

Имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации

А.К. Канаев^{1, 2}, Е.В. Опарин³, Е.В. Опарина²

¹ЗАО «Институт телекоммуникаций»,

Санкт-Петербург, 194100, Российская Федерация

²Петербургский государственный университет путей сообщения Императора Александра I,

Санкт-Петербург, 190031, Российская Федерация

³«Гипротрансигналсвязь» – филиал АО «Росжелдорпроект»,

Санкт-Петербург, 192007, Российская Федерация

*Адрес для переписки: Опарин@mail.ru

Информация о статье

Поступила в редакцию 29.09.2021

Поступила после рецензирования 18.11.2021

Принята к публикации 24.11.2021

Ссылка для цитирования: Канаев А.К., Опарин Е.В., Опарина Е.В. Имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 31–42. DOI:10.31854/1813-324X-2021-7-4-31-42

Аннотация: В данной статье приводится обзор взаимодействия противоборствующих сторон и основных этапов конфронтации организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации. Разработана имитационная модель, отражающая все этапы борьбы, позволяющая в зависимости от ресурсов организованного злоумышленника и системы обеспечения информационной безопасности получать вероятностно-временные характеристики результатов противоборства. Проведено моделирование при различных сценариях организации атаки на всех этапах противоборства, начиная от подавляющего преимущества организованного злоумышленника и заканчивая подавляющим преимуществом системы обеспечения информационной безопасности. Полученные результаты в общем случае могут быть использованы администраторами информационной безопасности и сетевыми администраторами для внесения корректив в стратегию организации защиты системы управления сетью тактовой сетевой синхронизации.

Ключевые слова: сеть тактовой сетевой синхронизации, телекоммуникационная система, система управления, атака, уязвимость, злоумышленник, система обеспечения информационной безопасности.

Введение

Одной из основных подсистем телекоммуникационной системы (ТКС) является сеть тактовой сетевой синхронизации (ТСС), которая выполняет функции формирования, передачи и распределения сигналов синхронизации, необходимых для поддержания работоспособного состояния всех цифровых устройств ТКС. Сеть ТСС находится в тесной взаимосвязи с другими подсистемами ТКС, оказывает существенное влияние на их работу и на функционирование всей ТКС в целом. Показатели качества услуг электросвязи неразрывно связаны с

показателями качества функционирования сети ТСС, а сигналы синхронизации и полезные информационные сигналы передаются, как правило, в одних и тех же цифровых потоках и по одним и тем же направляющим системам. Возникновение отказов на сети ТСС способно привести к значительному ухудшению качества передаваемой информации вплоть до полного отказа в предоставлении телекоммуникационных услуг [1, 2].

В силу указанных особенностей сеть ТСС является потенциально привлекательным местом проникновения в ТКС со стороны организованных

злоумышленников с целью оказать деструктивное и разрушающее воздействие. Особая опасность воздействия на сеть ТСС состоит в том, что влияние носит косвенный характер, при котором разрушение сети ТСС приводит к последующему возникновению отказов в ТКС. При возникновении подобных ситуаций могут возникать значительные затруднения по восстановлению процесса функционирования ТКС, так как зачастую невозможно достоверно определить причину возникновения отказов [1, 3].

Анализ различных потенциальных вариантов атак на сеть ТСС, таких как манипуляция синхросигналами, спуфинг в сети ТСС, атака повторного воспроизведения, атака подмены роли устройств и маршрутов в сети ТСС, перехват и удаление сообщений, показал, что наиболее опасной атакой на сеть ТСС, способной нанести максимальный ущерб при ее реализации, является атака на систему управления (СУ) ТСС. При четком соблюдении нормативных документов по построению сети ТСС, она в процессе своего функционирования является самовосстанавливающей системой. Отказ отдельного элемента сети ТСС даже высокого уровня иерархии, а также направляющих систем, систем размножения, распределения и восстановления сигналов синхронизации не приводит моментально к отказу всей сети ТСС. В то время как получение контроля злоумышленником над системой управления ТСС способно моментально привести к значительным отказам и приостановке процесса функционирования всей ТСС [3, 4].

Обзор характеристик противоборствующих сторон

Рассмотрим функционирование сети ТСС в условиях воздействия организованного злоумышленника как процесс взаимодействия сторон, имеющих кардинально противоположные цели. С одной стороны, присутствует организованный злоумышленник, стремящийся осуществить внедрение в СУ сетью ТСС и провести ряд деструктивных воздействий, снизить уровень показателей процесса функционирования сети ТСС, а с другой стороны, в составе ТКС присутствует система обеспечения информационной безопасности (СОИБ), стремящаяся предотвратить проникновение злоумышленника, локализовать его действия, обнаружить и идентифицировать его.

Система СОИБ должна выполнять ряд функций, среди которых основными являются [5–7]:

- осуществление заданной политики безопасности;
- оперативное и обоснованное управление всеми средствами информационной безопасности в соответствии с заданной политикой безопасности;

– осуществление постоянного мониторинга и аудита состояния информационной безопасности в сети ТСС.

К основным задачам системы СОИБ можно отнести:

– управление политикой безопасности, формирование локальных политик безопасности для отдельных комплексов технических средств, устройств и доведения ее до всех устройств локального управления и средств защиты;

– управление конфигурацией объектов и субъектов доступа (управление составом, версиями, компонентами сетевых элементов, устройств защиты информации и их программного обеспечения);

– обеспечение предоставления сервисов защиты распределенным прикладным системам, а также регистрацию защищенных приложений и их ресурсов;

– управление средствами криптографической защиты информации, в частности управление распределением и рассылкой ключей;

– пособытийное протоколирование;

– аудит безопасности, обеспечивающий получение и оценку объективных данных о текущем состоянии защищенности сети ТСС;

– мониторинг безопасности сети ТСС, обеспечивающий получение информации в реальном времени о состоянии сетевых элементов, активности сетевых устройств и о событиях в контексте информационной безопасности;

– поддержка регламентных мероприятий (смена паролей, устройств защиты).

Выполнение заданных функций и решение указанных задач реализуется с помощью элементов, входящих в состав подсистемы СОИБ, а именно: управления доступом; антивирусной защиты; обнаружения вторжений; обеспечения целостности; контроля (анализа) защищенности; безопасного межсетевое взаимодействия; регистрации и учета.

Организованный злоумышленник может характеризоваться различным образом. Основные характеристики организованного злоумышленника представлены на рисунке 1.

