УДК 621.39

Обобщенная модель действий злоумышленника на начальном этапе реализации атаки на систему управления сетью синхронизации

Generalized model of the attacker's actions at the initial stage of the cyberattack on a synchronization network control system

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

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

Привалов / Privalov A.
Александр Андреевич
(Privalov.1985@yandex.ru)
кандидат технических наук, доцент.
ФГБОУ ВО «Российский университет транспорта»,
доцент кафедры управления и защиты информации.
г. Москва

Ключевые слова: полумарковская модель – semi-Markov model; сеть синхронизации – synchronization network; телекоммуникационная система –telecommunication system; система управления – control system; атака – cyberattack; уязвимость – vulnerability; злоумышленник – the attacker; система обеспечения информационной безопасности – information security system.

В данной статье приводится оценка защищенности системы управления (СУ) сетью синхронизации телекоммуникационной системы от действий организованного злоумышленника на начальном этапе реализации атаки. Предлагается обобщённая полумарковская модель процесса, отражающего основные этапы реализации атаки организованного злоумышленника с выделением состояний, характеризующихся отличительным набором воздействий на СУ сетью синхронизации. На основе разработанной полумарковской модели производится вычисление стационарных характеристик защищенности СУ сетью синхронизации.

The article discusses an estimating of the security of the telecommunication system synchronization network control system from the actions of an organized attacker at the initial stage of a cyberattack. The authors propose a generalized semi-Markov model of the process reflecting the main stages of the implementation of an organized attacker's actions with the allocation of states characterized by a distinctive set of impacts on the synchronization network control system. On the basis of the developed semi-Markov model, the stationary characteristics of the security of the synchronization network control system are calculated.

Введение

Эффективное функционирование сетей связи и выполнение всех требований потребителей по обеспечению услугами связи на должном уровне основано на адекватном, оптимальном, оперативном, устойчивом и непрерывном управлении всеми подсистемами телекоммуникационной системы.

Устойчивое функционирование телекоммуникационной системы (ТКС) обеспечивается множеством подсистем, среди которых одной из наиболее важных является подсистема синхронизации.

Основной задачей сети синхронизации является формирование, передача, распределение и доставка сигналов синхронизации до цифрового оборудования ТКС с целью поддержания согласованного их взаимодействия [1–4]. Возникновение отказов в сети синхронизации и отклонение характеристик сигналов синхронизации от требуемых значений способно привести к значительному ухудшению качества передаваемой информации вплоть до полного отказа в предоставлении телекоммуникационных услуг. Указанная особенность свидетельствует о том, что особую важность приобретает процесс управления сетью синхронизации с обеспечением требуемых показателей её функционирования [5]. Учитывая специфику функционирования сети синхронизации и процессы, обеспечивающие её управление, можно сделать вывод, что СУ сетью синхронизации является потенциальным объектом атаки со стороны организованных злоумышленников.

Основные этапы реализации атаки на систему управления сетью синхронизации

В общем случае можно выделить 3 этапа реализации атаки организованным злоумышленником на СУ сетью синхронизации (рис. 1) [6–8]:

– предварительный сбор информации;
– реализация атаки;
– завершение атаки.

Обычно под атакой понимают именно второй этап, однако успешность реализации атаки существенно зависит и от первого и третьего этапов [6–8].

Этап предварительного сбора информации является основополагающим. Успешная реализация данного этапа является ключом к успешной реализации атаки. На данном этапе определяется цель атаки, как получение доступа к СУ сетью синхронизации, осуществляется сбор максимального количества информация о СУ сетью синхронизации, например, конфигурация и топология узлов СУ сетью синхронизации, тип установленной аппаратуры и программного обеспечения, а также любая вспомогательная информация, которая может помочь злоумышленнику в реализации атаки. На основе полученной информации злоумышленником проводится анализ доступных уязвимостей цели атаки, воздействуя на которые можно получить доступ к СУ сетью синхронизации. На основании анализа доступных уязвимостей злоумышленник выбирает необходимый инструментарий. Подобрав необходимый инструментарий для реализации атаки, злоумышленник переходит ко второму этапу. Выбор способа атаки также существенно зависит от квалификации злоумышленника.

