ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 3(45) / 2022

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИУ)»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА

ЧУВАРДИН О. П.,
руководитель Управления Федеральной службы по техническому и экспортному контролю России по Уральскому федеральному округу

ГЛАВНЫЙ РЕДАКТОР

СОКОЛОВ А. Н.,
к. т. н., доцент, зав. кафедрой «Защита информации», Южно-Уральский государственный университет (национальный исследовательский университет) (г. Челябинск)

ВЫПУСКАЮЩИЙ РЕДАКТОР

СОГРИН Е. К.

ВЁРСТКА

ШРАЙБЕР А. Е.

КОРРЕКТОР

ФЁДОРОВ В. С.

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76. ЮУрГУ, Издательский центр **Тел./факс (351) 267-97-01.**

Электронная версия журнала в Интернете: **www.info-secur.ru, e-mail: urvest@mail.ru**

16+

Journal of the Ural Federal District Information security

ISSN 2225-5435

№ 3(45) / 2022

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76 SUSU, Publishing Center
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

УДК 004.056

Вестник УрФО № 3(45) / 2022, с. 5–16

Хорев А.А.

DOI: 10.14529/secur220301

НЕКОТОРЫЕ ПОДХОДЫ К ОЦЕНКЕ ВОЗМОЖНОСТЕЙ ПЕРЕХВАТА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, ИСПОЛЬЗУЮЩИХ ЦИФРОВЫЕ ИНТЕРФЕЙСЫ

В статье в качестве показателей защищенности текстовой информации, выводимой на экран монитора СВТ, от перехвата средствами разведки побочные электромагнитных излучений (ПЭМИ), предложено использовать количество правильно распознанных ключевых слов и фраз в перехваченном тексте. Предложен методический подход к определению пороговых значений правильно распознанных ключевых слов и фраз в перехваченном тексте, которые зависят как от словесной и фразовой разборчивости текста, так и от его объема и характера. Получены аналитические соотношения для расчета словесной и фразовая разборчивости текста в зависимости от отношения информативный сигнал/шум на входе разведывательного приемника. Обоснованы пороговые значения отношений информативный сигнал/шум на входе разведывательного приемника для решения задач защиты текстовой информации, выводимой на экран монитора СВТ, от перехвата средствами разведки ПЭМИ.

Ключевые слова: *технический канал утечки информации, средство вычислительной техники, цифровой интерфейс, побочные электромагнитные излучения (ПЭМИ), перехват ПЭМИ, текстовая информация, разборчивость речи.*

SOME APPROACHES TO ASSESSING THE POSSIBILITIES OF INTERCEPTING SIDE ELECTROMAGNETIC RADIATION OF COMPUTER EQUIPMENT USING DIGITAL INTERFACES

In the article, it is proposed to use the number of correctly recognized keywords and phrases in the intercepted text as indicators of the security of textual information displayed on the screen of the SVT monitor from interception Transient ElectroMagnetic Pulse Emanation (TEMPE). A methodological approach is proposed to determine the threshold values of correctly recognized keywords and phrases in the intercepted text, which depend both on the verbal and phrasal intelligibility of the text, and on its volume and nature. Analytical relations are obtained for calculating the verbal and phrasal intelligibility of the text, depending on the ratio of the informative signal/noise at the input of the intelligence receiver. The threshold values of the informative signal/noise ratio at the input of the intelligence receiver are justified to solve the problems of protecting text information displayed on the screen of the SVT monitor from interception by means of the intelligence of the TEMPE.

Keywords: *technical channel of information leakage, computer equipment, digital interface, Transient ElectroMagnetic Pulse Emanation (TEMPE), interception of TEMPE, text information, speech intelligibility.*

Одним из наиболее опасных технических каналов утечки информации, обрабатываемой средствами вычислительной техники (СВТ), является канал утечки информации, возникающий вследствие побочных электромагнитных излучений (ПЭМИ) видеосистемы монитора [1].

В СВТ для передачи видеоданных широко используются цифровые интерфейсы DVI (Digital Visual Interface) и HDMI (High Definition Multimedia Interface), которые выполнены по стандарту последовательной передачи данных PanelLink с использованием технологии высокоскоростной передачи цифровых потоков TMDS [2].

При прохождении импульсных сигналов по видеокабелю вокруг последнего возникает побочное электромагнитное излучение (ПЭМИ).

Учитывая, что данные по интерфейсу TMDS передаются в последовательном виде, существует реальная возможность перехвата ПЭМИ и восстановления выводимого на экран монитора изображения.

Проведенные исследования показали, что если цвет пикселей изображения отличается, то и отличаются амплитуды «пиксельных» импульсов (группы импульсов, передающих цветовой код пикселя).

На рис. 1 и 2 приведены спектры ПЭМИ видеосистемы с интерфейсом DVI при выводе на экран монитора тестовых изображений: белый экран и черный экран, а на рис. 3 – осциллограмма видеосигнала ПЭМИ на выходе анализатора спектра в режиме нулевой полосы при выводе экран монитора тестового изображения в виде чередующиеся групп черных и белых полос.

Возможная упрощенная структурная схема средства перехвата ПЭМИ СВТ представлена на рис. 4.

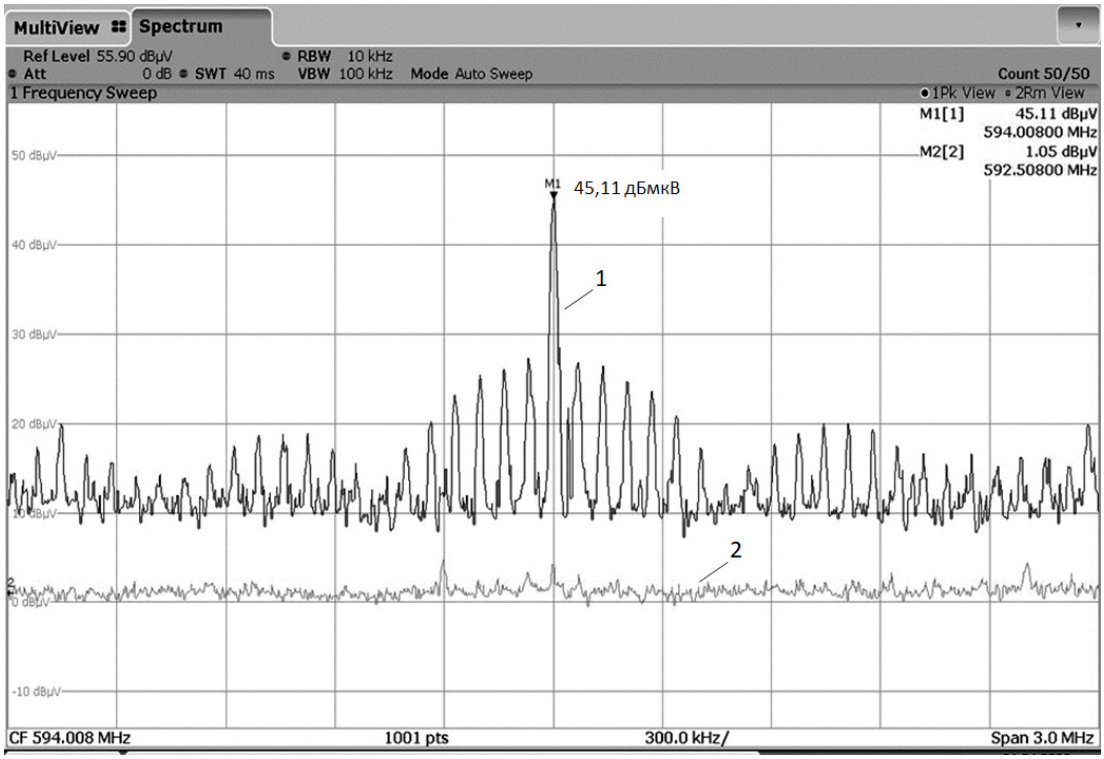

Рис. 1. Спектр ПЭМИ видеосистемы с интерфейсом DVI при выводе на экран монитора тестового изображения «белый» экран (1) и отключенной видеосистеме (2)