По наличию права постоянного или разового доступа в зону технологической сети СУ ТСС злоумышленники подразделяются на два класса:

– злоумышленники, не имеющие прямого доступа к оборудованию технологической сети СУ ТСС и реализующие угрозы из внешних сетей связи (внешние злоумышленники);

– злоумышленники, имеющие доступ к оборудованию технологической сети СУ ТСС и реализующие угрозы непосредственно в технологической сети СУ ТСС (внутренние злоумышленники).

На начальной стадии реализации атаки злоумышленники могут иметь различные возмож-

ности доступа к оборудованию технологической сети СУ ТСС:

- отсутствие прямого доступа (данный уровень характерен для внешних злоумышленников);
- уровень ограниченного доступа (данный уровень характерен для внутренних злоумышленников, которые являются рядовыми сотрудниками организаций по обслуживанию сети ТСС);
- уровень с полномочиями системного администратора (данный уровень характерен для внутренних злоумышленников, которые могут являться администраторами по настройке оборудования сети ТСС, данные злоумышленники могут знать топологию и структуру сети ТСС, характеристики используемого оборудования синхронизации, но в то же время обладать ограниченными сведениями по организации защиты от угроз информационной безопасности);
- уровень с полномочиями администратора безопасности (данный уровень характерен для внутренних злоумышленников, обладающих полной информацией о структуре и архитектуре системы СОИБ).

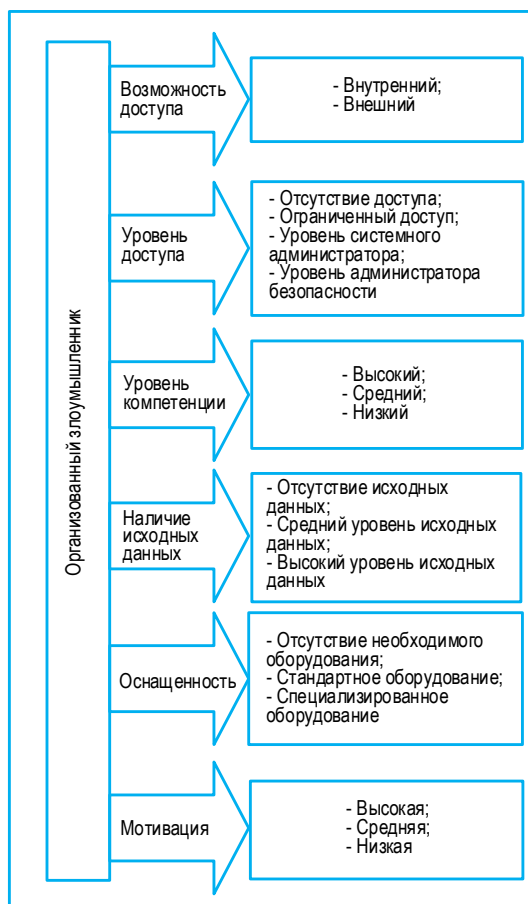


Рис. 1. Основные характеристики организованного злоумышленника

Fig. 1. Key Characteristics of an Organized Attacker

Уровень компетенции злоумышленников также может быть различным. Часть злоумышленников может обладать существенными знаниями о

предметной области функционирования сети ТСС и архитектуре информационных систем, а также иметь значительные навыки программирования. В то же время существуют злоумышленники, использующие готовые программные решения и не понимающие сути происходящих процессов.

Наличие исходных данных об объекте атаки у злоумышленника также может быть различным: от полного отсутствия сведений до наличия полного комплекта документации по процессу функционирования сети ТСС. Инструментарий у злоумышленников также может различаться: от базовых программно-аппаратных комплексов до специализированного оборудования, выполненного на заказ. Существенную роль при реализации атаки также играет мотивация злоумышленника. При более высокой мотивации следует ожидать более интенсивных атак.

Результат процесса взаимодействия организованного злоумышленника и системы СОИБ во многом определяются способностью сторон к добычанию сведений о противоположной стороне, эффективностью применения активных средств воздействия, способностью прогнозировать ситуации, принимать обоснованные и своевременные решения.

Несмотря на противоположность целей, организованного злоумышленника и систему СОИБ можно представить как субъекты, содержащие в себе механизмы выработки управленческих решений, инструменты по добычанию, обработке и передаче информации о противоположной стороне, и инструменты активного воздействия на противоположную сторону.

Процесс взаимодействия организованного злоумышленника и СОИБ

Проведенный анализ различных сценариев атак и мероприятий защиты от них позволил сформировать следующую модель процесса взаимодействия организованного злоумышленника и системы СОИБ. В основе построения данной модели лежит задание графа конфликтно обусловленных состояний, показанного на рисунке 2.

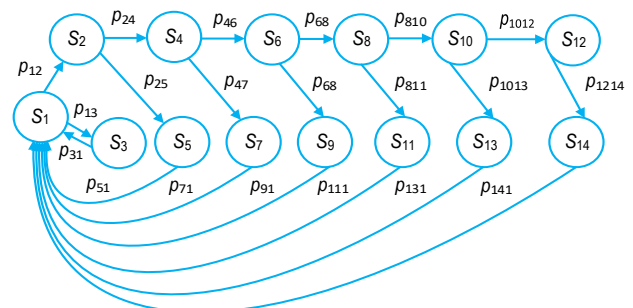


Рис. 2. Процесс взаимодействия организованного злоумышленника и системы СОИБ

Fig. 2. The Process of Interaction between an Organized Attacker and the IS Maintenance System

Как правило, злоумышленник реализует атаку в несколько этапов. Основными этапами при этом являются [1, 2, 4]:

- получение исходных данных об объекте атаки из открытых источников и методами социальной инженерии;
- поиск активных узлов и автоматизированных рабочих мест управления технологической сетью ТСС;
- определение структуры технологической сети СУ сетью ТСС;
- определение точек входа в технологическую сеть СУ сетью ТСС;
- анализ уязвимостей точек входа в технологическую сеть СУ сетью ТСС и поиск инструментария по их реализации;
- обход системы обнаружения вторжений и непосредственная реализация атаки.

Каждый из указанных этапов может быть либо реализован злоумышленником, в результате чего он перейдет к следующему, либо система СОИБ обнаружит вторжение, локализует злоумышленника и восстановит процесс функционирования сети ТСС в соответствии с нормативными значениями.

