УДК 004.056.057 ISSN 1995-5499
DOI: https://doi.org/10.17308/sait/1995-5499/2022/2/58-71
Поступила в редакцию 19.03.2022
Подписана в печать 29.06.2022

ОЦЕНКА ЭФФЕКТИВНОСТИ КОМПЕНСИРУЮЩИХ МЕР ЗАЩИТЫ ОТ APT-АТАК, ЭКСПЛУАТИРУЮЩИХ УЯЗВИМОСТЬ ZEROLOGON

© 2022 С. А. Будников✉, М. А. Пеливан, А. И. Бочарова

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю ул. 9 Января, 280а, 394020 Воронеж, Российская Федерация

Аннотация. Необходимость оценки эффективности создаваемых систем безопасности значимых объектов критической информационной инфраструктуры, определяет потребность в разработке простых и адекватных математических моделей реализации компьютерных атак. Использование методов математического моделирования ходе проектирования системы безопасности значимого объекта позволяет без значительных затрат и без какого-либо влияния на технологический процесс обосновать требования к системе в целом или к отдельным ее частям. Целью работы является разработка модели процесса проведения многоэтапной компьютерной атаки, эксплуатирующей уязвимость Zerologon, основанной на представлении ее марковским случайным процессом с дискретными состояниями и непрерывным временем. Используемые методы: методы теории марковских процессов, теории вероятностей, вычислительной математики, а также теории графов. Новизна работы заключается в применение методов вычислительной математики для функционального анализа результатов решения системы уравнений Колмогорова, что позволяет известными методами анализа непрерывных функций решать задачу оптимизации компенсирующих мер защиты, входящих в систему безопасности. Разработана математическая модель, позволяющая определить требуемые вероятностно-временные характеристики средств защиты в проектируемых системах безопасности. При оценке эффективности мер защиты введен показатель эффективности системы безопасности значимого объекта критической информационной инфраструктуры как отношение вероятности срабатывания системы безопасности к вероятности успешного завершения атаки нарушителем. Оценена зависимость времени защиты относительно соотношений временных параметров применяемых компенсирующих мер защиты и действий нарушителя. Результаты исследования можно использовать при проектировании систем безопасности значимых объектов критической информационной инфраструктуры с учетом задаваемых параметров системы безопасности и нарушителя.

Ключевые слова: значимый объект, компьютерная атака, компенсирующие меры защиты, критическая информационная инфраструктура, марковский процесс, система безопасности.

ВВЕДЕНИЕ

В настоящее время вопросы обеспечения безопасности информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, эксплуатируемых субъектами критической информационной инфраструктуры (КИИ), приобретают важное значение. Форсирование работ по созданию систем безопасности значимых объектов (ЗО) КИИ определяется

✉ Будников Сергей Алексеевич
e-mail: ivan20petrov@yandex.ru

не только требованиями нормативно-правовых и руководящих документов в области информационной безопасности [1, 2], но и резким ростом количества сообщений о компьютерных инцидентах на объектах КИИ Российской Федерации [4, 5], а также на объектах информационной инфраструктуры зарубежных стран [6].

В этих условиях особенно важными являются вопросы оценки эффективности создаваемых систем безопасности ЗО КИИ. Поэтому в ходе проектирования системы безопасности ЗО в целях тестирования рекомендовано ее макетирование или создание тестовой среды с использованием средств и методов моделирования [3].

Необходимость обоснования требований к мерам защиты, в том числе и компенсирующим, и оценки эффективности создаваемых систем безопасности ЗО КИИ определяет потребность в разработке простых и адекватных математических моделей реализации компьютерных атак. Использование методов математического моделирования в ходе проектирования системы безопасности ЗО позволяет без значительных затрат и влияния на функционирование реального объекта обосновать требования к системе в целом или ее отдельным частям.

Проведенный анализ методического обеспечения [7–10], применяемого в исследованиях в области обеспечения компьютерной безопасности, показал, что в случае сложных систем, к которым относятся ЗО КИИ, наиболее подходящими методами и подходами к моделированию компьютерных атак являются использование теории сетей Петри — Маркова [11] и марковских случайных процессов [12].

Одним из наиболее опасных сценариев целенаправленных программных воздействий на объекты КИИ и сети электросвязи [1] в настоящее время считается так называемая компьютерная атака типа Advanced persistent threat (APT-атака), реализуемая путем эксплуатации уязвимости BDU:2020-04016 Zerologon (CVE-2020-1472) [13]. Эта уязвимость основана на дефекте в реализации процедур аутентификации на контроллере домена под управлением операционных систем MS Windows Server 2008-2019 и позволяет нарушителю удаленно с помощью специально созданного приложения получить привилегии администратора домена MS Active Directory. Использование обновления, требующего принудительного использования всеми сетевыми устройствами вновь разработанного механизма безопасного удаленного вызова процедур с защищенным каналом Netlogon, приводит к нарушению корректной работы устройств АСУ ТП на базе уже не поддерживаемого производителями оборудования. Обновления всего парка программно-аппаратных средств АСУ ТП требует значительных затрат. «Откат» параметров групповой политики, позволяющих использовать не безопасный Netlogon, не устраняет эту уязвимость. Поэтому многие субъекты КИИ предпочитают не проводить принудительное обновление операционных систем, а использовать, в дополнении к применяемым в системе безопасности ЗО КИИ, компенсирующие меры защиты, исключающие возможность эксплуатации нарушителем этой уязвимости.

ОСНОВНАЯ ЧАСТЬ

Целью статьи является разработка модели процесса проведения многоэтапной целенаправленной компьютерной атаки, эксплуатирующей уязвимость Zerologon, основанной на представлении ее случайным марковским процессом с дискретными состояниями и непрерывным временем, и обоснование на ее основе требований к компенсирующим мерам защиты.

Основываясь на известном подходе, представляющем совокупности процессов, протекающих в системе безопасности ЗО КИИ и, связанных с деятельностью нарушителя, как единой процесс конфликтного взаимодействия в рамках целостной системы, можно считать, что при моделировании хода этой атаки эта система конфликтного взаимодействия S может находиться в множестве дискретных состояний $S_0, S_1, \ldots, S_n$, при этом переход (перескок) системы из состояния в состояние происходит по схеме марковских случайных процессов в любой момент времени t [14].