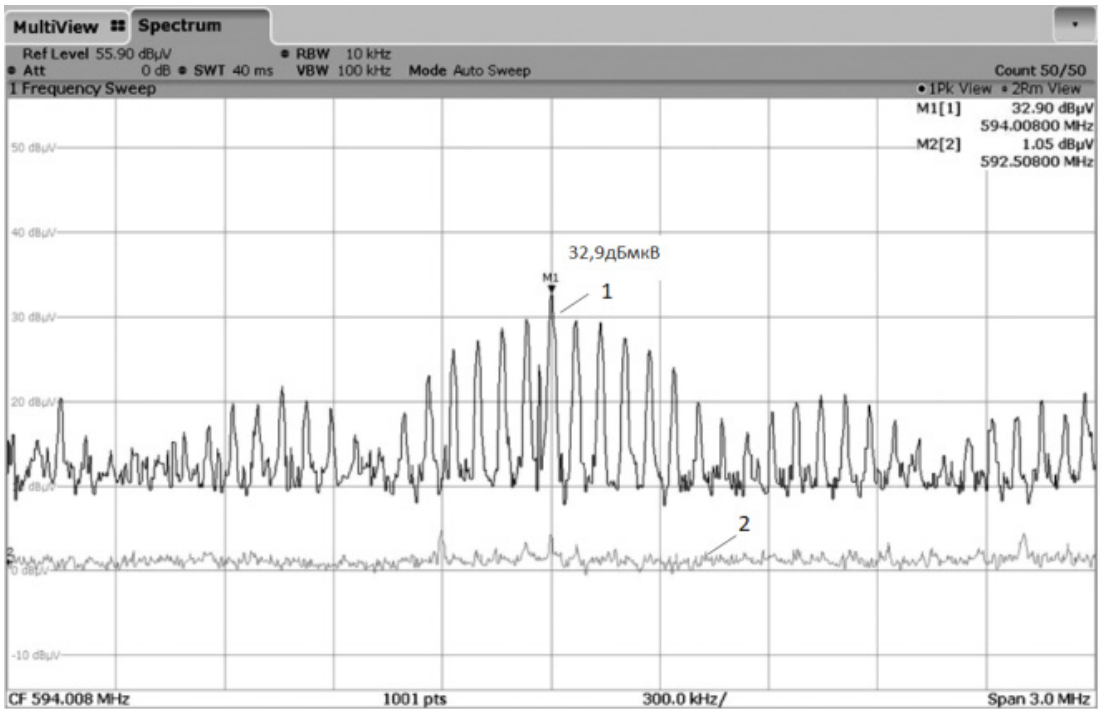

Рис. 2. Спектр ПЭМИ видеосистемы с интерфейсом DVI при выводе на экран монитора тестового изображения «черный» экран (1) и отключенной видеосистеме (2)

В качестве радиоприемного устройства средства перехвата ПЭМИ может использоваться, например, цифровой анализатор спектра R&S® FSW с широкополосной антенной R&S®HE600, а в качестве блока обработки – система обработки сигналов «NIGTHWATCH» [3].

СВТ часто используются для обработки

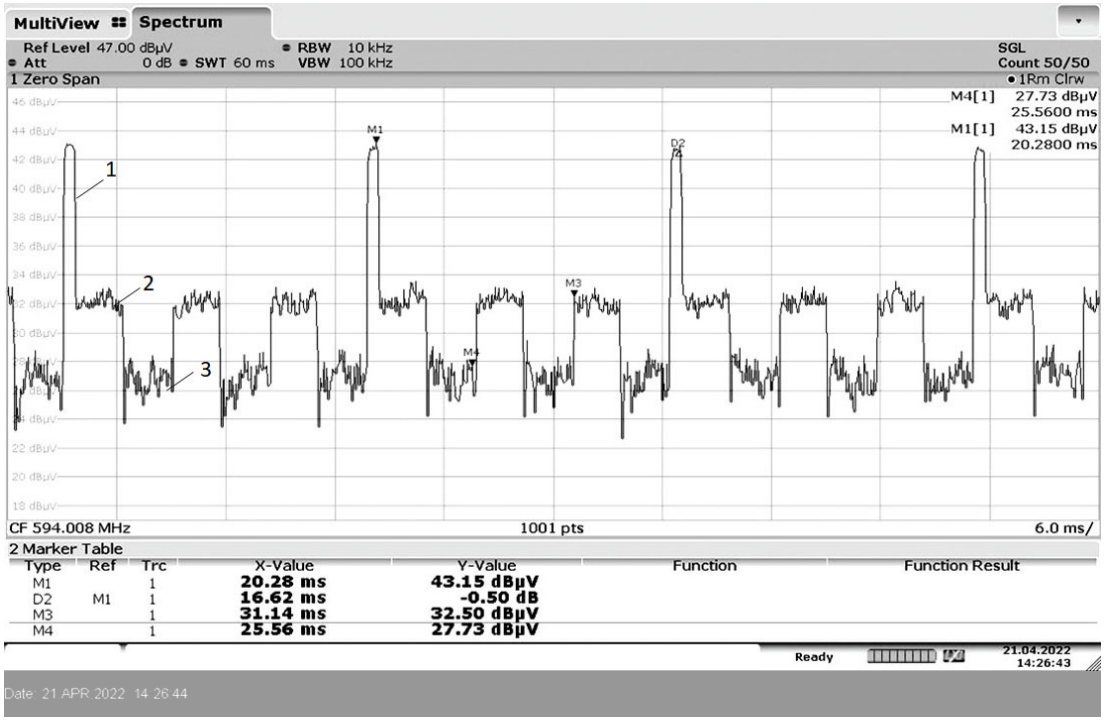

Рис. 3. Осциллограмма видеосигнала ПЭМИ видеосистемы с интерфейсом DVI на выходе анализатора спектра в режиме нулевой полосы (тест – чередующиеся группы черных и белых полос): 1 – синхроимпульс кадра, 2 – строки белого цвета, 3 – строки черного цвета

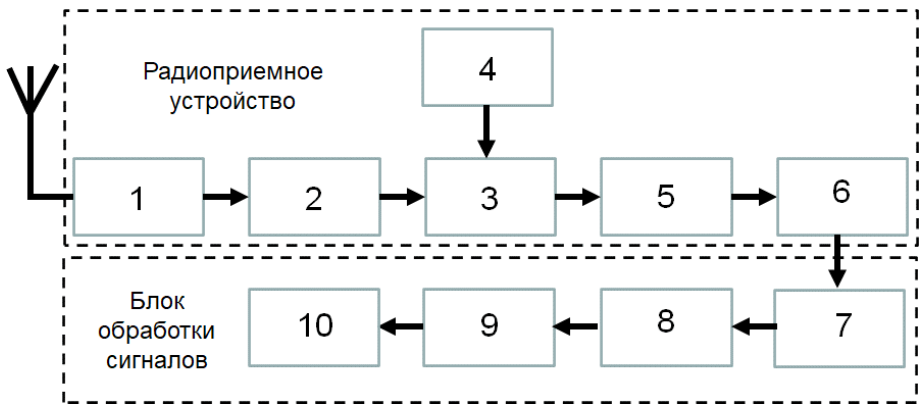

Рис. 4. Упрощенная структурная схема средства перехвата ПЭМИ СВТ:
1 – перестраиваемый полосовой фильтр высокой частоты; 2 – усилитель высокой частоты; 3 – смеситель; 4 – управляемый генератор (гетеродин); 5 – перестраиваемый полосовой фильтр промежуточной частоты; 6 – усилитель промежуточной частоты; 7 – видеодетектор; 8 – аналого-цифровой преобразователь; 9 – блок цифровой обработки сигналов; 10 – ЖК-монитор

текстовых документов, содержащих сведения ограниченного доступа.

Возможность перехвата ПЭМИ видеосистемы с интерфейсом DVI и восстановления текстового изображения, выводимого на экран монитора, подтверждена экспериментально (см. рис. 5) [4]. При этом для перехвата ПЭМИ использовался лабораторный комплекс, моделирующий работу комплекса перехвата ПЭМИ, схема которого приведена на рис. 3, в состав которого вошли:

– антенна измерительная дипольная АИ-5.0 (диапазон частот от 9 кГц до 2 ГГц);

– анализатор спектра R&S®FSW (диапазон частот от 1 Гц до 8 ГГц, полоса пропускания сигнала от 1 Гц до 80 МГц);

– цифровой запоминающий осциллограф R&S RTO 1022 (полоса частот до 2 ГГц, максимальная частота дискретизации сигналов 10 ГГц);

– система обработки сигналов на базе ноутбука.

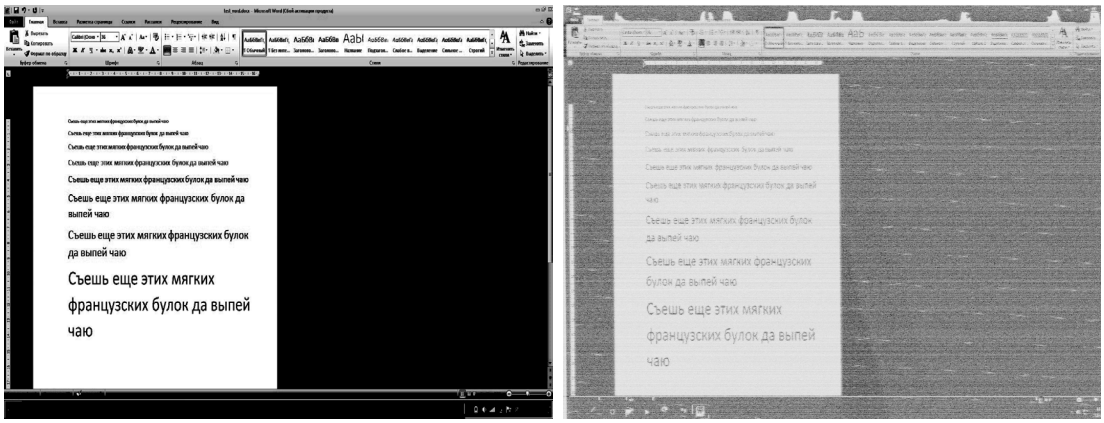

Рис. 5. Исходное текстовое изображение, выведенное на экран монитора (а), и восстановленное текстовое изображение (б)

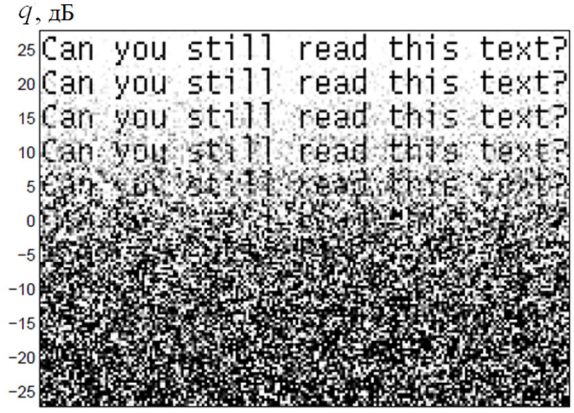

Рис. 6. Текстовое изображение, полученное при различных отношениях сигнал/шум q, дБ

Экспериментально установлено, что разборчивость текста на зашумленном изображении зависит от отношения сигнал/шум изображения (рис. 6) [5].