С учетом вышеизложенного модель процесса взаимодействия организованного злоумышленника и системы СОИБ будет включать следующие состояния:

S_1 – исходное состояние, которое характеризуется процессом функционирования сети ТСС в соответствии с нормативными значениями и отсутствием активных действий со стороны злоумышленника и системы СОИБ;

S_2 – злоумышленник получил необходимые ему данные о СУ сетью ТСС из открытых источников и методами социальной инженерии;

S_3 – система СОИБ локализовала злоумышленника на этапе сбора данных из открытых источников и методами социальной инженерии;

S_4 – злоумышленник осуществил поиск активных узлов и автоматизированных рабочих мест (АРМ) технологической сети СУ сетью ТСС;

S_5 – система СОИБ локализовала злоумышленника на этапе поиска активных узлов и АРМ технологической сети СУ сетью ТСС;

S_6 – злоумышленник определил структуру технологической сети СУ сетью ТСС;

S_7 – система СОИБ локализовала злоумышленника на этапе определения структуры технологической сети СУ сетью ТСС;

S_8 – злоумышленник определил точки входа в технологическую сеть СУ сетью ТСС;

S_9 – система СОИБ локализовала злоумышленника на этапе определения точек входа в технологическую сеть СУ сетью ТСС;

S_{10} – злоумышленник провел анализ уязвимостей точек входа в технологическую сеть СУ сетью ТСС и осуществил поиск инструментария по их реализации;

S_{11} – система СОИБ локализовала злоумышленника на этапе анализа уязвимостей точек входа в технологическую сеть СУ сетью ТСС;

S_{12} – злоумышленник осуществил обход системы обнаружения вторжений и реализовал атаку;

S_{13} – система СОИБ локализовала злоумышленника на этапе обхода системы обнаружения вторжений;

S_{14} – система СОИБ локализовала злоумышленника на этапе реализованной атаки.

Переход процесса взаимодействия организованного злоумышленника и системы СОИБ в состоянии S_{12} будет означать победу злоумышленника, а переход в состояния $S_3, S_5, S_7, S_9, S_{11}, S_{13}$ будет означать победу системы СОИБ.

Для исследования процесса противостояния организованного злоумышленника и системы СОИБ была построена имитационная модель (рисунок 3) в среде *AnyLogic* [8, 9]. Исходные данные для проведения имитационного моделирования приведены в таблице 1.

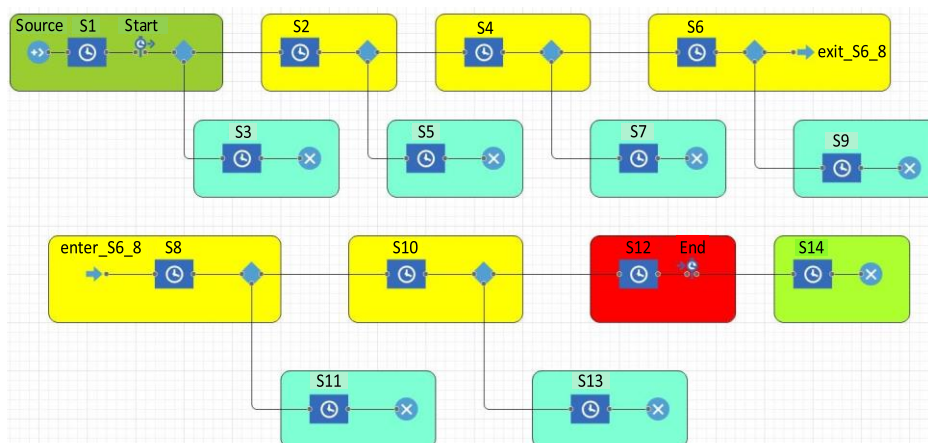
















Рис. 3. Имитационная модель процесса противостояния организованного злоумышленника и системы обеспечения информационной безопасности

Fig. 3. Simulation Model of the Process of Confrontation between an Organized Attacker and an Information Security System

ТАБЛИЦА 1. Исходные данные для проведения имитационного моделирования

TABLE 1. Initial Data for Simulation

№ п/п	Название состояния	Условное обозначение	Значение	Единицы измерения	
1.	Исходное состояние, которое характеризуется процессом функционирования сети ТСС в соответствии с нормативными значениями и отсутствием активных действий со стороны злоумышленника и системы СОИБ	S_1	 S1	normal(6,168)	час
2.	Состояние, когда злоумышленник получил необходимые ему данные о СУ сетью ТСС из открытых источников и методами социальной инженерии	S_2	 S2	uniform(600,840)	час
3.	Состояние, когда система СОИБ локализовала злоумышленника на этапе сбора данных из открытых источников и методами социальной инженерии	S_3	 S3	normal(0.2,1)	час
4.	Состояние, когда злоумышленник осуществил поиск активных узлов и АРМов управления технологической сетью ТСС	S_4	 S4	uniform(21,27)	час
5.	Состояние, когда система СОИБ локализовала злоумышленника на этапе поиска активных узлов и АРМов технологической сети СУ сетью ТСС	S_5	 S5	normal(0.4,2)	час
6.	Состояние, когда злоумышленник определил структуру технологической сети СУ сетью ТСС	S_6	 S6	uniform(9,15)	час
7.	Состояние, когда система СОИБ локализовала злоумышленника на этапе определения структуры технологической сети СУ сетью ТСС	S_7	 S7	normal(0.4,4)	час
8.	Состояние, когда злоумышленник определил точки входа в технологическую сеть СУ сетью ТСС	S_8	 S8	uniform(21,27)	час
9.	Состояние, когда система СОИБ локализовала злоумышленника на этапе определения точек входа в технологическую сеть СУ сетью ТСС	S_9	 S9	normal(0.4,6)	час
10.	Состояние, когда злоумышленник провел анализ уязвимостей точек входа в технологическую сеть СУ сетью ТСС и осуществил поиск инструментария по их реализации	S_{10}	 S10	uniform(36,60)	час
11.	Состояние, когда система СОИБ локализовала злоумышленника на этапе анализа уязвимостей точек входа в технологическую сеть СУ сетью ТСС	S_{11}	 S11	normal(0.4,10)	час
12.	Состояние, когда злоумышленник осуществил обход системы обнаружения вторжений и реализовал атаку	S_{12}	 S12	uniform(1,3)	час
13.	Состояние, когда система СОИБ локализовала злоумышленника на этапе обхода системы обнаружения вторжений	S_{13}	 S13	normal(0.4,12)	час
14.	Состояние, когда система СОИБ локализовала злоумышленника на этапе реализованной атаки	S_{14}	 S14	normal(1,24)	час

Исходные данные взяты, исходя из практики эксплуатации сетей ТСС и анализа проведения различных атак организованных злоумышленников, а также результатов локализации данных атак средствами СОИБ. Состояния S_2 , S_4 , S_6 , S_8 , S_{10} , S_{12} характеризуют действия организованного злоумышленника. Учитывая, что организационно-технические возможности злоумышленника зара-

нее не известны, в качестве распределения времени пребывания в данных состояниях было взято равномерное распределение. Состояния S_1 , S_3 , S_5 , S_7 , S_9 , S_{11} , S_{13} , S_{14} характеризуют действия системы СОИБ. В данных состояниях система технической эксплуатации ТСС восстанавливает и поддерживает нормативный режим функционирования ТСС, поэтому в качестве распределения времени пре-

бывания в данных состояниях было взято нормальное распределение.