В ходе реализации данной атаки нарушитель должен успешно пройти этапы, представляющие собой результаты отработки применяемых тактик и техник, приведенные в табл. 1. Название используемых злоумышленником тактик и техник взяты из базы данных атак и средств защиты — MITRE Att&ck (Adversarial Tactics, Techniques, and Common Knowledge — тактики, техники и общие знания) [15].

Тогда, с учетом сделанных заключений и ассоциативной формализации номера состояния (см. табл. 1), можно разметить граф состояний системы безопасности, вершины которого отражают состояния системы в ходе атаки в любой момент времени t, а дуги графа — направление протекания процесса. Анализ вершин и дуг данного графа показал, что, осуществляя свертку графа путем объединения последовательно соединенных вер-

Таблица 1. Этапы атаки, эксплуатирующей уязвимость Zerologon
[Table 1. Stages of an attack exploiting the Zerologon vulnerability]

№ п/п	**Состояния S**	**Содержание этапов атаки (вершины графа)**
1	*2*	*3*
1	S_0	Состояние системы до начала атаки
2	S_1	Проверка готовности и обновления инструментария нарушителя (Kali Linux)
3	S_2	Использование техники «System network configuration discovery» («Сбор информации о конфигурации и настройках сети»). Подключение к сети как DHCP-клиент и определение сетевых параметров
4	S_3	Использование программного средства Wireshark. Перехват пакетов и выявление IP-адресов основных узлов сети путем использования техники «Network Sniffing» («Получение аутентификационных данных путем перехвата и анализа сетевого трафика»)
5	S_4	Поиск контроллера домена путем сканирования SMB-устройств в сети путем использования техники «Network Service Scanning» («Получение информации о списке запущенных служб и о наличии в них уязвимостей путем сканирования портов»)
6	S_5	Эксплуатация уязвимости Zerologon (BDU:2020-04016) путем использования техники «Exploitation of Remote Services» («Эксплуатация уязвимостей программного обеспечения с целью получения доступа к удаленной системе с помощью сервисов удаленного доступа»)
7	S_6	Замена пароля контроллера домена путем использования техники «Credential Dumping» («Получение аутентификационных данных путем извлечения файлов операционной системы»)
8	S_7	Получение значений хэша от учетной записи «Администратор» с использованием модуля Secretsdump путем использования техники «Pass the Hash» («Получение доступа к информационной системе путем захвата хэша и его повторного использования с целью перехвата сеанса (без раскрытия пароля)»)
9	S_8	Повышение нарушителем привилегий и подключение к контроллеру домена от имени учетной записи «Администратор»
10	S_9	Получение доступа к интерактивной консоли на контроллере домена
11	S_{10}	Создание привилегированной учетной записи нарушителя

1	2	3
12	S_{11}	Добавление учетной записи нарушителя в группу администраторов домена путем использования техники «Account Manipulation» («Изменение учетных записей системы или домена»)
13	S_{12}	Поиск АРМ, представляющих интерес для нарушителя, путем использования техники «Account Discovery» («Получение списка учетных записей системы или домена»)
14	S_{13}	Удаленное подключение нарушителя к АРМ оператора технологической установки
15	S_{14}	Поиск файлов, содержащих специальное программное обеспечение контроля и управления технологическим процессом (проекты управления), на АРМ оператора технологической установки путем использования техники «Remote System Discovery» («Сбор информации о хостах в сети, доступных для реализации протокола удаленного доступа»)
16	S_{15}	Копирование на АРМ нарушителя файлов, содержащих проекты управления, с АРМ оператора технологической установки путем использования техники «Remote File Copy» («Удаленное копирование файлов»)
17	S_{16}	Блокирование доменной учетной записи оператора технологической установки
18	S_{17}	Несанкционированное принудительное отключение нарушителем от управления технологическим процессом АРМ оператора технологической установки путем удаленного выключения АРМ оператора с использованием техники «Endpoint Denial of Service» («DoS-атака в конечной точке»)
19	S_{18}	Срабатывание системы безопасности и блокирование действий нарушителя в ходе атаки
20	S_{19}	Успешное завершение атаки

шин, можно снизить его размерность и сократить анализируемое количество вершин с 20 до 14. При этом последовательно выполняемые этапы атаки заменены одним этапом. Свёрнутый граф атаки, эксплуатирующей уязвимость Zerologon, представлен на рис. 1.

Вершина S_0 представленного на рис. 1 графа определяет начальное состояние про-

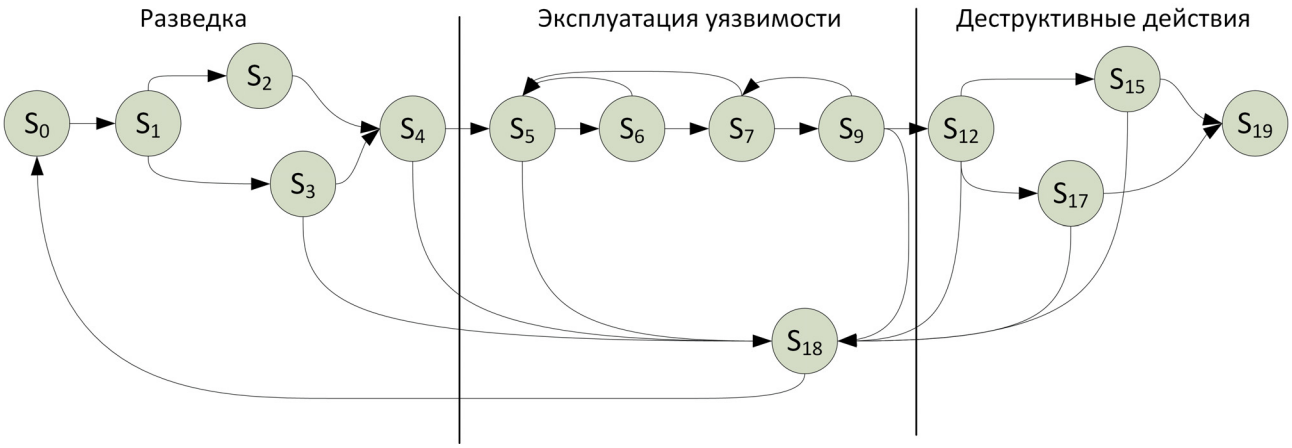

Рис. 1. Свернутый граф компьютерной атаки
[Fig. 1. Rolled up computer attack graph]

цесса проведения атаки. Переходные вероятности P_{ij} характеризуют переходы из i-го состояния к j-му состоянию со средним значением времени $\overline{t_{ij}}$.