Под отношением сигнал/шум текстового изображения обычно понимается разность средних яркостей белого и черного пикселей, а под шумом – среднеквадратическое отклонение яркости пикселей изображения, вызванное шумами приемника средства разведки:

$$q_c = 20\lg\left[\frac{(L_б - L_ч)}{\sigma_Ш}\right] = 20\lg(L_б - L_ч) - 20\lg(\sigma_ш), \quad (1)$$

где q_c – отношение сигнал/шум изображения, дБ;

$L_б$ – средняя яркость белых пикселей, гр. ярк.;

$L_ч$ – средняя яркость черных пикселей, гр. ярк.;

$\sigma_ш$ – среднеквадратическое отклонение яркости пикселей изображения, вызванное шумами приемника средства разведки, гр. ярк.

При перехвате изображения, выводимого на экран монитора, необходимо учитывать, что оно стабильно в течение некоторого времени ($T_а$), которое зависит от характера действий оператора ПЭВМ и может варьировать от нескольких секунд (при наборе текста) до нескольких минут (при чтении текста). Данный факт позволяет использовать методы накопления (усреднения) кадров, что существенно повышает отношение сигнал/шум (см. рис. 7) [5], [6]. Например, система обработки сигналов «NIGTHWATCH» способна усреднять до 65536 кадров [3].

Проведенные исследования показали, что накопление (усреднение) N изображений увеличивает отношение сигнал/ шум в раз (рис. 8) [6].

С учетом накопления (усреднения) кадров отношение сигнал/шум изображения ($q_{c.N}$) будет равно:

$$q_{c.N} = qc + 10\lg(N) = 20\lg(L_б - L_ч) - 20\lg(\sigma_ш) + 10\lg(N), \quad (2)$$

где q_c – отношение сигнал/шум изображения для одного кадра (N =1), дБ;

$N = T_а \cdot F_к$ – количество кадров, перехваченных за время $T_а$;

а) б) в)

Рис. 7. Результаты усреднения битовых изображений при исходном отношении сигнал/шум q_c = 2,56 дБ: а) – исходное изображение ($N_к$ = 1); б) – изображение, полученное усреднением пятидесяти кадров ($N_к$ = 50); в) – изображение, полученное усреднением ста кадров ($N_к$ = 100)

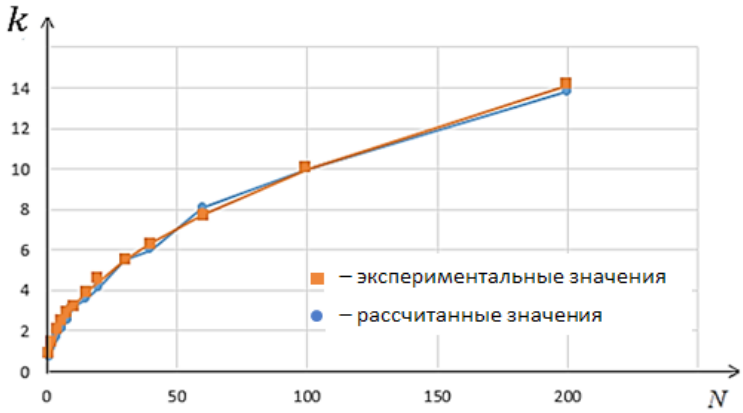

Рис. 8. Графики зависимости коэффициента улучшения отношения сигнал/шум (k) от количества усредняемых кадров (N)

$T_а$ – время, в течении которого изображение на экране монитора не меняется, с;

$F_к$ – частота обновления экрана монитора, Гц.

Полагая, что яркость каждого пикселя перехваченного изображения прямо пропорциональна соответствующему напряжению на входе разведывательного приемника, и учитывая только шумы на входе приемного устройства средства разведки, отношение сигнал/шум можно рассчитать по формуле:

$$q_{c.N} = q_c + 10\lg(N) = 20\lg(U_б - U_ч) - 20\lg(\sigma_U) + 10\lg(N), \quad (3)$$

где $U_б$ – напряжение на входе приемного устройства средства разведки, соответствующие напряженности электрической (магнитной) составляющей побочного электромагнитного излучения (ПЭМИ), возникающего при передаче по интерфейсу импульсов белого цвета, мкВ;

$U_ч$ – напряжение на входе приемного устройства средства разведки, соответствующие напряженности электрической (магнитной) составляющей ПЭМИ, возникающего при передаче по интерфейсу импульсов черного цвета, мкВ;

σ_U – среднеквадратическое отклонение напряжения шумов на входе приемного устройства средства разведки, мкВ.

Значения напряжений $U_б$ и $U_ч$ определяются инструментально-расчетным методом, предполагающим для каждого частотного интервала измерение уровней напряженностей электрической (магнитной) составляющей электромагнитного излучения информативных составляющих ПЭМИ (E), расчета затухания ПЭМИ на трассе СВТ – средство разведки (V_r) и расчета $U_б$ и $U_ч$ на входе приемного устройства с учетом значений калибровочных коэффициентов антенны средства разведки (k_a). Подробно данный метод описан в работах [1], [7], [8].

Учитывая, что спектр ПЭМИ дискретный, для каждого частотного интервала значения напряжений $U_{б.j}$ и $U_{ч.j}$ могут быть рассчитаны по формулам:

$$U_{б.j} \approx \sqrt{\sum_{i=1}^{N_j}\left(U_{б.j.i}\right)^2} \approx \sqrt{\frac{1}{V_{r.j}} \cdot \sum_{i=1}^{N_j}\left(\frac{E_{б.j.i}}{k_{a.j.i}}\right)^2} \approx \sqrt{\frac{1}{\frac{\sum_{i=1}^{M_j} V_{r.j.i}^{\,2}}{M_j}} \cdot \sum_{i=1}^{N_j}\left(\frac{E_{б.j.i}}{k_{a.j.i}}\right)^2}; \quad (4)$$

$$U_{ч.j} \approx \sqrt{\sum_{i=1}^{N_j}\left(U_{ч.j.i}\right)^2} \approx \sqrt{\frac{1}{V_{r.j}} \cdot \sum_{i=1}^{N_j}\left(\frac{E_{ч.j.i}}{k_{a.j.i}}\right)^2} \approx$$

$$\approx \sqrt{\frac{1}{\frac{\sum_{i=1}^{M_j} V_{r.j.i}{}^2}{M_j}} \cdot \sum_{i=1}^{N_j}\left(\frac{E_{ч.j.i}}{k_{a.j.i}}\right)^2}, \qquad (5)$$

где $U_{б.j.i}$ – напряжение информативного сигнала на входе приемного устройства на i-й частоте, входящей в состав j-го частотного интервала (тест – «белый экран»), мкВ;

$U_{ч.j.i}$ – напряжение информативного сигнала на входе приемного устройства на i-й частоте, входящей в состав j-го частотного интервала (тест – «черный экран»), мкВ;

N_j – количество частотных составляющих в j-м частотном интервале;

$E_{б.j.i}$ – напряженность поля информативной составляющей ПЭМИ на i-й частоте, входящей в состав j-го частотного интервала (тест – «белый экран»), измеренная на расстоянии 1 м от СВТ, мкВ/м;

$E_{ч.j.i}$ – напряженность поля информативной составляющей ПЭМИ на i-й частоте, входящей в состав j-го частотного интервала (тест – «черный экран»), измеренная на расстоянии 1 м от СВТ, мкВ/м;

$k_{a.j.i}$ – калибровочный коэффициент антенны средства разведки на i-й частоте, входящей в состав j-го частотного интервала, 1/м;

$V_{r.j}$ – среднее затухание ПЭМИ в j-м частотном интервале в точке размещения средства разведки на расстоянии r;

$V_{r.j.i}$ – затухание ПЭМИ на i-й частоте, входящей в состав j-го частотного интервала, в точке размещения средства разведки на расстоянии r;

M_j – количество частот, на которых проводился расчет затухания ПЭМИ в j-м частотном интервале.