Переходные вероятности из одного состояния в другое (1) указывают на характер противоборства между злоумышленником и системой СОИБ, а также на ресурсы противоборствующих сторон.

Следует отметить, что чем глубже злоумышленник преодолевает рубежи обороны СУ ТСС, тем, как правило, противодействие со стороны системы СОИБ возрастает. Результаты проведенного моделирования приведены на рисунках 4–7.

$$P = \begin{pmatrix} 0 & 0,9 & 0,1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0,7 & 0,3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0,6 & 0,4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,5 & 0,5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,3 & 0,7 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,05 & 0,95 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (1)$$

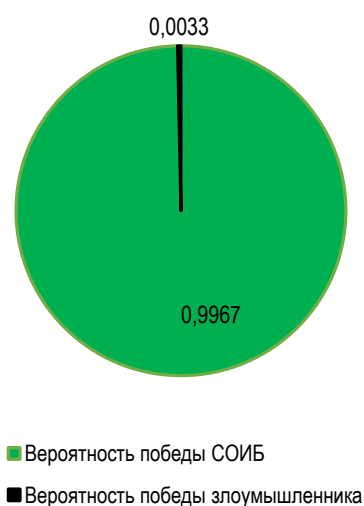


Рис. 4. Оценка вероятностей достижения цели злоумышленником и СОИБ

Fig. 4. Assessment of the Probabilities of Achieving a Goal by an Attacker and an Information Security System

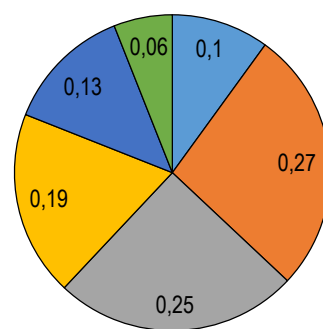


Рис. 5. Оценка отраженных атак относительно стадии их выявления

Fig. 5. Assessment of Reflected Attacks in Relation to the Stage of their Detection

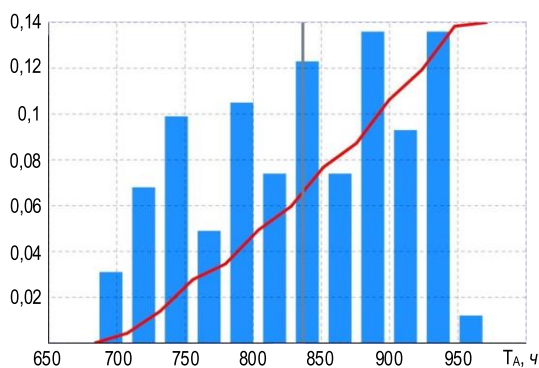


Рис. 6. Гистограмма времени реализации атаки

Fig. 6. Histogram of Attack Implementation Time

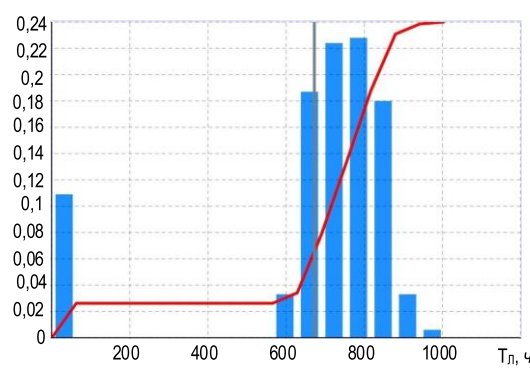
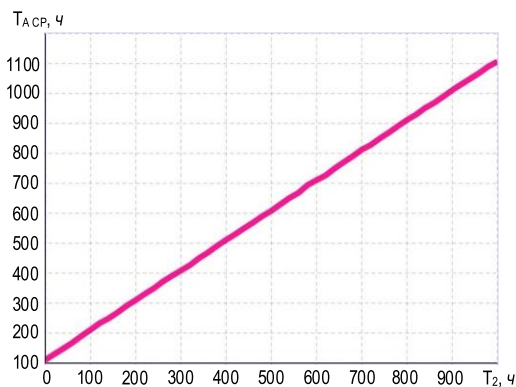


Рис. 7. Гистограмма времени локализации атаки

Fig. 7. Histogram of Attack Localization Time

Данная модель позволяет оценивать вероятностно-временные характеристики процесса противоборства между организованным злоумышленником и системой СОИБ. В статье приведена оценка среднего времени реализации атаки, среднего времени локализации деятельности злоумышленника, а также вероятностей завершения и отражения атаки. Результаты проведенного моделирования показывают, что среднее время реализации атаки T_{A_CP} на сеть ТСС составляет 836 ч, минимальное время составляет 700 ч, а максимальное – 957 ч. Среднее время локализации злоумышленника составляет 673 ч, при этом интервал локализации варьируется от 600 до 1000 ч. Также из гистограммы времени локализации атаки видно, что значительное число атак отражается на ранних стадиях.

Данная модель может служить основой для оценки степени защищенности СУ ТСС, причем как комплексно, так и для каждого отдельного рубежа защиты. Имея в наличии статистику отраженных и завершённых 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 средств, приведенная модель может служить основой для прогнозирования результатов атаки, времени ее завершения или отражения.



Влияние отдельных состояний на длительность реализации атаки организованным злоумышленником

Злоумышленник, осуществляющий атаку на СУ сети ТСС, имеет стремление сократить длительность всей атаки и получить доступ к сети ТСС в максимально короткие сроки. Финансовые, технические и материальные ресурсы, находящиеся в распоряжении злоумышленника, могут быть различным образом распределены между состояниями для выполнения задачи получения доступа. С учетом ограниченности финансовых, технических и материальных ресурсов злоумышленник стремится выработать такую стратегию расходования ресурсов, чтобы осуществить доступ в максимально короткие сроки.