При этом будем считать, этапы разведки и получения несанкционированного доступа нарушителем пройдены, за счет преодоления мер по обеспечению промышленной, функциональной и физической безопасности ЗО КИИТогда в соответствии с [12] процесс атаки будет описываться системой однородных дифференциальных уравнений Колмогорова, которую с учетом перехода от значений интенсивностей переходов λ_{ij} к средним значениям времени $\overline{t_{ij}}$ в общем виде для заданных начальных условий

$$P_{S0}(0)=1, P_{S1}(0)=0, P_{S2}(0)=0, P_{S3}(0)=0,$$
$$P_{S4}(0)=0, P_{S5}(0)=0, P_{S6}(0)=0, P_{S9}(0)=0,$$
$$P_{S12}(0)=0, P_{S15}(0)=0, P_{S17}(0)=0, P_{S18}(0)=0,$$
$$P_{S19}(0)=0.$$

можно записать как

$$\begin{cases}
\frac{d}{dt}P_{S0}(t)=\frac{P_{S18}(t)}{t_{18_0}}-\frac{P_{S0}(t)}{t_{0_1}};\\
\frac{d}{dt}P_{S1}(t)=\frac{P_{S0}(t)}{t_{0_1}}-\\
-\left(\frac{P_{S1}(t)}{t_{1_2}}+\frac{P_{S1}(t)}{t_{1_3}}\right);\\
\frac{d}{dt}P_{S2}(t)=\frac{P_{S1}(t)}{t_{1_2}}-\frac{P_{S2}(t)}{t_{2_4}};\\
\frac{d}{dt}P_{S3}(t)=\frac{P_{S1}(t)}{t_{1_3}}-\\
-\left(\frac{P_{S3}(t)}{t_{3_4}}+\frac{P_{S3}(t)}{t_{3_18}}\right);\\
\frac{d}{dt}P_{S4}(t)=\frac{P_{S2}(t)}{t_{2_4}}+\\
+\frac{P_{S3}(t)}{t_{3_4}}-\left(\frac{P_{S4}(t)}{t_{4_5}}+\frac{P_{S4}(t)}{t_{4_18}}\right);\\
\frac{d}{dt}P_{S5}(t)=\frac{P_{S4}(t)}{t_{4_5}}+\frac{P_{S6}(t)}{t_{6_5}}+\\
+\frac{P_{S7}(t)}{t_{7_5}}-\left(\frac{P_{S5}(t)}{t_{5_6}}+\frac{P_{S5}(t)}{t_{5_18}}\right);\\
\frac{d}{dt}P_{S6}(t)=\frac{P_{S5}(t)}{t_{5_6}}-\\
-\left(\frac{P_{S6}(t)}{t_{6_5}}+\frac{P_{S6}(t)}{t_{6_7}}\right);\\
\frac{d}{dt}P_{S7}(t)=\frac{P_{S6}(t)}{t_{6_7}}+\frac{P_{S9}(t)}{t_{9_7}}-\\
-\left(\frac{P_{S7}(t)}{t_{7_5}}+\frac{P_{S7}(t)}{t_{7_9}}\right);\\
\frac{d}{dt}P_{S9}(t)=\frac{P_{S7}(t)}{t_{7_9}}-\\
-\left(\frac{P_{S9}(t)}{t_{9_7}}+\frac{P_{S9}(t)}{t_{9_12}}+\frac{P_{S9}(t)}{t_{9_18}}\right);\\
\frac{d}{dt}P_{S12}(t)=\frac{P_{S9}(t)}{t_{9_12}}-\\
-\left(\frac{P_{S12}(t)}{t_{12_15}}+\frac{P_{S12}(t)}{t_{12_17}}+\frac{P_{S12}(t)}{t_{12_18}}\right);\\
\frac{d}{dt}P_{S15}(t)=\frac{P_{S12}(t)}{t_{12_15}}-\\
-\left(\frac{P_{S15}(t)}{t_{15_18}}+\frac{P_{S15}(t)}{t_{15_19}}\right);\\
\frac{d}{dt}P_{S17}(t)=\frac{P_{S12}(t)}{t_{12_17}}-\\
-\left(\frac{P_{S17}(t)}{t_{17_18}}+\frac{P_{S17}(t)}{t_{17_19}}\right);\\
\frac{d}{dt}P_{S18}(t)=\frac{P_{S3}(t)}{t_{3_18}}+\frac{P_{S4}(t)}{t_{4_18}}+\frac{P_{S5}(t)}{t_{5_18}}+\\
+\frac{P_{S9}(t)}{t_{9_18}}+\frac{P_{S12}(t)}{t_{12_18}}+\frac{P_{S15}(t)}{t_{15_18}}+\\
+\frac{P_{S17}(t)}{t_{17_18}}-\frac{P_{S18}(t)}{t_{18_0}};\\
\frac{d}{dt}P_{S19}(t)=\frac{P_{S15}(t)}{t_{15_19}}+\frac{P_{S17}(t)}{t_{17_19}};
\end{cases} \qquad (1)$$

Исследуемые переходы, физический смысл протекаемых при этом процессов, а также обозначения средних значений времени переходов и их типовые значения приведены в табл. 2.

Для простоты восприятия средних значений времени переходов, переводящих моделируемую систему из одного состояния в другое, связанных с деятельностью сторон, эти значения запишем в виде множества средних значений времен пребывания системы в различных состояниях **T**. Для графа, представленного на рис. 1, мощность данного множества равна 25, $|\mathbf{T}| = 25$, и содержание значений этого множества приведено в графе 5 в табл. 2.