Учитывая, что роль случайных антенн при излучении ПЭМИ СВТ выполняют проводники, соединяющие выход цифроаналогового преобразователя видеоадаптера с разъемом DVI, и кабель, соединяющий системный блок с монитором, будем полагать, что в излучении ПЭМИ доминирует электрическая составляющая электромагнитного поля Ес, которая в ближней зоне убывает обратно пропорционально кубу расстояния (~$1/r^3$), а дальней – обратно пропорционально расстоянию (~1/r). Предположим, что в средней зоне электрическая составляющая электромагнитного поля E_c убывает обратно пропорционально квадрату расстояния (~ $1/r^2$). Границей начала дальней зоны будем полагать расстояние r = 6λ. Тогда затухание $V_{r.j.i}$ можно рассчитать по формулам []:

1) Для частоты сигнала ПЭМИ ниже $f_i \leq$ ≤ 47,75МГц

$$V_{r.j.i} \approx \begin{cases} r^3 если r \leq \frac{47,75}{f_i}; \\ \frac{47,75 \cdot r^2}{f_i} если \frac{47,75}{f_i} < r \leq \frac{1800}{f_i}; \\ \frac{8,59 \cdot 10^4 \cdot r}{{f_i}^2} если r > \frac{1800}{f_i}; \end{cases} \qquad (6)$$

2) Для частоты сигнала ПЭМИ 47,75МГц < $< f_i \leq$ 1800МГц

$$V_{r.j.i} \approx \begin{cases} r^2 если r \leq \frac{1800}{f_i}; \\ \frac{1800 \cdot r}{f_i} если r > \frac{1800}{f_i}; \end{cases} \qquad (7)$$

3) Для частоты сигнала ПЭМИ f_i > 1800МГц

$$V_{r.j.i} \approx r, \qquad (8)$$

где f_i – i-я частота сигнала, МГц;

r – расстояние от СВТ до средства разведки, м.

Среднеквадратическое отклонение напряжения шумов на входе приемного устройства средства разведки в j-м частотном интервале зависит от уровня собственных шумов приемника и шумов антенны:

$$\sigma_U = \sqrt{\sigma_{ш.п.j}^2 + \sigma_{ш.а.j}^2}, \qquad (9)$$

где $\sigma_{ш.п.j}$ – среднеквадратическое отклонение напряжения собственных шумов приемного устройства средства разведки в j-м частотном интервале, мкВ;

$\sigma_{ш.п.j}$ – среднеквадратическое отклонение напряжения шумов антенны, приведенных ко входу приемного устройства средства разведки в j-м частотном интервале, мкВ.

Среднеквадратическое отклонение напряжения собственных шумов приемного устройства средства разведки в j-м частотном интервале рассчитаем по формуле:

$$\sigma_{ш.п.j} \approx \sqrt{\frac{\Delta F_j \cdot Z \cdot \sum_{i=1}^{M_j} N_{ш.j.i}}{M_j}}, \qquad (10)$$

где $N_{ш.j.i}$ – спектральная плотность мощности собственных шумов приемника средства разведки, измеренная на i-й частоте при полосе пропускания ΔF = 1Гц и отношении сигнал/шум q = 1 в j-м частотном интервале, Вт/Гц;

ΔF_j – ширина j-го частотного интервала, Гц;

M_j – количество частот, на которых проводилось измерение спектральной плотности мощности собственных шумов приемника средства разведки в j-м частотном интервале;

Z – входное сопротивление приемника средства разведки, Ом.

Среднеквадратическое отклонение напряжения шумов антенны, приведенных ко входу приемного устройства средства разведки в j-м частотном интервале, может быть рассчитано через спектральную чувствительность антенны $E_{ша}(f)$ и ее калибровочный коэффициент $k_a(f)$:

$$\sigma_{\text{ш.a.}j} \approx \sqrt{\frac{\Delta F_j \cdot \sum_{i=1}^{M_j} (E_{\text{ш.a.}j.i}/k_{a.j.i})^2}{M_j}}, \qquad (11)$$

где $E_{ш.a.j.i}$ – спектральная чувствительность антенны, измеренная при полосе пропускания ΔF = 1Гц и отношении сигнал/шум q = 1 на i-й частоте в j-м частотном интервале, мкВ/м·Гц;

$k_{a.j.i}$ – спектральный калибровочный коэффициента антенны средства разведки, измеренный при полосе пропускания на i-й частоте в j-м частотном интервале, 1/м;

ΔF_j – ширина j-го частотного интервала, Гц;

M_j – количество частот, на которых проводилось измерение спектральной чувствительности антенны в j-м частотном интервале.

Подставляя (5), (6), (10), (11) в (3) получим

$$q_{c.N.j} = 20\lg\left(\sqrt{\sum_{i=1}^{N_j}(E_{б.j.i}/k_{a.j.i})^2} - \sqrt{\sum_{i=1}^{N_j}(E_{ч.j.i}/k_{a.j.i})^2}\right) - 10\lg\left(\frac{\sum_{i=1}^{M_j} {V_{r.j.i}}^2}{M_j}\right) - 10\lg\left(\frac{\Delta F_j \cdot Z \cdot \sum_{i=1}^{M_j} N_{ш.j.i}}{M_j} + \frac{\Delta F_j \cdot \sum_{i=1}^{M_j}(E_{ш.a.j.i}/k_{a.j.i})^2}{M_j}\right) + 10\lg(N). \qquad (12)$$

На практике, как правило, уровень шумов антенны, приведенных ко входу приемника средства разведки, много больше уровня собственных шумов приемника. С учетом этого допущения формулу (12) можно записать в виде:

$$q_{c.N.j} \approx 20\lg\left(\sqrt{\sum_{i=1}^{N_j}(E_{б.j.i}/k_{a.j.i})^2} - \sqrt{\sum_{i=1}^{N_j}(E_{ч.j.i}/k_{a.j.i})^2}\right) - 10\lg\left(\frac{\sum_{i=1}^{M_j} {V_{r.j.i}}^2}{M_j}\right) - 10\lg\left(\frac{\Delta F_j \cdot \sum_{i=1}^{M_j}(E_{ш.a.j.i}/k_{a.j.i})^2}{M_j}\right) + 10\lg(N). \qquad (13)$$

На практике напряженность поля, калибровочные коэффициенты антенн и чувствительность антенны измеряются в дБ. С учетом этого формулу (13) запишем в виде

$$q_{c.N.j} \approx \sqrt{\sum_{i=1}^{N_j} 10^{0,1(E_{ч.j.i} - k_{a.j.i})}} - 20\lg\left(\sqrt{\sum_{i=1}^{N_j} 10^{0,1(E_{б.j.i} - k_{a.j.i})}} - \sqrt{\sum_{i=1}^{N_j} 10^{0,1(E_{ч.j.i} - k_{a.j.i})}}\right) - 10\lg\left(\frac{\sum_{i=1}^{M_j} {V_{r.j.i}}^2}{M_j}\right) - 10\lg\left(\frac{\Delta F_j \cdot \sum_{i=1}^{M_j} 10^{0,1(E_{ш.a.j.i} - k_{a.j.i})}}{M_j}\right) + 10\lg(N), \qquad (14)$$

где $E_{б.j.i}$ – напряженность поля информативной составляющей ПЭМИ на i-й частоте, входящей в состав j-го частотного интервала (тест – «белый экран»), измеренная на расстоянии 1 м от СВТ, дб(мкВ/м);

$E_{ч.j.i}$ – напряженность поля информативной составляющей ПЭМИ на i-й частоте, входящей в состав j-го частотного интервала (тест – «черный экран»), измеренная на расстоянии 1 м от СВТ, дБ(мкВ/м);

$k_{a.j.i}$ – калибровочный коэффициент антенны средства разведки на i-й частоте, входящей в состав j-го частотного интервала, дБ(1/м);

$E_{ш.a.j.i}$ – спектральная чувствительность антенны, измеренная при полосе пропускания ΔF = 1Гц и отношении сигнал/шум q = 1 на i-й частоте в j-м частотном интервале, дБ(мкВ/м·Гц);

Целью перехвата текстового изображения, выводимого на экран монитора, является получение смыслового содержания этого текста, поэтому в качестве показателя оценки возможности перехвата ПЭМИ СВТ техническим средством разведки (ТСР) используем словесную и фразовую разборчивость перехваченного текста.

Под словесной разборчивостью текста понимается отношение количества правильно распознанных слов к общему количеству слов в перехваченном тексте, а под фразовой разборчивостью – соответственно отношение количества правильно распознанных фраз к общему количеству фраз в перехваченном тексте.

Разборчивость текста отображает качественную область понятности, которая выражается в категориях подробности составляемой справки о перехваченном тексте.

Исходя из оценок качества перехваченного текста можно сформулировать цели защиты текстовой информации, выводимой на экран монитор, и критерии их достижения (табл. 1).

Проведенные исследования показали, что разборчивость текста (W), выводимого на экран монитора, можно рассчитать по формуле [6], [9]:

$$W \approx \Phi(Q_1 \cdot q_c - Q_2), \qquad (15)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} exp\left(-\frac{t^2}{2}\right) dt$ – интеграл вероятности;

q_c – отношение сигнал/шум изображения, дБ;

Таблица 1

Цели защиты текстовой информации, при ее обработке СВТ, и критерии их достижения

Цели защиты текстовых документов при их обработке СВТ	Критерии эффективности защиты текстовых документов при их обработке СВТ
Скрытие тематики текста	Количество правильно распознанных слов не позволяет установить тематику текста
Скрытие содержания текста	Количество правильно распознанных фраз не позволяет составить аннотацию перехваченного текста (краткую справку о содержании перехваченного текста).

Q_1 и Q_2 – коэффициенты, зависящие от размера шрифта и особенностей восприятия оператором букв (цифр) на зашумленном изображение.

Значения Q_1 и Q_2, определенные по результатам экспериментальных исследований, приведены в табл. 2 [6].