Полумарковская модель действий злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации

Проведенный анализ процесса проведения атак позволил сформировать следующую обобщенную полумарковскую модель действий злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации (рис. 2).

Данная модель отражает все основные действия организованного злоумышленника. Несмотря на большое многообразие видов атак и инструментов по их реализации, обобщенная модель действий злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации обязательно включает в себя следующие состояния [7, 9–13]:

s_1 – злоумышленник определяет цель атаки по получению доступа к СУ сетью синхронизации;

s_2 – злоумышленник получает исходные данные о СУ сетью синхронизации с помощью методов социальной инженерии;

s_3 – злоумышленник получает исходные данные о СУ сетью синхронизации из открытых источников;

s_4 – злоумышленник осуществляет поиск активных узлов и АРМов СУ сетью синхронизации;

s_5 – злоумышленник определяет структуру СУ сетью синхронизации;

s_6 – злоумышленник определяет точки входа в СУ сетью синхронизации;

s_7 – злоумышленник проводит анализ уязвимостей точек входа в СУ сетью синхронизации и осуществляет поиск инструментария по их реализации;

s_8 – злоумышленник осуществляет обход системы обнаружения вторжений и систем обеспечения информационной безопасности (СОИБ);

s_9 – злоумышленник проводит основную фазу атаки в соответствии со своими замыслами, инструментарием и квалификацией.

Процесс действий злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации выглядит следующим образом. Исходным состоянием является состояние s_1, когда злоумышленник определяется целью по получению доступа к СУ сетью синхронизации.

На следующем этапе в состояниях s_2 и s_3 злоумышленник приложит все свои усилия, чтобы получить как можно больше информации и исходных данных об объекте атаки. Применяя методы социальной инженерии и построив доверительные отношения с обслуживающим персоналом, администраторами СУ сетью синхронизации и даже руководством обслуживающей организации, злоумышленник способен получить структурные схемы связи, пароли доступа, настройки аппаратуры и другую ценную информацию. У злоумышленника также существует возможность получения ценных исходных данных из открытых источников.

Рис. 1. Этапы реализации атаки

Следующим этапом в состоянии s_4 злоумышленник будет осуществлять поиск активных узлов и АРМов технологической сети передачи данных (СПД) СУ сетью синхронизации. Как правило, СУ сетью синхронизации имеет распределенную структуру с множеством серверов и АРМов, которые могут быть разнесены географически, иметь разное функциональное и логическое назначение, а также разный уровень привилегий по управлению сетью синхронизации. Так как СУ сетью синхронизации функционирует по технологической СПД, злоумышленник организует изучение топологии технологической СПД СУ сетью синхронизации с целью обнаружить уязвимые сервера, узлы и АРМы.

Если у злоумышленника не будет доступа ко внутренней части технологической СПД СУ сетью синхронизации, то он начнет сканировать межсетевые шлюзы и сторонние серверы, чтобы получить представление о пограничных элементах технологической СПД СУ сетью синхронизации, после чего попытается проникнуть во внутреннюю сеть. При получении доступа во внутреннюю сеть злоумышленник начнет сканировать и отображать её.

Как только злоумышленник выявит активные узлы, АРМы и сервера, следующим этапом в состоянии s_5 будет определение топологии технологической СПД СУ сетью синхронизации путем трассировки маршрутов передачи сообщений.

На следующем этапе s_6 злоумышленник будет выяснять функционирующее программное обеспечение на каждом узле, версию данного программного обеспечения, а также определять потенциальные точки входа в СУ сетью синхронизации.

На основе информации о типе установленного программного обеспечения на конкретном узле СУ сетью синхронизации злоумышленник может найти уязвимые места, проведя соответствующий анализ.

На следующем этапе в состоянии s_7 для определения и анализа уязвимостей точек входа в СУ сетью синхронизации злоумышленники обычно используют сканеры поиска уязвимых мест, которые позволяют автоматизировать процесс подключения к СУ сетью синхронизации и проверить СУ на наличие уязвимых мест.