Для решения составленной системы уравнений Колмогорова используем конечноразностный многошаговый метод численного интегрирования обыкновенных дифферен-

Таблица 2. Физический смысл формализуемых переходов
[Table 2. The physical meaning of formalized transitions]

№ п/п	Обозначения	Физический смысл переходов	Обозначение времени	Значение, мин
1	*2*	*3*	*4*	*5*
1	$S_0 \to S_1$	Проверка готовности и обновления инструментария Kali Linux	$\overline{t}_{0\_1}$	10
2	$S_1 \to S_2$	Выбор техники «System network configuration discovery». Подключение к сети как DHCP-клиент и определение сетевых параметров	$\overline{t}_{1\_2}$	5
3	$S_1 \to S_3$	Выбор техники «Network Sniffing». Перехват пакетов и выявление IP-адресов основных узлов сети	$\overline{t}_{2\_3}$	8
4	$S_2 \to S_4$	Поиск контроллера домена путем сканирования SMB-устройств в сети, используя технику «Network Service Scanning»	$\overline{t}_{2\_4}$	10
5	$S_3 \to S_4$	Поиск контроллера домена путем сканирования SMB-устройств в сети, используя технику «Network Service Scanning»	$\overline{t}_{3\_4}$	10
6	$S_3 \to S_{18}$	Обнаружение средствами защиты информации факта сканирования и его блокирование. Неудача в поиске контроллера домена	$\overline{t}_{3\_18}$	8
7	$S_4 \to S_5$	Эксплуатация уязвимости Zerologon (BDU:2020-04016). Техника «Exploitation of Remote Services»	$\overline{t}_{4\_5}$	12
8	$S_4 \to S_{18}$	Обнаружение средствами защиты информации факта эксплуатации уязвимости Zerologon и реализация защитных мер	$\overline{t}_{4\_18}$	20
9	$S_5 \to S_6$	Замена пароля контроллера домена с использованием техники «Credential Dumping»	$\overline{t}_{5\_6}$	13
10	$S_5 \to S_{18}$	Обнаружение средствами защиты информации факта замены пароля контроллера домена, блокирование	$\overline{t}_{5\_18}$	3
11	$S_6 \to S_5$	Обнаружение средствами защиты информации факта замены пароля контроллера домена, разрыв соединения	$\overline{t}_{6\_5}$	9

1	2	3	4	5
12	$S_6 \to S_7$	Получение значений HASH от учетной записи «Администратор» с использованием модуля Secretsdump путем применения техники «Pass the Hash»	$\overline{t}_{6\_7}$	4
13	$S_7 \to S_5$	Блокирование получения значений HASH	$\overline{t}_{7\_5}$	5
14	$S_7 \to S_9$	Подключение к контроллеру домена от имени учетной записи «Администратор». Получение доступа к интерактивной консоли на контроллере домена	$\overline{t}_{7\_9}$	5
15	$S_9 \to S_7$	Блокирование $S_{12} \to S_{15}$ на контроллере домена	$\overline{t}_{9\_7}$	10
16	$S_9 \to S_{12}$	Поиск АРМ, представляющих интерес для нарушителя	$\overline{t}_{9\_12}$	13
17	$S_9 \to S_{18}$	Блокирование созданной учетной записи нарушителя	$\overline{t}_{9\_18}$	20
18	$S_{12} \to S_{15}$	Поиск файлов, содержащих проекты управления, на АРМ оператора	$\overline{t}_{12\_15}$	18
19	$S_{12} \to S_{17}$	Удаленное выключение АРМ оператора путем использования техники «Endpoint Denial of Service»	$\overline{t}_{12\_17}$	5
20	$S_{12} \to S_{18}$	Блокирование поисковых процедур нарушителя	$\overline{t}_{12\_18}$	40
21	$S_{15} \to S_{19}$	Копирование файлов, содержащих проекты управления	$\overline{t}_{15\_19}$	10
22		Блокирование процессов несанкционированного копирования файлов, содержащих проекты управления	$\overline{t}_{15\_18}$	20
23	$S_{17} \to S_{18}$	Блокирование процессов удаленного выключения	$\overline{t}_{17\_18}$	30
24	$S_{17} \to S_{19}$	Завершение атаки после выключения АРМ оператора	$\overline{t}_{17\_19}$	5
25	$S_{18} \to S_0$	Блокирование действий нарушителя, попытка проведения новой атаки	$\overline{t}_{18\_0}$	100

циальных уравнений первого порядка — метод Адамса, реализованный в среде MathCad [16]. С применением численной реализации данного метода можно вычислить значения $S_{15} \to S_{18}$ вероятностей $P_{Si}(\mathbf{T}, t)$ во всех исследуемых состояниях S_i, где $i \in \{0, 1, 2, 3, 4, 5, 6, 7, 9, 12, 15, 17, 18, 19\}$ в зависимости от времени t.

При оценке эффективности системы безопасности объекта КИИ в качестве показателя эффективности мер защиты от реализации компьютерной атаки, эксплуатирующей уязвимость Zerologon, используем отношение вероятностей нахождения в состояниях S_{18} и S_{19}, имеющих трактовку (см. табл. 1): «Срабатывание системы безопасности и блокирование действий нарушителя в ходе атаки» и «Успешное завершение атаки»,

$$W(\mathbf{T}, t) = \frac{P_{S18}(\mathbf{T}, t)}{P_{S19}(\mathbf{T}, t)}, \qquad (2)$$

где $P_{S18}(\mathbf{T}, t)$ — вероятность срабатывания системы безопасности и блокирования действий нарушителя в ходе атаки;

$P_{S19}(\mathbf{T},t)$ — вероятность успешного завершения атаки ко времени t при заданных значениях множеств параметров $\mathbf{T}$, приведенных далее.

Превышение значений единицы показателя (2) говорит об эффективности функционирования системы безопасности в момент времени t.

Определимся, что множество временных параметров $\mathbf{T}$ включает в себя параметры компенсирующих мер защиты и параметры нарушителя, таких что $\mathbf{T} = \mathbf{T}^{ЗИ} \bigcup \mathbf{T}^{наруш}$, $\mathbf{T}^{ЗИ}$ — подмножество значений временных параметров, характеризующих систему безопасности (мер защиты), $\mathbf{T}^{наруш}$ — подмножество значений временных параметров, характеризующих нарушителя.

Для типовых заданных значений множества параметров компенсирующих мер защиты $\mathbf{T}^{ЗИ}$, приведенных в столбце 5 табл. 2 при численном решении системы (1) получены графические зависимости вероятностей нахождения в различных состояниях моделируемой системы $P_{Si}(\mathbf{T},t)$. Будем считать, что варьируемыми параметрами в модели являются временные параметры компенсирующих мер защиты информации $\mathbf{T}^{ЗИ}$, а временные параметры нарушителя, взятые из табл. 2, $\mathbf{T}^{наруш} = \{\overline{t}_{1\_2}, \overline{t}_{3\_4}, \overline{t}_{4\_5}, \overline{t}_{5\_6}, \overline{t}_{6\_7}, \overline{t}_{7\_9}, \overline{t}_{9\_12}, \overline{t}_{12\_15}, \overline{t}_{12\_17}, \overline{t}_{15\_19}, \overline{t}_{17\_19}, \overline{t}_{18\_0}\}$ определяются его квалификацией и задаются как исходные данные.