Задаваясь пороговым (требуемым) значе-

Таблица 2

Значения коэффициентов Q_1 и Q_2, определенные по результатам экспериментальных исследований

Показатель распознавания текста	Значение коэффициента Q_1	Значение коэффициента Q_2
Словесная разборчивость W_c	0,89	8,58
Фразовая разборчивость $W_ф$	1,65	14,74

нием разборчивости текста, из формулы (15) легко найти пороговое отношение сигнал/шум (δ)

$$\delta \approx [\Phi^{-1}(W_п) + Q_2]/Q_1, \qquad (16)$$

где $W_п$ – пороговое значение разборчивости текста;

$\Phi^{-1}(x)$ – функция, обратная $\Phi(x)$.

Однако не все распознанные слова или фразы относятся к ключевым, по которым можно установить тематику текста и составить его аннотацию.

Одним из методов определения ключевых фраз и слов в тексте является метод экспертных оценок.

С целью определения относительного количества ключевых фраз и слов в тексте были проведены экспериментальные исследования [9]. Для исследования были выбраны 10 текстов научного стиля технической тематики (статьи из научных журналов) объемом 1300 – 2300 слов (80 – 150 фраз) и 10 текстов публицистического стиля (статьи в блогах, журналах, различного рода новостные статьи) объемом 600 –1000 слов (60 – 100 фраз).

В результате проведенных исследований было установлено, что количество ключевых фраз, необходимое для составления аннотации текста составило: в текстах научного стиля технической тематики составляет от 9 до 13% (среднее значение 10,9%), а в текстах публицистического стиля – от 7 до 12% (среднее значение 8,5%) от общего количества фраз;

Аналогичные исследований были проведены в работе [10]. Для исследования были выбраны 4 текста разной тематики, объемом от 800 до 2500 слов (110 – 500 фраз). В результате проведенных исследований было установлено, что количество ключевых фраз, необходимое для составления аннотации текста составило от 9,5 до 14,1% (среднее значение 11,8%) от общего количества фраз в тексте.

Проведенный анализ показал, что для определения тематики текста необходимо от 5 до 10 ключевых слов. При этом по результатам экспериментальных исследований [10] установлено, что количество ключевых слов составляет от 2,8 до 3,9% (среднее значение 3,2%) от общего количества слов в тексте. А для составления аннотации текста достаточно 25 – 35 ключевых фраз.

Количество распознанных ключевых слов ($N_{с.кл}$) и фраз ($N_{ф.кл}$) в перехваченном тексте можно рассчитать по формулам:

$$N_{с.кл} = N_с \cdot W_с \cdot N_{с.ср}; \qquad (17)$$

$$N_{ф.кл} = N_ф \cdot W_ф \cdot N_{ф.ср}, \qquad (18)$$

где $N_с$ – общее количество слов в перехваченном тексте;

$N_ф$ – общее количество фраз в перехваченном тексте;

$N_{с.ср}$ – относительное количество ключевых слов в перехваченном тексте;

$N_{ф.ср}$ – относительное количество ключевых фраз в перехваченном тексте;

$W_с$ – словесная разборчивость перехваченного текста;

$W_ф$ – фразовая разборчивость перехваченного текста.

Задаваясь пороговым значением ключевых слов ($N_{с.п}$), необходимых для установления тематики текста, и пороговым значением ключевых фраз ($N_{ф.п}$), необходимых для составления аннотации текста, из уравнений (16) и (17) легко получить пороговые значения словесной ($W_{с.п}$) и фразовой ($W_{ф.п}$) разборчивости текста

$$W_{с.п} = N_{с.п} / (N_с \cdot N_{с.ср}); \quad (19)$$

$$W_{ф.п} = N_{ф.п} / (N_ф \cdot N_{ф.ср}). \quad (20)$$

Следовательно, в качестве показателя эффективности защиты текстовой информации при ее обработке СВТ целесообразно использовать количество правильно распознанных ключевых слов ($N_{с.кл}$) и фраз ($N_{ф.кл}$) в перехваченном тексте, которые зависят как от словесной и фразовой разборчивости текста, так и от его объема и характера.

Учитывая, что словесная и фразовая разборчивости текста зависят от отношения сигнал/шум, можно установить критерии эффективности защиты текстовых документов, выводимых на экран монитора (см. табл. 3).

Допустим, для текста, состоящего из 270

Таблица 3

Показатели и критерии эффективности защиты текстовой информации, при ее обработке СВТ

Цели защиты текстовых документов	Условия достижения цели защиты	Показатель эффективности защиты текстовых документов	Критерии эффективности защиты текстовых документов
Скрытие тематики текста	Количество правильно распознанных слов не позволяет установить тематику текста	Отношение информативный сигнал/шум на входе разведывательного приемника (q)	$q \le \delta_с$; $\delta_с \approx [\Phi^{-1}(W_{с.п}) + 8{,}58] / 0{,}89$; $W_{с.п} = N_{с.п} / (N_с \cdot N_{с.ср})$.
Скрытие содержания текста	Количество правильно распознанных фраз не позволяет составить аннотацию перехваченного текста (краткую справку о содержании перехваченного текста)	Отношение информативный сигнал/шум на входе разведывательного приемника (q)	$q \le \delta_ф$; $\delta_ф \approx [\Phi^{-1}(W_{ф.п}) + 14{,}74] / 1{,}65$; $W_{ф.п} = N_{ф.п} / (N_ф \cdot N_{ф.ср})$.

фраз, объемом в 1500 слов, достаточно 5 ключевых слов и 25 ключевых фраз, а $N_{с.ср} = 0{,}028$ и $N_{ф.ср} = 0{,}095$. Тогда:

$$W_{с.п} = 5 / (1500 \cdot 0{,}028) \approx 0{,}12;$$

$$W_{ф.п} = 25 / (270 \cdot 0{,}095) \approx 0{,}97.$$

Подставляя значения пороговой разборчивости в формулу (16) получаем пороговые значения отношения сигнал/шум:

– для фразовой разборчивости текста:

$\delta_ф \approx [\Phi^{-1}(0{,}97) + 14{,}74] / 1{,}65 \approx 10{,}1$ дБ;

– для словесной разборчивости текста:

$\delta_с \approx [\Phi^{-1}(0{,}12) + 8{,}58] / 0{,}89 \approx 8{,}3$ дБ.

Для оценки возможностей средств разведки по перехвату ПЭМИ СВТ часто используют такое понятие, как опасная зона R2, под которой понимается пространство вокруг СВТ, в пределах которого отношение информативный сигнал/шум для ПЭМИ СВТ на входе разведывательного приемника (q) превышает допустимое (нормированное) значение (δ). То есть, это пространство вокруг СВТ, в пределах которого возможет перехват ПЭМИ и восстановление текста, выводимого на экран монитора, с требуемым для решения задач разведки качеством.

Расчет опасной зоны R2 осуществляется в следующей последовательности:

– на основе измеренных значений спектральных составляющих ПЭМИ СВТ для расстояния r = 1 м ($V_r = 1$) для каждого j-го частотного интервала по формулам (12) - (14) рассчитываются отношения сигнал/шум ($q_{с.N.j}$) и сравниваются с пороговым значением (δ);

– если для j-го частотного интервала $q_{с.N.j} > \delta$, то с шагом Δr = 1 м по формулам (6) – (8) рассчитывается затухание ПЭМИ и по формулам (12) - (14) рассчитываются отношения сигнал/шум ($q_{с.N.j}$) с учетом затухания и сравниваются с пороговым значением (δ). Для каждого частотного интервала расчет проводится до тех пор, пока $q_{с.N.j} \le \delta$. Минимальные значения r_j, при которых выполняется условие $q_{с.N.j} \le \delta$, фиксируются;

– за значение R2 принимается максималь-

ное значение из $\{r_j\}$ для всех частотных интервалов, то есть $R2 = \max\{r_j\}$.

Выводы

– в качестве обобщенного показателя эффективности защиты текстовой информации, выводимой на экран монитора СВТ, от перехвата средствами разведки ПЭМИ, целесообразно использовать количество правильно распознанных ключевых слов и фраз в перехваченном тексте;

– предложен методический подход к определению пороговых значений правильно распознанных ключевых слов и фраз в перехваченном тексте, которые зависят как от словесной и фразовой разборчивости текста, так и от его объема и характера;

– экспериментально установлено, что словесная и фразовая разборчивости перехваченного текста зависят от отношения информативный сигнал/шум на входе разведывательного приемника. Получены аналитические соотношения для расчета словесной и фразовая разборчивости текста в зависимости от отношения информативный сигнал/шум на входе разведывательного приемника;

– обоснованы пороговые значения отношений информативный сигнал/шум на входе разведывательного приемника для решения задач защиты текстовой информации, выводимой на экран монитора СВТ, от перехвата средствами разведки ПЭМИ.

Литература

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2010. – 436 с.

2. DVI (Digital Visual Inter face). – URL: https://ru.bmstu.wiki/DVI_(Digital_Visual_Interface)#.D0.92.D0.B8.D0.B4.D1.8B_DVI (дата обращения: 28.08.2022).