В дальнейшем на этапе s_8 злоумышленник осуществляет обход систем обнаружения вторжений и систем СОИБ СУ сетью синхронизации.

Преодолев все рубежи обороны СУ сетью синхронизации в состоянии s_9, злоумышленник готов к основной фазе реализации атаки. Основная фаза реализации атаки может выражаться следующими угрозами информационной безопасности для сети синхронизации [1, 8–13]:

– манипуляция синхросигналами и пакетами, содержащими сигналы точного времени;

– спуфинг в сети синхронизации;

– атака повторного воспроизведения или добавления задержки. Добавленная задержка может быть постоянной, дрожащей или медленно блуждающей;

– атака подмены роли устройств в сети синхронизации;

– атака подмены маршрутов передачи сигналов синхронизации;

– перехват и удаление сообщений, содержащих информацию о качестве сигналов синхронизации;

– атака на использование уязвимостей в протоколах передачи сигналов точного времени, ошибок реализации или неправильных конфигураций устройств (например, атака NTPDDoS);

– сетевая разведка, при которой злоумышленник может использовать получаемые данные для сбора информации, такой как как адреса и местоположения узлов, принимающих синхросигналы и сигналы точного времени. Сетевая разведка может быть применена путем пассивного прослушивания или отправки вредоносных сообщений от отдельных узлов и сбор ответов. Прослушивая сообщения, злоумышленник может изучить сетевые задержки, которые могут дать

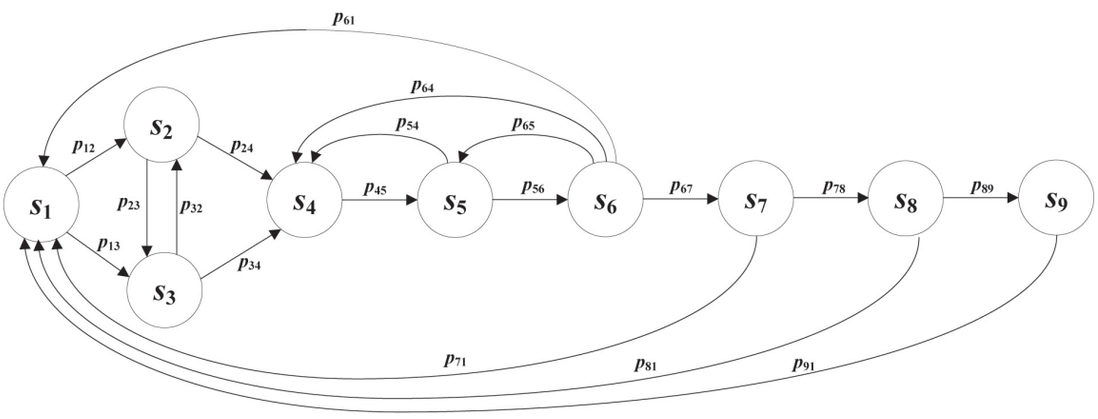

Рис. 2. Обобщенная модель действий злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации

информацию о топологии сети и узлах. Кроме того, такие свойства, как частота сигналов, сообщений и пакетов или время, в которое они отправлены, могут идентифицировать узлы, даже если сетевые адреса скрыты или зашифрованы.

Помимо данных угроз злоумышленник, завладев СУ сетью синхронизации, способен управлять параметрами электропитания, климатики, охранно-пожарного оборудования отдельных устройств.

Определение стационарных характеристик процесса, описывающего действия злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации

Основными стационарными характеристиками, определяющими защищенность СУ сетью синхронизации, будут являться [7–8, 14]:

– стационарные вероятности $(\pi_i), i = 1,...,9; i \in S$ пребывания в произвольный момент времени в каждом из состояний s_i, характеризуемых определенным набором действий злоумышленника;

– среднее время цикла начального этапа реализации атаки T_I.