Проведем исследование трех вариантов построения систем безопасности объекта КИИ в условиях воздействия компьютерных атак, эксплуатирующих уязвимость Zerologon, характеризуемых наборами средств защиты с временными параметрами $\mathbf{T}1$, $\mathbf{T}2$, $\mathbf{T}3$. Набор временных значений параметров мер защиты от реализации компьютерной атаки $\mathbf{T}1$ представляет собой набор типовых значений временных характеристик мер защиты информации, приведенных в табл. 2. Во втором варианте построения системы безопасности, соответствующему набору значений $\mathbf{T}2$, используются средства защиты, в которых среднее время срабатывания меры защиты от сниффинга $t_{\text{WireShark}}$ увеличивается с 8 до 15 минут [17]. То есть средства обнаружения сниффинга путем вскрытия сетевых интерфейсов, работающих в promiscous-режиме, во втором варианте системы безопасности объекта КИИ работают медленнее. В наборе значений $\mathbf{T}3$ в отличие от $\mathbf{T}2$ дополнительно увеличено среднее время защиты от получения хэш-значений паролей из памяти t_{HASH} с 10 до 15 минут. Соответственно время контроля над процессами и приложениями, присутствующими на серверах или узлах с помощью системы обнаружения проникновений в третьем варианте построения системы безопасности больше чем во втором.

Это значит, что набор мер, характеризуемых временными параметрами $\mathbf{T}1$, лучше чем набор мер, характеризуемых временными параметрами $\mathbf{T}2$ и набор мер $\mathbf{T}2$, лучше чем набор мер $\mathbf{T}3$.

Результат решения уравнения (1) для различных наборов временных значений параметров мер защиты от реализации компьютерной атаки $\mathbf{T} = \{\mathbf{T}1, \mathbf{T}2, \mathbf{T}3\}$ в виде графиков приведен на рис. 2. Как видно из рисунка, последовательное ухудшение временных параметров мер защиты по двум показателям $\mathbf{T}2$ и $\mathbf{T}3$ приводит к снижению времени защиты $t^1_{защиты} > t^2_{защиты} > t^3_{защиты}$. Как отмечалось ранее, значение этого времени определяет длительность эффективного функционирования системы безопасности и как, следствие, время устойчивого функционирования КИИ в условиях целенаправленных компьютерных атак, эксплуатирующей уязвимость Zerologon, с 664 (для набора временных параметров $\mathbf{T}1$) до $t^2_{защиты} = 584$ (для набора временных параметров $\mathbf{T}2$) и $t^3_{защиты} = 548$ (для набора временных параметров $\mathbf{T}3$) минут.

Анализ смещения влево при ухудшении параметров защиты значений времени защиты $t_{защиты}$, показанного на рис. 2, позволяет сделать вывод, что многопараметрическая функция эффективности мер защиты от компьютерной атаки, эксплуатирующей уязвимость Zerologon, является монотонно убывающей во времени функцией.

Полученные результаты предполагают возможность обоснования временных требований по мерам защиты для заданного значения времени защиты $t_{защиты}$. Анализ этапов компьютерной атаки, представленных пере-

ходами графа на рисунке 1 позволяет выявить конфликтно обусловленные состояния, начиная с которых реализуются те или иные меры защиты. Например, успешность SMB-сканирования ресурсов сети и обнаружение контроллера домена в корпоративной сети характеризует переход $S_3 \to S_4$, а эффективное срабатывание меры защиты от SMB- сканирования ресурсов сети системы безопасности объектов КИИ — $S_3 \to S_{18}$. Поскольку параметры меры защиты и возможностей нарушителя задаются значениями средних времен $\overline{t}_{3\_4}$ и $\overline{t}_{3\_18}$ соответственно, то рассмотрим процедуру обоснования требований к временных характеристикам мер защиты от сканирования SMB-устройств в сети относительно возможностей нарушителя, т. е.

$$K_{SMB} = \overline{t}_{3\_18} \Big/ \overline{t}_{3\_4} \qquad (3),$$

где K_{SMB} — коэффициент превосходства возможностей системы безопасности;

$\overline{t}_{3\_18}$ — среднее время срабатывания меры защиты от сканирования SMB-устройств в сети;

$\overline{t}_{3\_4}$ — среднее время, необходимое нарушителю для проведения SMB-сканирования ресурсов сети и обнаружения контроллера домена.

Тогда значения времени срабатывания компенсирующей меры защиты от сканирования SMB-устройств в сети можно записать как $\overline{t}_{3\_18} = K_{SMB}\,\overline{t}_{3\_4}$. С использованием описанного выше подхода к описанию времени срабатывания меры защиты проведем анализ времени эффективного функционирования системы безопасности в зависимости от значений вводимых коэффициентов превосходства возможностей системы безопасности на различных этапах компьютерной атаки, связанных с эксплуатацией уязвимости Zerologon: K_{SMB}, $K_{Zerologon}$, K_{HASH}, $K_{AccountPolice}$, K_{CMD}. Время эффективного функционирования системы безопасности t определяется в результате решения неравенства вида

$$\arg\limits_{t}\,(W(\mathbf{T},t) > 1), \qquad (4)$$

где $\mathbf{T}^{ЗИ} = \mathbf{K} \times \mathbf{T}^{наруш}$ — временные параметры компенсирующих мер защиты информации,