3. ANT product data. – URL: https://habr.com/ru/post/209746/? (дата обращения: 28.08.2022).

4. Хорев А.А., Феизов С.А. Экспериментальные исследования возможности перехвата текстовых изображений, выводимых на экран монитора// Международная конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2020». Доклады. – М.: РНТОРЭС имени А.С. Попова. 2020. – С. 259. – 264. – URL: https://elibrary.ru/item.asp?id=45676396 (дата обращения: 28.08.2022).

5. Kuhn G. Compromising emanations: eavesdropping risks of computer displays. This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the Universityof Cambridge, Wolfson College. – URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf (дата обращения: 28.08.2022).

6. Хорев А.А. Методика оценки вероятности распознавания текстовых символов на зашумленных изображениях// Вестник УрФО «Безопасность в информационной сфере». – Челябинск, УрФО. – 2019. – № 4(34) – С. 5. – 14. – URL: https://www.elibrary.ru/item.asp?id=41879982 (дата обращения: 28.08.2022).

7. Хорев А.А. Контроль защищенности средств вычислительной техники от утечки информации по техническим каналам. Часть 1// Специальная техника. – М.: 2015. – № 1. – С. 53 – 63.

8. Хорев А.А. Контроль защищенности средств вычислительной техники от утечки информации по техническим каналам. Часть 2// Специальная техника. – М.: 2015. – № 2. – С. 36 – 63.

9. Прохоренко Л.А. Экспериментальные исследования распознавания оператором текстовой информации на зашумленных изображениях: магистерская диссертация: 10.04.01. – М.: МИЭТ, 2018. – 67 с.

10. Чеботарева А.Д. Методика оценки необходимого количества фраз из перехваченного сообщения для составления аннотации к тексту//Международная конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2019». Доклады. – М.: РНТОРЭС имени А.С. Попова. 2019. – С. 345. – 350. – URL: https://www.elibrary.ru/item.asp?id=39137570&pff=1 https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf (дата обращения: 28.08.2022).

References

1. Khorev A.A. Tekhnicheskaya zashchita informatsii: ucheb. posobiye dlya studentov vuzov. V 3-kh t. T. 1. Tekhnicheskiye kanaly utechki informatsii. - M.: NPTS «Analitika», 2010. – 436 p.

2. DVI (Digital Visual Inter face). - URL: https://ru.bmstu.wiki/DVI_(Digital_Visual_Interface)#.D0.92.D0.B8.D0.B4.D1.8B_DVI (data obrashcheniya: 28.08.2022).

3. ANT product data. – URL: https://habr.com/ru/post/209746/? (data obrashcheniya: 28.08.2022).

4. Khorev A.A., Feizov S.A. Eksperimental'nyye issledovaniya vozmozhnosti perekhvata tekstovykh izobrazheniy, vyvodimykh na ekran monitora// Mezhdunarodnaya konferentsiya «Radioelektronnyye ustroystva i sistemy dlya infotelekommunikatsionnykh tekhnologiy – REUS-2020». Doklady. – M.: RNTORES imeni A.S.Popova. 2020. – P. 259. – 264. – URL: https://elibrary.ru/item.asp?id=45676396 (data obrashcheniya: 28.08.2022).

5. Kuhn G. Compromising emanations: eavesdropping risks of computer displays. This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the Universityof Cambridge, Wolfson College. – URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf (дата обращения: 28.08.2022).

6. Khorev A.A. Metodika otsenki veroyatnosti raspoznavaniya tekstovykh simvolov na zashumlennykh izobrazheniyakh// Vestnik UrFO «Bezopasnost' v informatsionnoy sfere». – Chelyabinsk, UrFO. – 2019. – № 4(34) – P. 5. – 14. – URL: https://www.elibrary.ru/item.asp?id=41879982 (data obrashcheniya: 28.08.2022).

7. Khorev A.A. Kontrol' zashchishchennosti sredstv vychislitel'noy tekhniki ot utechki informatsii po tekhnicheskim kanalam. Chast' 1// Spetsial'naya tekhnika. – M.: 2015. – № 1. – P. 53–63.

8. Khorev A.A. Kontrol' zashchishchennosti sredstv vychislitel'noy tekhniki ot utechki informatsii po tekhnicheskim kanalam. Chast' 2// Spetsial'naya tekhnika. – M.: 2015. – № 2. – P. 36–63.

9. Prokhorenko L.A. Eksperimental'nyye issledovaniya raspoznavaniya operatorom tekstovoy informatsii na zashumlennykh izobrazheniyakh: magisterskaya dissertatsiya: 10.04.01. – M.: MIET, 2018. – 67 p.

10. Chebotareva A.D. Metodika otsenki neobkhodimogo kolichestva fraz iz perekhvachennogo soobshcheniya dlya sostavleniya annotatsii k tekstu//Mezhdunarodnaya konferentsiya «Radioelektronnyye ustroystva i sistemy dlya infotelekommunikatsionnykh tekhnologiy – REUS-2019». Doklady. – M.: RNTORES imeni A.S.Popova. 2019. – S. 345 – 350. – URL: https://www.elibrary.ru/item.asp?id=39137570&pff=1 https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf (data obrashcheniya: 28.08.2022).

ХОРЕВ Анатолий Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность», «Национальный исследовательский университет «МИЭТ». 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1, МИЭТ. E-mail: horev@miee.ruю

HOREV Anatoly Anatolevich, doctor of technical Sciences, Professor, head of the Department «Information security», National Research University of Electronic Technology. 124498, Moscow, Zelenograd, Shokin square, house 1, MIET. E-mail: horev@miee.ru.

УДК 004.454

Вестник УрФО № 3(45) / 2022, с. 17–23

Куц Д.В., Поршнев С.В., Куц М.П.

DOI: 10.14529/secur220302

АНАЛИЗ МЕХАНИЗМОВ УДАЛЕНИЯ ФАЙЛОВ НА SSD НАКОПИТЕЛЯХ

В статье обсуждаются особенности механизмов удаления выбранных файлов, хранящихся на SSD-накопителях, оказывающие влияние на хранение и удаление данных. Описаны отличия механизмов удаления файлов SSD- от HDD-накопителей, а также особенности данных механизмов, используемых SSD-накопителях с файловой системой NTFS, в которой включена поддержка команд TRIM и Deallocate, а также результаты исследования поведение SDD-накопителя с аномалиями при использовании команды TRIM. На основе данных результатов сделан обоснованный вывод о возможностях программного восстановления данных на SSD-накопителях.

Ключевые слова: *TRIM, deallocate, восстановление данных, solid-state drive, NTFS, твердотельный накопитель, выравнивание износа, сборка мусора.*

Kuts D.V., Porshnev S.V., Kuts M.P.

THE ANALYSIS OF FILE DELETION MECHANISMS ON SSD DRIVES

This article describes the specifics of SSD drives work that occurs when single files are deleted. The differences between SSD drives and traditional HDD-type drives in terms of behavior when deleting data are considered. The mechanisms of SSD operation that affect storage and deletion of data on drives are considered. Analysis of behavior of a number of SSD drives with the NTFS file system with support of TRIM and Deallocate commands is carried out. A study of behavior of drive with anomalies in TRIM operation is carried out. The conclusion about the possibilities of software data recovery on SSD is made.

Keywords: *TRIM, deallocate, data recovery, solid-state drive, NTFS, solid state drive, wear leveling, garbage collection.*

Анализ современного рынка накопителей информации на жестких дисках позволяет сделать вывод о том, что происходит активная замена HDD-накопителей более высокопроизводительными SSD-накопителями, надежность хранения данных на которых оказывается сравнимой с аналогичной характеристикой HDD-накопителей. В этой связи сегодня в большинстве серверных и десктопных решений в качестве основного носителя используются SSD-накопители, а HDD-накопители используются в качестве дополнительных накопителей для хранения больших объёмов данных, не требующих высокой скорости доступа.

Несмотря на то, что для операционной

системы (ОС) и для конечного пользователя SSD-накопитель по логике своей работы мало чем отличается от HDD-накопителя (за исключением быстродействия), на SSD-накопителях используются принципиально иные механизмы записи, хранения, удаления данных. Напомним, что на SSD-накопителе в качестве хранилища данных преимущественно используют NAND-память [1]. Данный тип памяти обладает высокой скоростью чтения, записи и значительной надёжностью, которому, однако, присущи некоторые недостатки. Из них основным оказывается конечный ресурс ячеек памяти на запись в них данных. Напомним, что в современных накопителях на жестких дисках ресурс памяти на запись определяется максимальным гарантированным объёмом записанной информации за весь срок пользования SSD-накопителя (англ. Total Bytes Written, TBW). При этом очевидно, что необходимым условием использование данного параметра является выполнение требования о том, количество операций записи в каждую ячейки памяти SSD-накопителя будет примерно одинаковым. Однако ОС, напротив, многие системные файлы (например, журнал транзакций, файл подкачки, log-файлы и др.), перезаписывает соответствующие данные в одни и те же ячейки памяти многократно, в то время как другие ячейки, в которые записаны не изменяемые регулярно данные, оказываются использованные, фактически, однократно. В результате возникает проблема неравномерного износа ячеек памяти SSD-накопителей, для решения которой используется технология выравнивания износа (англ. Wear Leveling), реализованная в контроллере SSD-накопителя [2], которая делает NAND-память надёжной и отказоустойчивой.