Исходными данными для оценки стационарных характеристик процесса, описывающего действия злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации, являются [7–8, 14]:

1. Матрица переходных вероятностей из одного состояния в другое $\Pi = (p_{ij})$;

2. Матрица функций распределения условных случайных времен пребывания рассматриваемого процесса атаки в каждом из s_i состояний $F_{ij}(t)$;

Стационарную вероятность пребывания рассматриваемого процесса атаки в произвольный момент времени в каждом из состояний s_i можно вычислить по следующей формуле [7–8, 14]:

$$\pi_i = \frac{P_i T_i}{\sum\limits_{j \in S} P_j T_j} (i, j = 1,...,9; i, j \in S; \sum\limits_{i \in S} \pi_i = 1) \quad (1)$$

где P_i, P_j – стационарная вероятность пребывания вложенной однородной марковской цепи в состоянии s_i и s_j, T_i, T_j – математическое ожидание безусловного времени пребывания процесса атаки в каждом состоянии, S – общее число состояний.

Для оценки математического ожидания безусловного времени пребывания процесса реализации атаки в каждом состоянии воспользуемся следующими выражениями [7–8, 14] (2, 3):

$$T_i = \sum_{j \in S} p_{ij} T_{ij} \quad (2)$$

$$T_{ij}(t) = \int_0^\infty [1 - F_{ij}(t)] dt \quad (3)$$

где T_{ij} – математическое ожидание условного времени пребывания в каждом состоянии процесса реализации атаки.

Для оценки стационарной вероятности пребывания вложенной однородной марковской цепи в состоянии s_i используем следующее выражение [7–8, 14] (4, 5):

$$P_i = \frac{D_i}{\sum\limits_{j=1}^{n} D_j} \quad (4)$$

где $D_i(D_j)$ – минор, получаемый вычеркиванием $i(j)$ строки и $i(j)$ столбца матрицы D.

$$D = \begin{pmatrix} 1-p_{11} & -p_{12} & ... & -p_{1n} \\ -p_{21} & 1-p_{22} & ... & -p_{2n} \\ ... & ... & ... & ... \\ -p_{n1} & -p_{n2} & ... & 1-p_{nn} \end{pmatrix} \quad (5)$$

Для оценки среднего времени цикла начального этапа реализации атаки и общего времени второго и третьего этапов реализации атаки конечное множество состояний S процесса реализации атаки (рис. 2) разделим на два непересекающихся подмножества состояний: состояний, в которых злоумышленник проводит подготовительные действия к атаке $S_I \subset S$, и состояний, в которых проводится атака $\overline{S_I} \subset S$. Отметим, что $S_I \cup \overline{S_I} = 0$.

S_I будут являться состояния s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8. $\overline{S_I}$ будет являться состояние s_9.

При наличии указанных исходных данных среднее время цикла начального этапа и общее время второго и третьего этапов можно найти по следующим выражениям [7–8, 14]:

$$T_I = \frac{\sum\limits_{i \in S_I} P_i T_i}{\sum\limits_{i \in S_+} P_i \sum\limits_{j \in S_I} p_{ij}} \quad (6)$$

$$T_{II,III} = \frac{\sum\limits_{i \in S_I} P_i T_i}{\sum\limits_{i \in S_-} P_i \sum\limits_{j \in S_I} p_{ij}} \quad (7)$$

где S_+ и S_- – подмножество граничных состояний, обуславливающих переход из подмножества S_I в подмножество $\overline{S_I}$ и наоборот.

Подмножеством граничных состояний является состояние s_8. Подмножеством граничных состояний является состояния s_9.

Оценив стационарные вероятности π_i пребывания процесса реализации атаки в произвольный момент времени в каждом из состояний s_i (рис. 2) можно определить коэффициент исправного действия $К_и$ СУ сети синхронизации на начальном этапе реализации атаки.

