систему управления сетью тактовой сетевой синхронизации / А.К. Канаев, М.А. Сахарова, Е.В. Опарин // Информация и Космос. – 2020. – № 4. – С. 46–56.

5. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства / М.А. Коцыняк, А.И. Осадчий, М.М. Коцыняк [и др.]. – Санкт-Петербург : ЛО ЦНИИС, 2014. – 126 с.

6. Обзор подходов к определению актуальных угроз информации телекоммуникационным системам и предложения по их совершенствованию / М.А. Ефремов, И.В. Калуцкий, М.О. Таныгин, А.Г. Фрундин // Телекоммуникации. – 2017. – № 5. – С. 27–33.

7. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры / И.Б. Саенко, О.С. Лаута, М.А. Карпов, А.М. Крибель // Электросвязь. – 2021. – № 1. – С. 36–44.

8. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов / И. Котенко, И. Саенко, О. Лаута, А. Крибель // Первая миля. – 2021. – № 6 (98). – С. 64–71.

9. Буйневич, М. В. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации / М.В. Буйневич, В.В. Покусов, К.Е. Израилов // Информатизация и связь. – 2021. – № 4. – С. 66–73.

10. Киселева, М. В. Имитационное моделирование систем в среде AnyLogic : учебно-методическое пособие / М.В. Киселева. – Екатеринбург : УГТУ – УПИ, 2009. – 88 с.

11. Лимановская, О. В. Моделирование производственных процессов в AnyLogic 8.1 : лабораторный практикум / О.В. Лимановская, Т.И. Алферьева. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 136 с.