Технология Wear Leveling основана на совместном использовании абстрагированного логического адресного пространства SSD-накопителя и физических адресов ячеек памяти микросхем, обеспечиваемом технологией FTL (Flash Translation Layer), которая обеспечивает сопоставление логических и физических адресов SSD-накопителей. В данной технологии в случае записи новых данных логические адреса физических адресов ячеек памяти заменяются на адреса менее изношенных ячеек, что и обеспечивает равномерный износ каждой ячейки памяти носителя на твердом диске. К недостаткам технологии FTL следует отнести трудности, возникающие при перезаписи данных на SSD-накопитель, которые, в свою очередь, приводят к возникновению проблем гарантированного стирания файлов, связанных с тем, что данные, недоступные логически, микросхемах памяти остаются до тех пор, пока не доберётся «сборщик мусора».

Сборка мусора (Garbage collection) – это технология, осуществляющая зачистку неиспользуемого пространства SSD-накопителя. Ещё одна особенность памяти NAND состоит в том, что каждая ячейка памяти, перед повторной записью должна быть очищена. Процесс стирания в NAND-памяти, однако, значительно медленнее, чем запись или чтение. Соответственно, лучшей стратегией для SSD-накопителя является заблаговременная подготовка очищенных ячеек памяти для их быстрой записи в случае необходимости. Таким образом, на SSD-накопителях происходит регулярный процесс сборки мусора, что обеспечивает поддержку высокого быстродействия SSD-накопителя.

Одним из эффективных способов повысить эффективность сборки мусора на накопителе является информирование управляющего контроллера накопителя ОС о тех блоках данных, которые принадлежали уже удалённым файлам, а потому могут быть очищены. Данное информирование реализуется с помощью команды TRIM интерфейса SATA или Deallocate для интерфейса PCI-E. Отметим, что сборка мусора не заменяет функционал TRIM на SSD-накопителе, но, наоборот, TRIM помогает бы сборке мусора быть более эффективной и производительной [3]. Удаление данных может быть выполнено в фоновом режиме, в то время как пользователь использует ОС или может быть запрограммировано на очистку после перезагрузки [4], с которой, однако, на практике авторам сталкиваться не приходилось. При удалении файла, с включёнными командами TRIM или Deallocate, сектора с его данными, как показывает опыт, очищаются примерно за 5-15 секунд. Это порождает распространённое мнение о том, что восстановить удалённые файлы на SSD-накопителе с включённой командой TRIM без аппаратного вмешательства и чтения напрямую с микросхем памяти невозможно. Результаты нашего исследования, обсуждаемые далее, свидетельствуют о том, что данное утверждение оказывается не вполне справедливым.

Изначально отметим, что, во-первых, ко-

манды TRIM и Deallocate, даже будучи активными, не работают на внешних накопителях, подключенных через USB порт; во-вторых, команды TRIM и Deallocate не функционируют на виртуальных машинах и в RAID-массивах; в-третьих, особенности файловой системы NTFS не позволяют отрабатывать команд TRIM и Deallocate для файлов, хранящих содержимое в резидентных атрибутах [5] (размером менее 700 байт), что, потенциально, дает возможность восстановления любых удалённых файлов на SSD-накопителе. Кроме того, команды TRIM и Deallocate не работают при повреждении файловой системы тома или при его удалении. Также необходимо отметить, что в случаях, не имеющих отношения к вышеперечисленным, реализация сборки мусора на SSD-накопителе целиком и полностью лежит на производителе устройства. Для этой технологии нет единого стандарта, поэтому каждый производитель SSD реализует её по-своему. Следовательно, реализация работы команд TRIM и Deallocate и последующего затирания неактуальных данных сборщиком мусора, может существенно отличаться на накопителях разных производителей.

В рамках нашего исследования, мы использовали доступные нам SSD-накопители от 7 различных производителей, в том числе компаний Azerty, Samsung, Crucial, Kingston, Transcend, ADATA, Intel. Названия тестируемых моделей и их производителей представлены в табл. 1.

Таблица 1

Тестируемые модели SSD-накопителей

Модель SSD накопителя	Производитель	Ёмкость	Интерфейс
Bory R500 (029-1118)	Azerty	240 Gb	SATA III
870 EVO MZ-77E500BW	Samsung	500 Gb	SATA III
CT480BX500SSD1	Crucial	500 Gb	SATA III
SUV400S37/120G	Kingston	120 Gb	SATA III
TS256GSSD230S	Transcend	256 Gb	SATA III
AGAMMIXS11P-512GT-C	ADATA	512 Gb	NVMe M.2
SSDPEKKW256G8	Intel	256 Gb	NVMe M.2

В проведенных экспериментах была использована ОС Windows 10 Enterprise 21H2. Каждый из накопителей имел по одному системному разделу с файловой системой NTFS. В качестве ПО для проведения исследований, нами использовались 16-теричные редакторы WinHex и HxD. В ходе исследования проводились измерения времени, затрачиваемого соответствующим SSD-накопителем на затирание данных удаленных файлов разных размеров. Отметим, что у всех SSD-накопителей время затирания данных файлов, примерно, оказалось в пределах 5-15 секунд. В тоже время было обнаружено, что накопители производителей Samsung и Crucial не очищали стирали некоторую информацию из удаленных файлов, чем обеспечивалась возможность их программного восстановления в течении продолжительного периода времени. Также, нами были обнаружены фрагменты удалённых файлов, даже после отработки командой TRIM и сборщиком мусора. Для более детального исследования был проведён эксперимент, устанавливающий зависимость успешной отработки командой TRIM и последующей сборки мусора от размера удаляемого файла.

Объектом исследования стал накопитель Samsung 870 EVO MZ-77E500BW. В рамках первого этапа, на накопителе создавались по 10 файлов различного размера со случайными повторяющимися текстовыми сигнатурами, обеспечивающими быстрый поиск данных файлов на жестком диске (рис. 1). Цель данного эксперимента состояла: в проверке гипотезы о ли зависимость скорости отработки команды TRIM и сборщика мусора от размера файла; установлени зависимости числа случаев, в которых затирание не данных не произошло, от размера удаляемого файла; выявлении условий, при выполнении которых на накопителя остаются фрагменты удаленных файлов.

В ходе экспериментов каждый файл удалялся через проводник, минуя корзину. Далее, после удаления каждого файла с помощью 16-теричного редактора HxD проводился анализ содержимого секторов, в которых ранее размещался удаленный файл, с целью нахождения отметки времени соответствую-

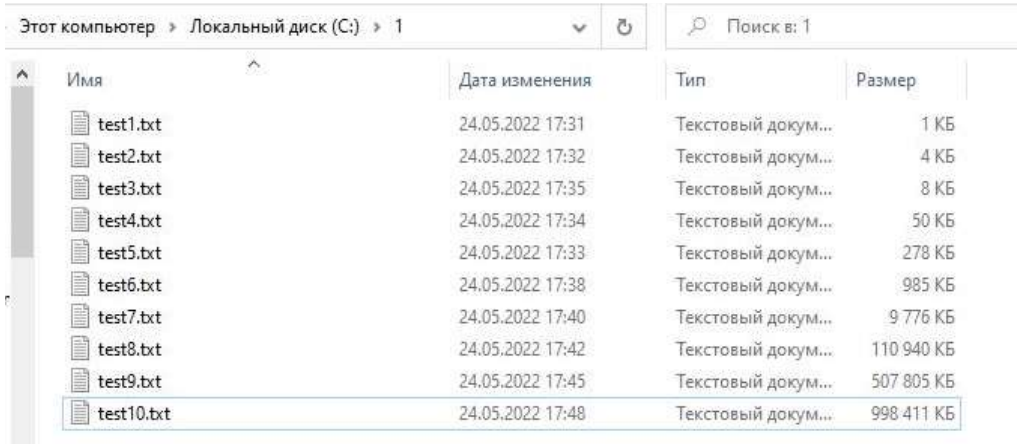

Рис. 1 Файлы различного размера, используемые в исследовании

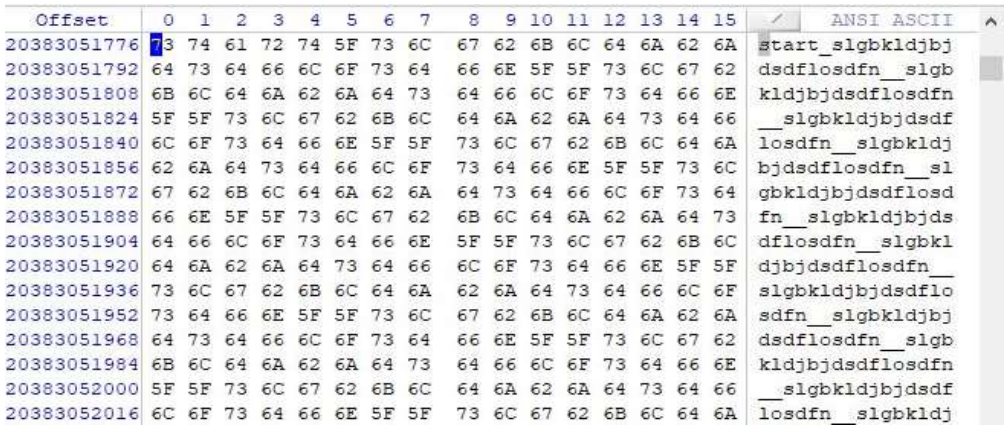

Рис. 2 Пример содержимого удаляемого файла

щей затиранию соответствующей информации. При этом, априори, мы ожидали, что данные сектора после удаления файлы могли быть отданы другому файлу и перезаписаны средствами файловой системы. Описанное действие можно обнаружить по факту принадлежности этих секторов новому файлу, так как, маловероятно, что данные сектора были бы перезаписаны нулями (что происходит при затирании информации с помощью сборщика мусора). Типичные экспериментальные результаты представлены в табл. 2.