Коэффициент исправного действия $К_и$ СУ сетью синхронизации является показателем, характери-

зующим устойчивость СУ сетью синхронизации в процессе её функционирования, в том числе в условиях воздействия атак организованных злоумышленников [15].

$$К_{и} = \sum_{i \in S_I} \pi_i \tag{8}$$

Расчет численных значений стационарных характеристик процесса, описывающего действия злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации

В качестве примера ниже приведена оценка стационарных характеристик процесса, описывающего действия злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации. В качестве исходных приняты следующие данные. Матрица переходных вероятностей имеет следующий вид (9):

$$П = \begin{pmatrix} 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.2 & 0 & 0.8 & 0 & 0 & 0 \\ 0.1 & 0 & 0 & 0.1 & 0.1 & 0 & 0.7 & 0 & 0 \\ 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0.8 & 0 \\ 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.8 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{9}$$

В качестве распределения условных случайных времен пребывания в каждом из s_i состояний $F_{ij}(t)$ принято экспоненциальное распределение со следующей матрицей интенсивностей переходов (10):

$$\Lambda = \begin{pmatrix} 0 & \frac{1}{720} & \frac{1}{360} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{180} & \frac{1}{24} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{180} & 0 & \frac{1}{24} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{24} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & \frac{1}{24} & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & \frac{1}{24} & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, ч^{-1} \tag{10}$$

Таким образом, после последующего расчёта на основе предложенного подхода и разработанной обобщенной модели действий злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации были получены следующие стационарные вероятности пребывания в произвольный момент времени в каждом из состояний s_i (11):

$$\pi_i = \begin{pmatrix} 0.648 & 0.122 & 0.122 & 0.041 & 0.036 & 0.026 \\ 1.891 \times 10^{-3} & 8.403 \times 10^{-4} & 6.723 \times 10^{-4} \end{pmatrix} \tag{11}$$

Среднее время цикла начального этапа и общего времени второго и третьего этапов реализации атаки будут иметь следующие значения (12, 13):

$$T_I = \frac{\sum_{i \in S_I} P_i T_i}{\sum_{i \in S_+} P_i \sum_{j \in S_I} p_{ij}} = \frac{P_1T_1 + P_2T_2 + P_3T_3 + P_4T_4 + P_5T_5 + P_6T_6 + P_7T_7 + P_8T_8}{P_8 p_{89}} = 1.487 \times 10^3 \text{ ч} \approx 62 \text{сут.} \tag{12}$$

$$T_{II,III} = \frac{\sum_{i \in S_I} P_i T_i}{\sum_{i \in S_-} P_i \sum_{j \in S_I} p_{ij}} = \frac{P_9 T_9}{P_9 p_{91}} = 1 \text{ ч} \tag{13}$$

Данные значения показывают, что злоумышленник получит доступ к СУ сетью синхронизации через 62 суток, а получив доступ, будет распоряжаться ею в течение 1 часа, в течение данного часа системы обеспечения информационной безопасности должны его обнаружить, локализовать его активность и восстановить процесс функционирования СУ сетью синхронизации.

Соответственно, коэффициент исправного действия $К_{и}$ СУ сетью синхронизации на начальном этапе реализации атаки примет следующее значение (14):

$$К_{и} = \sum_{i \in S_I} \pi_i = 0.999 \tag{14}$$

Коэффициент исправного действия $К_{и}$ СУ сетью синхронизации имеет достаточно высокое значение, что выглядит вполне логичным, так как в статье рассматривается начальный этап реализации атаки на СУ сетью синхронизации, когда по сути злоумышленник только начинает готовиться к атаке и проводит подготовительные действия.

Оценим также влияние интенсивностей действий злоумышленника и систем обеспечения информационной безопасности на коэффициент исправного действия $К_{и}$ СУ сетью синхронизации, среднее время цикла начального этапа и общее время второго и третьего этапов реализации атаки. В результате проведенного моделирования были получены следующие результаты (рис. 3–4).