Построенная имитационная модель позволяет оценивать среднюю длительность реализации атаки организованным злоумышленником в зависимости от длительности нахождения процесса противоборства в отдельном состоянии. Отметим, что сокращение времени нахождения в конкретном состоянии, как правило, связано с более интенсивным расходованием ресурсов для данного состояния.

Таким образом, злоумышленник может распределять имеющиеся ресурсы для решения разноплановых задач по отдельным состояниям в соответствии с выбранной стратегией сокращения длительности получения доступа. Результаты моделирования приведены на рисунке 8.

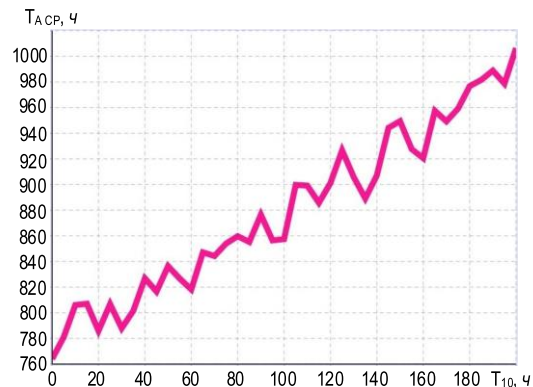


Рис. 8. Зависимость среднего времени атаки организованным злоумышленником от длительности нахождения в состояниях S_2 и S_{10}

Fig. 8. Dependence of the Average Attack Time by an Organized Attacker on the Duration of Being in States S_2 and S_{10}

По результатам моделирования видно, что в соответствии с приведенными исходными данными (см. таблицу 1) и матрицей переходных вероятностей (1), среднее время атаки организованным злоумышленником существенно зависит от времени пребывания в состоянии S_2 и меньше от пребывания в остальных состояниях. Полученный результат можно объяснить тем, что в состоянии S_2 злоумышленник осуществляет сбор исходных данных об объекте атаки и в данном состоянии он наименее подвержен обнаружению. Учитывая эти ре-

зультаты, злоумышленник может наиболее рационально использовать существенную часть ресурсов в те моменты времени, когда готовит свою атаку, т. к. сокращение времени пребывания в состоянии S_2 существенно повлияет на сокращение длительности всей атаки. Если у злоумышленника есть определенные требования к длительности цикла реализации атаки, он может выбирать соответствующую стратегию расходования ресурсов и пребывания в конкретных состояниях для получения доступа к сети ТСС.

Влияние отдельных состояний на длительность локализации организованного злоумышленника системой обеспечения информационной безопасности

В свою очередь, сетевые администраторы и администраторы безопасности имеют стремление сократить время обнаружения злоумышленника, его локализации и поддержания процесса функционирования сети ТСС. Ресурсы, находящиеся в распоряжении сетевых администраторов и администраторов безопасности, также ограничены и могут быть различным образом распределены между состояниями для выполнения общей задачи. С

учетом ограниченности финансовых, технических и материальных ресурсов в системе СОИБ, сетевые администраторы и администраторы безопасности стремятся выработать такую стратегию расходования ресурсов, чтобы сократить время обнаружения организованного злоумышленника.

Построенная имитационная модель позволяет оценивать среднее время локализации злоумышленника в зависимости от длительности нахождения в отдельном состоянии. Результаты моделирования приведены на рисунках 9–11.

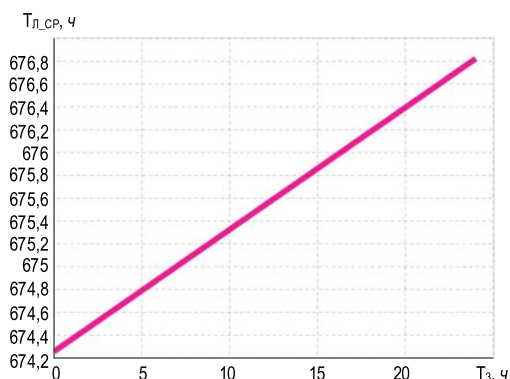
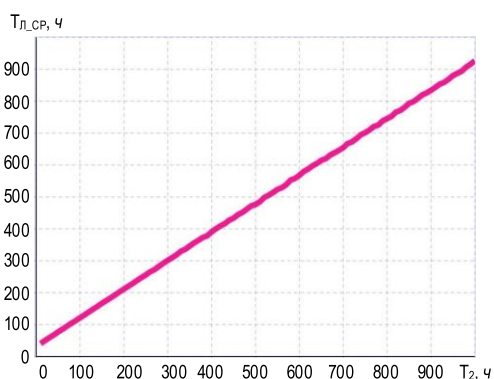


Рис. 9. Зависимость среднего времени локализации злоумышленника от длительности нахождения в состояниях S_2 и S_3
Fig. 9. Dependence of the Average Time of an Attacker's Localization on the Duration of Being in States S_2 and S_3

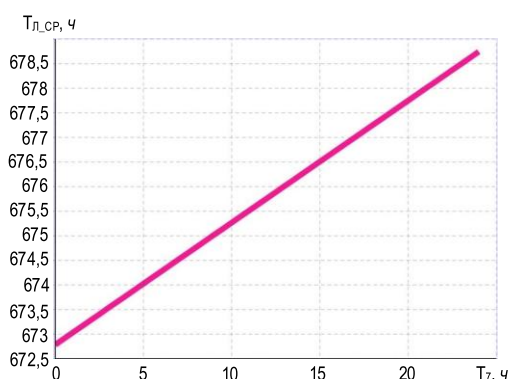
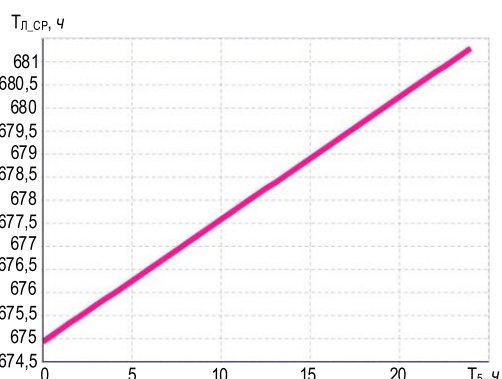