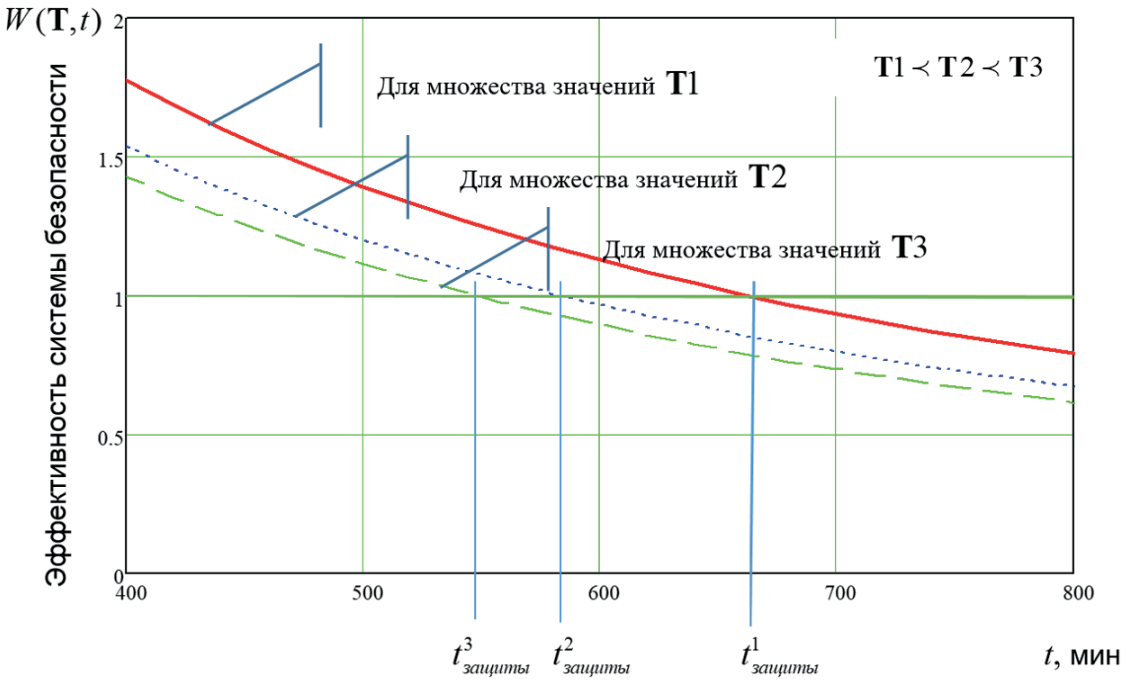

Рис. 2. Функция эффективности системы безопасности для различных наборов значений временных параметров средств защиты информации $\mathbf{T}$

[Fig. 2. The function of the effectiveness of the security system for different sets of values of time parameters of information $\mathbf{T}$ *security tools]*

характеризующие эффективность системы безопасности относительно возможностей нарушителя.

Результаты расчетов представлены на рис. 3, на котором показаны зависимости времени защиты t (результаты решения уравнения (4)) от соотношения K временных параметров действий нарушителя и реагирования системы безопасности на атаки, связанные с эксплуатацией сканирования SMB-устройств в сети (SMB), уязвимости Zerologon (Zerologon), получения значений HASH от учетной записи «Администратор» (HASH), повышения полномочий и замены пароля контроллера домена (AccountPolice), получения доступа к интерактивной консоли на контроллере домена (CMD).

Анализ полученных значений показывает наличие следующих закономерностей. При создании системы безопасности объекта КИИ, ориентированной на защиту от компьютерных атак, эксплуатирующих уязвимость Zerologon, наибольший вклад в увеличение времени защиты вносят специализированные меры защиты, направленные на обнаружение средствами защиты информации факта замены пароля контроллера домена и последующий разрыв соединения (AccountPolice и Zerologon). Применение универсальных меры защиты от сканирования SMB-устройств в сети, получения удаленного доступа к командной консоли вносит меньший вклад в увеличение времени защиты.

В тоже время превосходство системы безопасности в оперативности реагирования на атаки, направленные на замену пароля контроллера домена, при $K_{AccountPolice} \le 1$ обеспечивает время защиты не менее 1600 минут. Превосходство в оперативности противодействия реализации использования техники «Pass the Hash» $K_{HASH} \le 1$ позволяет гарантировать время защиты около 700 минут. Значения превосходства в оперативности доступа к интерактивной консоли $K_{CMD} \le 1$ обеспечивает время защиты не менее 558 минут. Подобные выводы можно сделать и в отношении остальных временных характеристик системы безопасности объекта КИИ.

Основываясь на минимаксном критерии принятия решений [18] можно считать, что

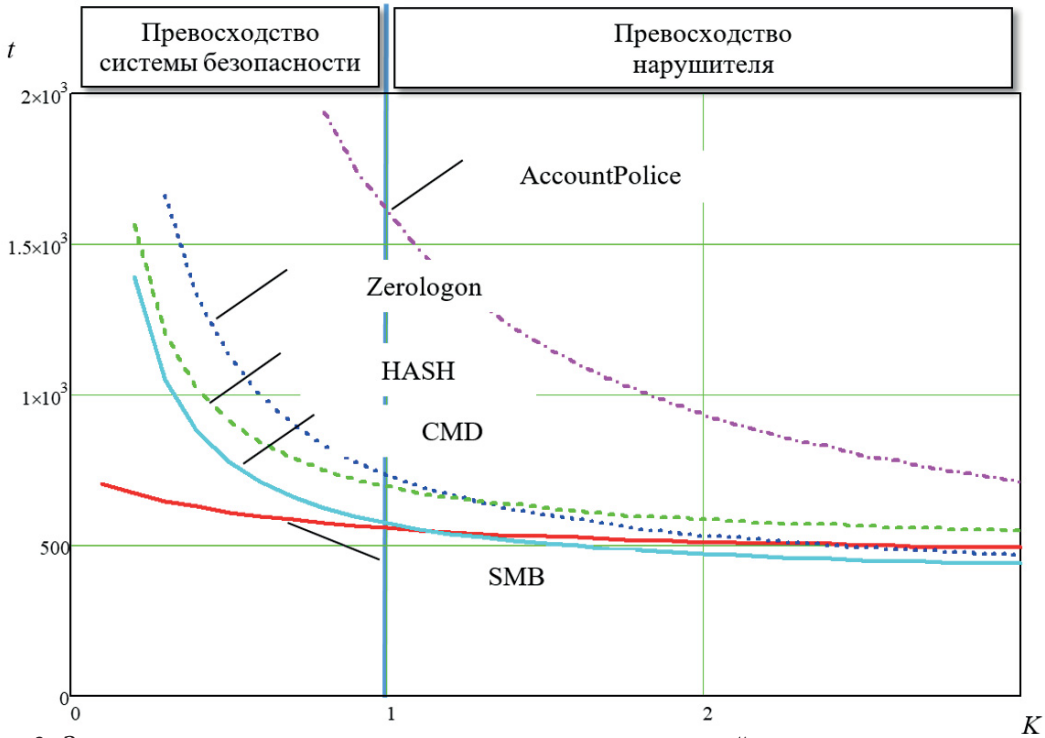

Рис. 3. Зависимости времени защиты t от соотношений временных параметров нарушителя и мер защиты

[Fig. 3. The dependences of the protection time t on the ratios of the time parameters of the violator and the protection measures]

равенство возможностей системы безопасности и нарушителя приведет к наихудшему значению времени защиты равному 558 минут. Это говорит о том, что комплекс мер защиты, реализуемый в системе безопасности объекта КИИ должен обеспечивать обновление параметров безопасности не реже чем один раз в рабочую смену (540 минут = 9 часов).