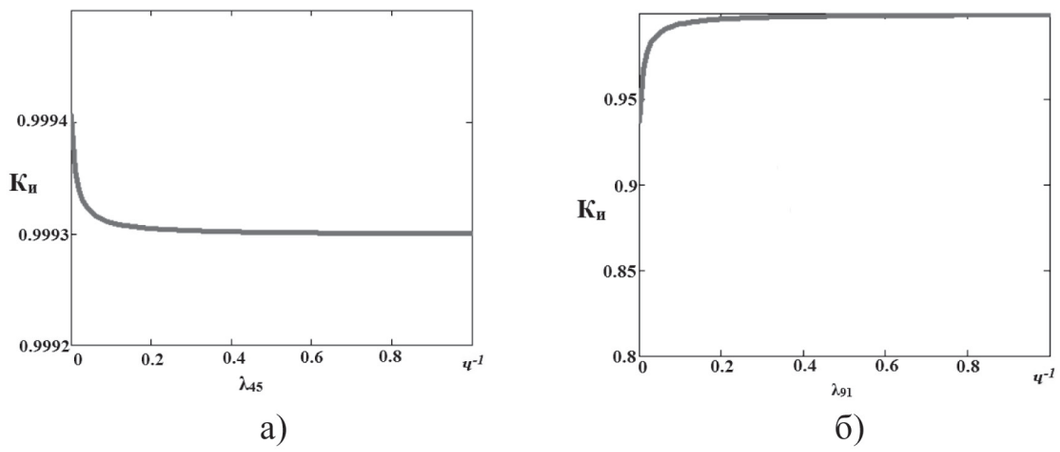

Рис. 3. Зависимость коэффициента исправного действия Ки СУ сетью синхронизации от интенсивности определения злоумышленником структуры технологической СПД СУ сетью синхронизации (а) и от интенсивности функционирования систем обеспечения информационной безопасности (б)

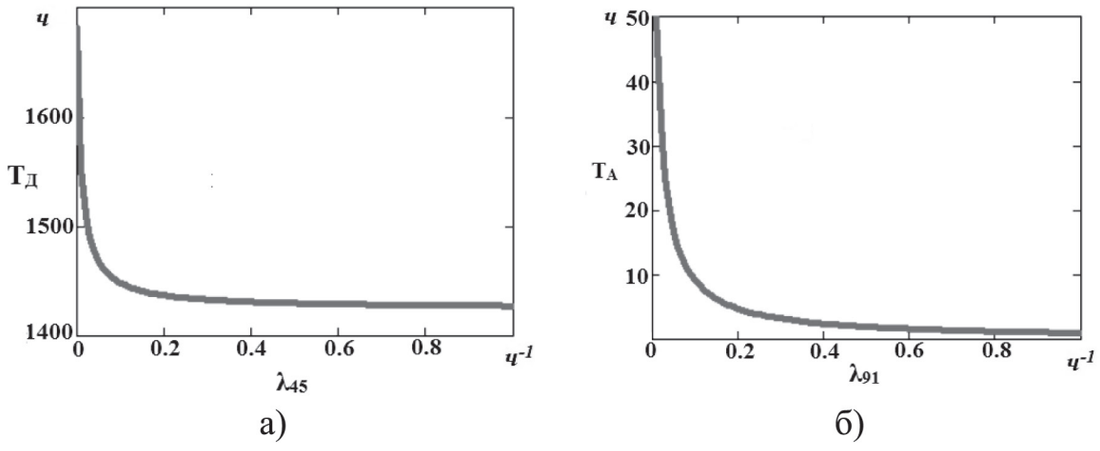

Рис. 4. Зависимость времени цикла начального этапа реализации атаки от интенсивности определения злоумышленником структуры технологической СПД СУ сетью синхронизации (а) и общего времени второго и третьего этапов реализации атаки от интенсивности функционирования систем обеспечения информационной безопасности (б)

По результатам моделирования можно сделать следующие выводы:

– увеличение интенсивности действий злоумышленника снижает коэффициент исправного действия Ки СУ сетью синхронизации, а действия систем СОИБ повышают его, однако коэффициент исправного действия Ки СУ сетью синхронизации на начальном этапе реализации атаки еще достаточно высок в следствие того, что злоумышленник только начинает свою атаку;

– интервал интенсивности попыток действий организованного злоумышленника и действий систем СОИБ можно разделить на 2 диапазона. В первом диапазоне незначительное изменение интенсивности действий злоумышленника или действий систем СОИБ приводит к значительному изменению коэффициента исправного действия Ки. Во втором диапазоне изменение интенсивности противоборствующих сторон не приводит к значительному изменению коэффициента исправного действия Ки. Оценив данные диапазоны, злоумышленник может оптимально управлять своими усилиями по организации атаки на СУ сетью синхронизации, а администраторы безопасности соответственно управлять средствами защиты;

– по результатам моделирования можно также оценить время доступа (ТД) организованным злоумышленником к СУ сетью синхронизации и время, в течение которого злоумышленник будет контролировать СУ сетью синхронизации (ТА) в зависимости от ресурсов самого злоумышленника и ресурсов систем СОИБ.