Рис. 10. Зависимость среднего времени локализации злоумышленника от длительности нахождения в состояниях S_5 и S_7
Fig. 10. Dependence of the Average Time of an Intruder's Localization on the Duration of Being in States S_5 and S_7

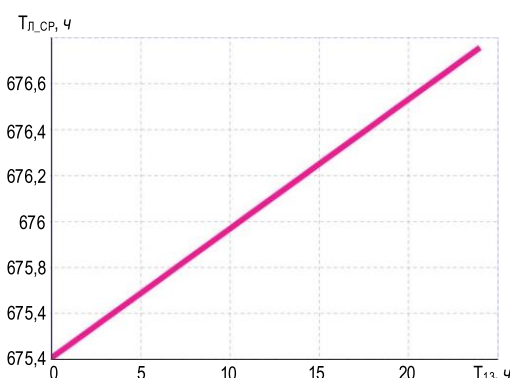
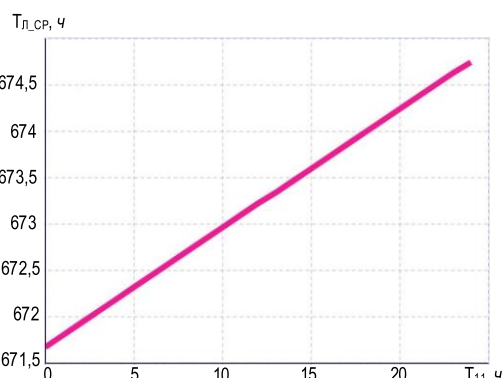


Рис. 11. Зависимость среднего времени локализации злоумышленника от длительности нахождения в состояниях S_{11} и S_{13}
Fig. 11. Dependence of the Average Time of an Attacker's Localization on the Duration of Being in States S_{11} and S_{13}

Среднее время локализации злоумышленника существенно зависит от времени пребывания в состоянии S_2 . Данный факт объясняется тем, что в указанном состоянии злоумышленник занимает активную позицию по сравнению с функционированием средств защиты и его деятельность на текущем этапе наиболее скрытна. Злоумышленник может долго выжидать, подбирая наиболее подходящий момент для атаки, что, соответственно, сказывается на общем времени его локализации. В остальных состояниях злоумышленник более активен, а значит, более заметен, и вынужден действовать быстро. В целом с возрастанием времени пребывания в состояниях, время локализации злоумышленника возрастает, но с разной интенсивностью. Отслеживая динамику данных интенсивностей, сетевые администраторы и администраторы безопасности могут оптимально распределить ресурсы по рубежам защиты, с целью наиболее оперативной локализации злоумышленника.

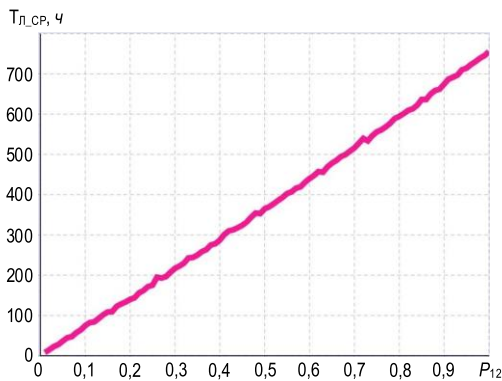


Рис. 12. Зависимость среднего времени локализации злоумышленника от вероятности переходов p_{12} и p_{13}

Fig. 12. Dependence of the Average Time of Localization of an Attacker on the Probability of Transitions p_{12} and p_{13}

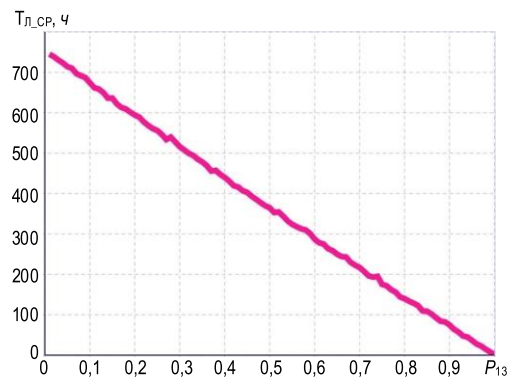
Исходя из результатов приведенного моделирования, видно, что на отдельных этапах противоборства, с ростом оснащенности и ресурсов системы СОИБ среднее время его локализации уменьшается. Наоборот, в случаях, когда злоумышленник может навязать борьбу, среднее время локализации злоумышленника возрастает.

Указанные взаимосвязи и значения переходных вероятностей, исходя из требований к длительности времени локализации злоумышленника, могут служить основой для изменения технических характеристик отдельных подсистем системы СОИБ на различных рубежах защиты. Производя модернизацию отдельных подсистем системы СОИБ, возможно добиться изменения значений переходных вероятностей, а, следовательно, привести вероятность отражения атаки и длительность локализации злоумышленника к нормативным значениям.

Длительность времени локализации злоумышленника в зависимости от соотношения сил на различных этапах противоборства

Существенную роль на длительность времени локализации злоумышленника оказывают характеристики самого злоумышленника, системы СОИБ и соотношение их ресурсов на различных этапах противоборства. Данное влияние выражается в значениях переходных вероятностей между состояниями процесса противоборства. Высокие значения ресурсов и подготовленности, как правило, характерны для повышенных значений переходных вероятностей, связанных с деятельностью злоумышленника или системы СОИБ.

Представленная имитационная модель противоборства злоумышленника и системы СОИБ позволяет отслеживать взаимосвязь между значениями переходных вероятностей и средним временем локализации злоумышленника. Примеры данных взаимосвязей приведены на рисунке 12.



Рассматривать среднее время атаки от значений переходных вероятностей нет особой необходимости, так как на рассмотрение попадают только реализованные атаки, при которых на каждом этапе атаки злоумышленник оказался сильнее системы СОИБ. При этом общее время атаки складывается из времен тех операций, которые осуществил злоумышленник в каждом состоянии. Данное положение подтверждается следующими графиками (рисунок 13).

Заключение

Сеть ТСС является важной подсистемой ТКС, непосредственно влияющей на качество предоставления услуг связи, в связи с чем она является потенциальным объектом атаки со стороны организованных злоумышленников. Особый класс угроз по отношению к сети ТСС представляют собой угрозы при реализации атак на СУ ТСС, способных нанести значительный вред процессу функционирования сети ТСС.