Используя полученные значения можно определять технические требования по оперативности реагирования на инциденты компьютерной безопасности на различных этапах компьютерной атаки с учетом временных возможностей нарушителя.

ЗАКЛЮЧЕНИЕ

Таким образом, в условиях возрастания угроз реализации компьютерных атак против ЗО КИИ актуальной задачей является разработка простых и адекватных математических моделей, позволяющих протестировать и оценить эффективность системы безопасности в ходе ее проектирования. Применение теории марковских процессов с дискретными состояниями и непрерывным временем позволяет достаточно точно формализовать процесс компьютерной атаки. Применение численных методов решения систем однородных дифференциальных уравнений, реализованных в среде проведения вычислительных расчетов Mathcad позволило не только получить графические зависимости вероятностей нахождения в том или ином состоянии моделируемой системы, но и ввести новый функциональный показатель эффективности средств защиты от реализации компьютерной атаки $W(\mathbf{T},t)$. Введенный количественный показатель эффективности позволяет наглядно продемонстрировать эффективность обоснованных временных параметров компенсирующих мер защиты, входящих в систему безопасности, и обосновать необходимость обновления параметров защиты не реже чем один раз в 9 часов.

КОНФЛИКТ ИНТЕРЕСОВ

Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон РФ от 26.07.2017 № 187-ФЗ // Собрание законодательства Российской Федерации от 31 июля 2017 г. № 31 ст. 4736.

2. Об утверждении Требований к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 // Электронный фонд правовых и нормативно-технических документов [Электронный ресурс]. 2021. – URL: https://docs.cntd.ru/document/542615513 (дата обращения: 15.09.2021).

3. Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 // Электронный фонд правовых и нормативно-технических документов [Электронный ресурс]. 2021. – URL: https://docs.cntd.ru/document/542616931 (дата обращения: 15.09.2021).

4. APT-атаки на промышленные компании в России. Обзор тактик и техник, Positive Technologies, 2019. // Positive Technologies [Электронный ресурс]. 2019. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-industry-2019/ (дата обращения: 15.09.2021).

5. Ландшафт угроз для систем промышленной автоматизации Второе полугодие 2019 // [Электронный ресурс]. 2019. – URL: https://ics-cert.kaspersky.ru/media/KASPERSKY_H22019_ICS_REPORT_FINAL_RU.pdf (дата обращения: 19.07.2021).

6. 2020 Cybersecurity threat trends outlook // [Электронный ресурс]. 2020. – URL: https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/ (дата обращения: 01.07.2021).

7. *Котенко Д. И., Котенко И. В., Саенко И. Б.* Методы и средства моделирования атак в больших компьютерных сетях: состояние // Труды СПИИРАН. – 2012. – № 3(22). – С. 5–30.

8. *Андреещев И. А., Будников С. А., Гладков А. В.* Полумарковская модель оценки конфликтной устойчивости информационной инфраструктуры // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2017. – № 1. – С. 10–17.

9. *Язов Ю. К., Соловьев С. В.* Защита информации в информационных системах от несанкционированного доступа. – Воронеж : Кварта, 2015. – 440 с.

10. *Добрышин М. М., Закалкин П. В.* Модель компьютерной атаки типа «Phishing» на локальную компьютерную сеть // Вопросы кибербезопасности. – 2021. – № 2(42). – С. 17–25. doi 10.21681/2311-3456-2021-2-17-25.

11. *Язов Ю. К., Анищенко А. В.* Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах. Монография. – Воронеж : Кварта, 2020. – 173 с.

12. *Вентцель Е. С., Овчаров Л. А.* Теория случайных процессов и ее инженерные приложения. – М. : Высшая школа, 2000. – 383 с.

13. Zerologon: уязвимость в протоколе Netlogon позволяет захватить контроллер домена // 2020. [Электронный ресурс]. – URL: https://www.kaspersky.ru/blog/cve-2020-1472-domain-controller-vulnerability/29085 / (дата обращения: 21.11.2020 г.).

14. *Вентцель Е. С.* Исследование операций. – М. : Советское радио, 1972. – 552 с.

15. Официальный сайт MITRE Att&ck // 2021. [Электронный ресурс]. – URL: https://attack.mitre.org/ (дата обращения 25.04.2021 г.).

16. *Охорзин В. А.* Оптимизация экономических систем. Примеры и алгоритмы в среде Mathcad. – М. : Финансы и статистика, 2005. – 144 с.

17. Обзор рынка средств защиты от целенаправленных атак. [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-protection-platform / (дата обращения 25.11.2021 г.).

18. *Таха, Хемди А.* Введение в исследование операций, 7-е издание: Пер. с англ. – М. : Издательский дом «Вильяме», 2005. – 912 с.

Будников Сергей Алексеевич — д-р. техн. наук, доцент, главный научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России» SPIN-код: 3768-5223.
E-mail: ivan20petrov@yandex.ru
ORCID iD: https://orcid.org/0000-0003-2285-494X

Пеливан Михаил Анатольевич — младший научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России».
E-mail: witcher89158779996@yandex.ru
ORCID iD: https://orcid.org/0000-0001-8529-9627

Бочарова Анастасия Ивановна — ведущий инженер ФАУ «ГНИИИ ПТЗИ ФСТЭК России».
E-mail: ai.bocharova@yandex.ru
ORCID iD: https://orcid.org/0000-0002-4811-4088

DOI: https://doi.org/10.17308/sait/1995-5499/2022/2/58-71 ISSN 1995-5499
Received 19.03.2022
Accepted 29.06.2022

EVALUATION OF THE EFFECTIVENESS OF COMPENSATING PROTECTION MEASURES AGAINST APT ATTACKS EXPLOITING ZEROLOGON VULNERABILITIES