Заключение

Система синхронизации является важной подсистемой ТКС, непосредственно влияющей на качество предоставления услуг связи, и следовательно, потенциальным объектом атаки со стороны организованных злоумышленников.

В результате проделанной работы получена обобщенная модель действий злоумышленника на начальном этапе реализации атаки на СУ сетью синхронизации. Данная модель позволяет производить оценку стационарных характеристик защищенности и уязвимости СУ сетью синхронизации от действий организованного злоумышленника с использованием математического аппарата полумарковских процессов.

Полученные результаты позволят на основе анализа отдельных средств защиты СУ сетью синхронизации, статистики архива отраженных и завершенных атак, а также различных методов тестирования оценить показатели защищенности и уязвимости СУ сетью синхронизации, а следовательно, сделать вывод о целесообразности использования или внедрения отдельного вида средств защиты.

Предполагается, что функции распределения условных случайных времен пребывания в каждом из состояний будут определяться из практики и анализа результатов контрольных тестирований, что позволит получить модель действий злоумышленника с реальными свойствами. Данная модель универсальна, отличается полнотой учёта состояний и может быть применена к любой СУ сетью синхронизации, а также позволяет определять стационарные характеристики процесса действий злоумышленника для каждого состояния, что позволяет при наложении нормативных требований на стационарные характеристики формировать множество стратегий защиты от действий организованного злоумышленника.

Литература

1. Канаев, А. К. Основы построения и эксплуатации системы синхронизации в телекоммуникационной системе : учебное пособие / А.К. Канаев, Е.В. Опарин. – Санкт-Петербург : Информационный издательский учебно-научный центр "Стратегия будущего", 2016. – 172 с.

2. Ванчиков, А. С. Синхронизация в современных сетях операторского класса / А.С. Ванчиков // Автоматика, связь, информатика. – 2018. – № 8. – С. 19–20.

3. 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.

4. Горбачев, Н. С. Синхронизация цифровых сетей связи : методические указания / Н.С. Горбачев, С.А. Батраков, А.В. Ряполов. – Омск : Омский государственный университет путей сообщения, 2014. – 31 с.

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

6. Лукацкий, А. В. Обнаружение атак / А.В. Лукацкий. – Санкт-Петербург : БХВ-Петербург, 2003. – 596 с.

7. Скудис, Э. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите / Э. Скудис ; пер. с англ. – Москва : ДМК Пресс, 2003. – 512 с.

8. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. – Москва : ДМК Пресс, 2017. – 434 с.

9. 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.

10. Добрышин, М. М. Предложение по совершенствованию систем противодействия DDoS-атакам / М.М. Добрышин // Телекоммуникации. – 2018. – № 10. – С. 32–38.

11. Добрышин, М. М. Моделирование процессов деструктивных воздействий на компьютерную сеть связи с применением компьютерной атаки типа «Человек посередине» / М.М. Добрышин // Телекоммуникации. – 2019. – № 11. – С. 32–36.

12. Добрышин, М. М. Модель разнородных компьютерных атак, проводимых одновременно на узел компьютерной сети

связи / М.М. Добрышин // Телекоммуникации. – 2019. – № 12. – С. 31–35.

13. Mizrahi, T. RFC7384 Security Requirements of Time Protocols in Packet Switched Networks / T. Mizrahi. – 36 p.

14. Шубинский, И. Б. Структурная надёжность информационных систем. Методы анализа / И. Б. Шубинский. – Ульяновск : Печатный двор, 2012. – 216 с.

15. 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.