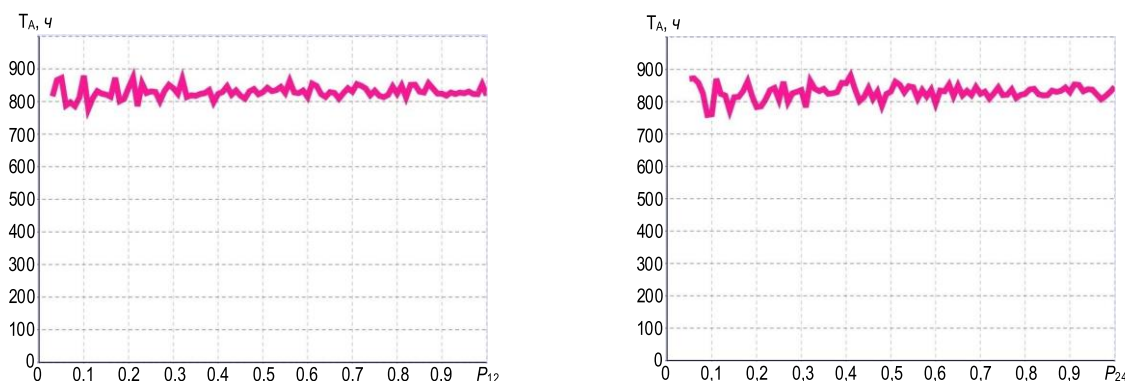


Рис. 13. Зависимость среднего времени атаки организованным злоумышленником от вероятности переходов p_{12} и p_{24}
 Fig. 13. Dependence of the Average Attack Time by an Organized Attacker on the Probability of Transitions p_{12} and p_{24}

В работе получена имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации. В качестве исходных данных для построения модели взяты результаты анализа отдельных средств защиты СУ сети ТСС и всей сети ТСС, статистики архива отраженных и завершенных атак, а также различных методов тестирования. Данная модель включает в себя все этапы противоборства, а также учитывает ресурсы противоборствующих сторон на различных этапах борьбы, выраженные через значения переходных вероятностей и длительности времен нахождения в состояниях.

Полученная модель позволяет производить оценку результатов противоборства на различных этапах борьбы, а также в результате всего противостояния в целом в зависимости от характеристик организованного злоумышленника и системы СОИБ. В результате проведенного моделирования получены зависимости длительностей реализации атаки и длительностей локализации злоумышленника при различных сценариях противоборства, а также характеристиках злоумышленника и системы СОИБ. Полученная имитационная модель и результаты моделирования могут быть использованы администраторами безопасности и сетевыми администраторами для внесения корректив в стратегию защиты СУ ТСС.

Вопросы моделирования угроз информационной безопасности, а также процессов взаимодействия систем СОИБ и организованных злоумышленников активно освещены как в зарубежной, например [10–11], так и в отечественной литературе [12–16]. Анализ различных литературных источников показал, что для исследования вопросов информационной безопасности, учитывая особую актуальность данных вопросов, применяются практически все методы моделирования

Тем не менее, вопросам информационной безопасности в сетях ТСС и системах передачи точного времени пока уделено недостаточно внимания. В связи с чем в данной статье и представлены результаты по формированию модели противоборства организованного злоумышленника и системы СОИБ. Аппарат имитационного моделирования выбран, учитывая особую сложность существующих и перспективных сетей ТСС, а также систем их управления при многообразии различных вариантов атак.

Представляемый математический аппарат для описания процесса взаимодействия системы СОИБ и организованных злоумышленников в сетях ТСС применен впервые. В качестве перспективной области применения можно отметить сеть ТСС железнодорожного транспорта, которая уже сейчас насчитывает тысячи элементов, а после планируемой в ближайшие годы модернизации может значительно вырасти.

Список используемых источников

1. Давыдкин П.Н., Колтунов М.Н., Рыжков А.В. Тактовая сетевая синхронизация. М.: Эко-Трендз, 2004. 205 с.
2. Канаев А.К., Опарин Е.В. Предложения по построению интеллектуальной системы поддержки принятия решений по управлению сетью тактовой сетевой синхронизации // Труды учебных заведений связи. 2017. Т. 3. № 4. С. 43–53.
3. Буренин А.Н., Курносков В.И. Теоретические основы управления современными телекоммуникационными сетями. М.: Наука, 2011. 464 с.
4. Канаев А.К., Опарин Е.В., Сахарова М.А. Полумарковская модель действий злоумышленника при атаке на систему управления сетью тактовой сетевой синхронизации // Информация и космос. 2020. № 4. С. 46–56.
5. Коцыняк М.А., Осадчий А.И., Коцыняк М.М., Лаута О.С., Дементьев В.Е., Васюков Д.Ю. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. СПб.: ЛО ЦНИИС, 2014. 126 с.

6. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2017. 434 с.
7. Ефремов М.А., Калущий И.В., Таныгин М.О., Фрундин А.Г. Обзор подходов к определению актуальных угроз информации телекоммуникационным системам и предложения по их совершенствованию // Телекоммуникации. 2017. № 5. С. 27–33.
8. Киселева М.В. Имитационное моделирование систем в среде AnyLogic. Екатеринбург: УГТУ – УПИ, 2009. 88 с.
9. Лимановская О.В., Алферьева Т.И. Моделирование производственных процессов в AnyLogic 8.1: лабораторный практикум. Екатеринбург: Издательство Уральского университета, 2019. 136 с.
10. Zedan A. El-Farra, N.H. A machine-learning approach for identification and mitigation of cyberattacks in networked process control systems // Chemical Engineering Research and Design. 2021. Vol. 176. PP. 102–115. DOI:10.1016/j.cherd.2021.09.016
11. Khazaei J. Cyberattacks with limited network information leading to transmission line overflow in cyber-physical power systems // Sustainable Energy, Grids and Networks. 2021. Vol. 27. DOI:10.1016/j.segan.2021.100505
12. Kothenko I., Saenko I., Lauta O., Karpov M. Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks // Energies. 2021. Vol. 14. Iss. 18. DOI:10.3390/en14185963
13. Саенко И.Б., Лаута О.С., Карпов М.А., Крибель А.М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. 2021. № 1. СС. 36–44. DOI:10.34832/ELSV.2021.14.1.004
14. Котенко И., Саенко И., Лаута О., Крибель А. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6(98). С. 64–71. DOI:10.22184/2070-8963.2021.98.6.64.70
15. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. СС. 66–73. DOI:10.34219/2078-8320-2021-12-4-66-73
16. Буйневич М.В., Власов Д.С. Аналитический обзор моделей инсайдеров информационных систем // Информатизация и связь. 2020. № 6. С. 92–98.