© 2022 S. A. Budnikov✉, M. A. Pelivan, A. I. Bocharova

State scientific research testing institute of problems of technical protection of information FSTEC
280a, 9 Yanvarya Street, 394020 Voronezh, Russian Federation

Annotation. The need to assess the effectiveness of the security systems being created for significant objects of critical information infrastructure determines the need for the development of simple and adequate mathematical models for the implementation of computer attacks. The use of mathematical modeling methods during the design of a security system of a significant object allows, without significant costs and without any influence on the technological process, to justify the requirements for the system as a whole or for its individual parts. The aim of the work is to develop a model of the process of conducting a multi-stage computer attack that exploits the Zerologon vulnerability, based on its representation by a Markov random process with discrete states and continuous time. Used methods: methods of the theory of Markov processes, probability theory, computational mathematics, as well as graph theory. The novelty of the work lies in the application of computational mathematics methods for the functional analysis of the results of solving the Kolmogorov system of equations, which allows using the known methods of analyzing continuous functions to solve the problem of optimizing the compensating protection measures included in the security system. A mathematical model has been developed that makes it possible to determine the required probabilistic-temporal characteristics of protective equipment in the designed security systems. When evaluating the effectiveness of protection measures, an indicator of the effectiveness of the security system of a significant object of critical information infrastructure was introduced as the ratio of the probability of the security system being triggered to the probability of successfully completing the attack by the intruder. The dependence of the protection time on the ratio of the time parameters of the applied compensatory protection measures and the actions of the intruder is estimated. The results of the study can be used in the design of security systems for significant objects of critical information infrastructure, taking into account the specified parameters of the security system and the intruder.
Keywords: significant object, computer attack, compensating protection measures, critical information infrastructure, Markov process, security system.

CONFLICT OF INTEREST

The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.

REFERENCES

1. On the security of the critical information infrastructure of the Russian Federation. Federal Law of the Russian Federation of July 26, 2017 No. 187-FZ. Collection of Legislation of the Russian Federation of July 31, 2017 No. 31 Art. 4736.

2. On approval of the Requirements for the creation of security systems for significant facilities of the CII of the Russian Federation and ensuring their functioning. Order of the FSTEC of Russia dated December 21, 2017 No. 235. Electronic fund of legal and regulatory documents [Electronic resource]. 2021. URL: https://docs.cntd.ru/document/542615513 (accessed: 15.09.2021).

3. On approval of the Requirements for ensuring the safety of significant objects of the KII of the Russian Federation. Order of the FSTEC

✉ Budnikov Sergey A.
e-mail: ivan20petrov@yandex.ru

of Russia dated December 25, 2017 No. 239. Electronic fund of legal and regulatory documents [Electronic resource]. 2021. URL: https://docs.cntd.ru/document/542616931 (accessed: 15.09.2021).

4. ART attacks on industrial companies in Russia. Overview of tactics and techniques, Positive Technologies, 2019. Positive Technologies [Electronic resource]. 2019. - URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-industry-2019/ (accessed: 15.09.2021).

5. Threat landscape for industrial automation systems Second half of 2019. [Electronic resource]. 2019. URL: https://ics-cert.kaspersky.ru/media/KASPERSKY_H22019_ICS_REPORT_FINAL_RU.pdf (accessed: 19.07.2021).

6. 2020 Cybersecurity threat trends outlook. [Electronic resource]. 2020. URL: https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/ (accessed 01.07.2021).

7. *Kotenko D. I., Kotenko I. V. and Saenko I. B.* (2012) Methods and tools for modeling attacks in large computer networks: state of the art. *Proceedings of SPIIRAS*. No 3(22). P. 5–30.

8. *Andreeshchev I. A., Budnikov S. A. and Gladkov A. V.* (2017) Semi-Markov model for assessing the conflict stability of information infrastructure. *Bulletin of the Voronezh State University. Series: System Analysis and Information Technologies*. No 1. P. 10–17.

9. *Yazov Yu. K. and Solovyov S. V.* (2015) Protection of information in information systems from unauthorized access. *Voronezh : Quarta*. 440 p.

10. *Dobryshin M. M. ND Zakalkin P. V.* (2021) A model of a Phishing-type computer attack on a local computer network. *Cybersecurity Issues*. No 2(42). P. 17–25. doi 10.21681/2311-3456-2021-2-17-25.

11. *Yazov Yu. K. and Anishchenko A. V.* (2020) Petri-Markov nets and their application for modeling the processes of implementation of information security threats in information systems. Monograph. *Voronezh : Quarta*. 173 p.

12. *Venttsel E. S. and Ovcharov L. A.* (2000) Theory of random processes and its engineering applications. *Moscow : Higher School*. 383 p.

13. Zerologon: a vulnerability in the Netlogon protocol allows you to capture a domain controller. 2020. [Electronic resource]. URL: https://www.kaspersky.ru/blog/cve-2020-1472-domain-controller-vulnerability/29085/ (accessed: 21.11.2020).

14. *Wentzel E. S.* (1972) Research operations. *Moscow : Soviet radio*. 552 p.

15. Official website of MITER Att&ck. 2021. [Electronic resource]. URL: https://attack.mitre.org/ (accessed: 25.04.2021).

16. *Okhorzin V. A.* (2005) Optimization of economic systems. Examples and algorithms in the Mathcad environment. *Moscow : Finance and statistics*. 144 p.

17. Overview of the market for protection against targeted attacks. [Electronic resource]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-protection-platform/ (Accessed 11/25/2021).

18. *Taha and Hemdi A.* (2005) Introduction to operations research, 7th edition: Per. from English. *Moscow : Publishing house "William"*. 912 p.

Budnikov Sergey A. — DSc in Technical sciences, docent, Chief Researcher FAI «State scientific research testing institute of problems of technical protection of information FSTEC of Russia».
E-mail: ivan20petrov@yandex.ru
ORCID iD: https://orcid.org/0000-0003-2285-494X

Pelivan Mikhail A. — junior researcher FAI «State scientific research testing institute of problems of technical protection of information FSTEC of Russia».
E-mail: witcher89158779996@yandex.ru
ORCID iD: https://orcid.org/0000-0001-8529-9627

Bocharova Anastasia I. — Lead Engineer FAI «State scientific research testing institute of problems of technical protection of information FSTEC of Russia». E-mail: ai.bocharova@yandex.ru
ORCID iD: https://orcid.org/0000-0002-4811-4088