* * *

A Simulation Model of the Confrontation between an Organized Attacker and an Information Security System in the Implementation of an Attack on a Network Management System of Clock Network Synchronization

A. Kanaev^{1, 2} , E. Oparin³ , E. Oparina² 

¹Institute of Telecommunications, CJSC,
St. Petersburg, 194100, Russian Federation

²Emperor Alexander I St. Petersburg State Transport University,
St. Petersburg, 190031, Russian Federation

³Giprotranssignalsvyaz – branch of Roszheldorproekt, JSC,
St. Petersburg, 192007, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-31-42

Received 29th September 2021

Revised 18th November 2021

Accepted 24th November 2021

For citation: Kanaev A., Oparin E., Oparina E. A Simulation Model of the Confrontation between an Organized Attacker and an Information Security System in the Implementation of an Attack on a Network Management System of Clock Network Synchronization. *Proc. of Telecom. Universities*. 2021;7(4):31–42. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-31-42

Abstract: This article provides an overview of the interaction between the warring parties and the main stages of the confrontation between the organized attacker and the information security system in the implementation of an attack on the network management system of clock network synchronization. A simulation model has been developed that reflects all stages of the struggle, which allows, depending on the resources of an organized attacker

and the information security system, to obtain probabilistic and temporal characteristics of the results of the confrontation. Simulation has been carried out for various scenarios of organizing an attack at all stages of the confrontation, from the overwhelming advantage of an organized malefactor to the overwhelming advantage of an information security system. The results obtained in the general case can be used by security administrators and network administrators to make adjustments to the strategy of organizing the protection of the network management system of clock network synchronization.


Keywords: clock network synchronization network, telecommunication system, control system, attack, vulnerability, attacker, information security system.

References


1. Davydkin P.N., Koltunov M.N., Ryzhkov A.V. *Clock Network Synchronization*. Moscow: Eco-Trends Publ.; 2004. 205 p. (in Russ.)
2. Kanaev A., Oparin E. Proposals for Intellectual System Construction of Support of Decision-Making Management of Network Synchronization. *Proc. of Telecom. Universities*. 2017;3(4):43–53. (in Russ.)
3. Burenin A.N., Kurnosov V.I. *Theoretical Foundations of Modern Telecommunication Networks Management*. Moscow: Nauka Publ.; 2011. 464 p. (in Russ.)
4. Kanaev A.K., Oparin E.V., Sakharova M.A. Semi-Markov Model of an Attacker's Actions in an Attack on a Network Management System of Clock Network Synchronization. *Information and Space*. 2020;4:46–56. (in Russ.)
5. Kotsynyak M.A., Osadchiy A.I., Kotsynyak M.M., Lauta O.S., Dementyev V.E., Vasyukov D.Yu. *Ensuring the Stability of Information and Telecommunication Networks in the Context of Information Confrontation*. St. Petersburg: Leningrad Branch of the Central Research Institute of Communications Publ.; 2014. 126 p. (in Russ.)
6. Biryukov A.A. *Information Security: Defense and Attack*. Moscow: DMK Press Publ.; 2017. 434 p. (in Russ.)
7. Yefremov M.A., Kalutskiy I.V., Tanygin M.O., Frundin A.G. Approach Review for Actual Threat Allocation for Telecommunication System Information and Suggestions for System Improvement. *Telecommunications*. 2017;5:27–33. (in Russ.)
8. Kiseleva M.V. *Simulation Modeling of Systems in the Anylogic Environment*. Ekaterinburg: Ural State Technical University Publ.; 2009. 88 p. (in Russ.)
9. Limanovskaya O.V., Alferieva T.I. *Modeling Production Processes in AnyLogic 8.1: Laboratory Practice*. Yekaterinburg: Ural Federal University Publ.; 2019. 136 p. (in Russ.)
10. Zedan A. El-Farra, N.H. A machine-learning approach for identification and mitigation of cyberattacks in networked process control systems. *Chemical Engineering Research and Design*. 2021;176:102–115. DOI:10.1016/j.cherd.2021.09.016
11. Khazaei J. Cyberattacks with limited network information leading to transmission line overflow in cyber-physical power systems. *Sustainable Energy, Grids and Networks*. 2021;27. DOI:10.1016/j.segan.2021.100505
12. Kothenko I., Saenko I., Lauta O., Karpov M. Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks. *Energies*. 2021;14(18). (in Russ.) DOI:10.3390/en14185963
13. Saenko I.B., Lauta O.S., Karpov M.A., Kribel A.M. Model of Threats to Information and Telecommunication Network Resources as a Key Asset of Critical Infrastructure. *Electrosvyaz*. 2021;1:36–44. (in Russ.) DOI:10.34832/ELSV.2021.14.1.004
14. Kothenko I., Saenko I., Lauta O., Kribel A. The Method of Early Detection of Cyber Attacks Based on Integration of Fractal Analysis and Statistical Methods. *Last mile*. 2021;6(98):64–71. (in Russ.) DOI:10.22184/2070-8963.2021.98.6.64.70
15. Buinevich M.V., Pokussov V.V., Izrailov K.E. Threats Model of Information and Technical Interaction in the Integrated Information Protection System. *Informatizaciya i svyaz*. 2021;4:66–73. (in Russ.) DOI:10.34219/2078-8320-2021-12-4-66-73
16. Buinevich M.V., Vlasov D.S. Analytical Review of Models of Information Systems. *Informatizaciya i svyaz*. 2020;6: 92–98. (in Russ.)

Сведения об авторах:


КАНАЕВ
Андрей Константинович

доктор технических наук, профессор, заместитель генерального директора по спецпроектам ЗАО «Институт телекоммуникаций», профессор кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, Kanaev@itian.ru
 <https://orcid.org/0000-0002-1578-2629>

ОПАРИН
Евгений Валерьевич

кандидат технических наук, инженер I категории отдела связи «Гипротрансигналсвязь» – филиал АО «Росжелдорпроект», OnapuH@mail.ru
 <https://orcid.org/0000-0003-4622-9161>

ОПАРИНА
Екатерина Владимировна

кандидат технических наук, старший преподаватель кафедры «Механика и прочность материалов и конструкций» Петербургского государственного университета путей сообщения Императора Александра I, sirayaekaterina@mail.ru
 <https://orcid.org/0000-0003-3380-506X>