Таблица 2

Результаты проверки качества удаления файлов разных размеров с накопителя Samsung 870 EVO MZ-77E500BW

Имя файла	Размер (байт)	Отработка TRIM	Время затирания (сек)	Наличие фрагментов
test1	1002	нет	–	–
test2	4048	нет	–	–
test3	7 513	нет	–	–
test4	51 048	да	8.1	нет
test5	284 480	да	10.0	да (14 144 байт)
test6	1 008 008	да	6.4	да (8 584 байт)
test7	10 010 008	да	8.3	нет
test8	113 602 508	да	10.5	да (12 236 байт)
test9	519 991 928	да	9.0	нет
test10	1 022 372 072	да	5.7	нет

Из табл. 2 видно, что:

1) качество работы сборщика мусора явным образом зависит от размера файла и файлы, при этом удаленные файлы размером менее 7 КБ не затираются;

2) скорость затирания файла не зависит от его размера;

3) в ряде случае данные файла затирались не полностью и на накопителе оставалась информация, находившаяся ранее в конце удаленных файлов, объем который составлял 8-14 Кб.

Для более точного определения максимального размера удаляемого файла, который не затирается сборщиком мусора на SSD-накопителе, была проведена дополнительная серия испытаний, в ходе которой затиралась три файла, размеры которых были отличны друг от друга (см. табл. 3).

Из табл. 3 видно, что максимальный размер затираемого файла составляет ~ 10÷15 килобайт. Для уточнения размера удаляемого файла была проведена еще одна серию экспериментов, результаты которой представлены в табл. 4.

Таблица 3

Результаты поиска максимального размера файла, не затираемого накопителем при удалении

Имя файла	Размер (байт)	Отработка TRIM	Время затирания (сек)	Наличие фрагментов
test1	10 032	нет	–	–
test2	15 272	да	7.5	нет
test3	20 038	да	6.9	да (3142 байта)

Из табл. 4 видно, что минимальный размер затираемого файла на накопителе Samsung 870 EVO MZ-77E500BW составляет ~12.5Кб. Для всех файлов меньшего размера данный накопитель ведёт себя практически как жёсткий диск и не обеспечивает затирание удаленных файлов через сборщика мусора, что с достаточно высокой вероятностью позволяет восстанавливать эти файлы программными методами. Также было обнаружено, что в тех случаях, когда сборщик мусора не затирал некоторые ячейки памяти при первоначальном его использовании, то и далее при его повторном использовании данные ячейки оставались не затертыми. Эти данные хранятся в памяти до тех пор, пока не будут перезаписаны файловой системой. Кроме этого, данный накопитель в ряде случаев, даже после успешной отработки команды TRIM и сборщика мусора, не очищал окончание файлов. Оставшиеся фрагменты имели размер ~8÷14 Кб, что позволяет для некоторых типов файлов восстановить часть информации. Точную зависимость наличия фрагмента файла при затирании от его размера установить не удалось, однако примерно треть всех удаляемых файлов, размер которых превышал 20 Кб, в итоге оставляли после себя «хвосты». Одновременно с этим следует отметить, что некоторые, весьма распространённые типы файлов могут содержать достаточные объёмы информации и при этом иметь размер менее 12,5 Кб.

Таблица 4

Результаты поиска максимального размера файла, не затираемого накопителем при удалении

Имя файла	Размер (байт)	Отработка TRIM	Время затирания (сек)	Наличие фрагментов
test1	11 028	нет	–	–
test2	12 024	нет	–	–
test3	13 012	да	9.8	нет
test4	14 019	да	7.7	нет

В этой связи уместно отметить, что, например, файл текстового процессора MS Word формата DOCX с 760 символами текста имеет размер, примерно 12,5 Кб и, следовательно, не очищается командой TRIM на данном накопителе. Файл DOCX, созданный в редакторе Wordpad с одним символом текста имеет размер 1947 байт, следовательно, фай-

лы, созданные в этом редакторе, могут содержать достаточно большие объёмы текста в файлах размером менее 12,5 Кб. Файл электронных таблиц MS Exel с одним байтом информации имеет размер 8 458 байт, что также позволяет хранить в нем достаточно данных. При этом его объем не будет превосходить 12,5 Кб.

Обнаруженные особенности механизма стирания информации на накопителе Samsung 870 EVO MZ-77E500BW, в первую очередь, в зависимости отработки команды TRIM от размера файла и наличии «хвостов» файлов при их затирании, были также обнаружены на накопителях Samsung 860 EVO MZ-76E500BW и Crucial CT480BX500SSD1, поэтому целенаправленные исследования особенностей выполнения команды TRIM на этих накопителях являются целью дальнейших исследований.

Таким образом, программное восстановление удалённых данных на некоторых SSD-накопителях даже с включёнными командами TRIM или Deallocate вполне может быть результативным, особенно, для файлов небольшого размера. Для реализации надёжного программного затирания файлов, необходимо использовать специализированные инструменты, которые эффективно работают на HDD-носителях, и делают невозможным программное восстановление данных на SSD-носителях. В тоже время понятно, что они не смогут обеспечить гарантированное затирание данных файла на микросхемах памяти SSD, ввиду специфики работы технологии выравнивания износа (Wear Leveling). Следовательно, вопрос гарантированного затирания отдельных файлов на SSD-носителях остаётся актуальным.

Литература

1. Корнвелл М. «Анатомия твердотельного накопителя» Communications of the ACM, 2012, том 55, №12, С. 59–63.

2. Технология выравнивания износа в устройствах с флэш-памятью nand. [Электронный ресурс]. URL: https://www.micron.com/-/media/client/global/documents/products/technical-note/nand-flash/tn2942_nand_wear_leveling.pdf

3. Рент Т.М. «SSD контроллер». [Электронный ресурс] 9 Апр. 2010.

4. Мартин Н., Зиммерман Д., «Анализ вызовов устройствами с флеш-памятью для криминалистов». Университет Небраски, 15 окт. 2015.

5. Губанов Ю.А., Афонин О.А., "Восстановление данных на SSD накопителях: Понимание TRIM, сборки мусора и исключений" 2014. [Электронный ресурс]. URL: https://belkasoft.com/ssd-2014.

References

1. Kornvell M. «Anatomiya tverdotel'nogo nakopitelya» Communications of the ACM, 2012, tom 55, №12, P. 59–63.

2. Tekhnologiya vyravnivaniya iznosa v ustroystvakh s flesh-pamyat'yu nand. [Elektronnyy resurs]. URL: https://www.micron.com/-/media/client/ global/documents/products/technical-note/nand-flash/tn2942_ nand_wear_ leveling.pdf

3. Rent T.M. «SSD kontroller». [Elektronnyy resurs] 9 Apr. 2010.

4. Martin N., Zimmerman D., «Analiz vyzovov ustroystvami s flesh-pamyat'yu dlya kriminalistov». Universitet Nebraski, 15 okt. 2015.

5. Gubanov YU.A., Afonin O.A., "Vosstanovleniye dannykh na SSD nakopitelyakh: Ponimaniye TRIM, sborki musora i isklyucheniy" 2014. [Elektronnyy resurs]. URL: https://belkasoft.com/ssd-2014.

КУЦ Дмитрий Владимирович, старший преподаватель Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: d.v.kutc@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.v.porshnev@urfu.ru

КУЦ Мария Петровна, преподаватель кафедры Иностранных языков и образовательных технологий, Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Куйбышева, 48а. E-mail: m.p.kutc@urfu.ru

KUTS Dmitry Vladimirovich, senior teacher of the Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail:d.v.kutc@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Full Professor, Head of Unit, Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: s.v.porshnev@urfu.ru

KUTS Maria Petrovna, teacher of the Department of Foreign Languages and Educational Technologies, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Kuibysheva street, 48a. E-mail:m.p.kutc@urfu.ru

УДК 004.414.23 + 519.711.2 Вестник УрФО № 3(45) / 2022, с. 24–33

Шамонин Е. Д.

DOI: 10.14529/secur220303

МОДЕЛИРОВАНИЕ ДИСКОВОЙ ПОДСИСТЕМЫ ЭВМ НА ОСНОВЕ ТВЕРДОТЕЛЬНОГО НАКОПИТЕЛЯ В РЕЖИМЕ ЧТЕНИЯ

В последнее время отмечается заметное вытеснение традиционных накопителей на жестких магнитных дисках — НЖМД (Hard Disk Drive, HDD) твердотельными носителями — ТТН (Solid State Drive, SSD), построенными на основе интегральных микросхем (ИМС) flash-памяти не только из сегмента персональных компьютеров, но и из сегмента центров обработки данных (ЦОД). Это происходит по следующим причинам [1]:

• конечное снижение суммарной стоимости закупки плюс стоимости эксплуатации за счет снижения энергопотребления на 60% (для каждой стой-ки, в которой заменили устройства);

• повышение производительности системы хранения данных (СХД) на основе ТТН в 40 раз по сравнению с СХД на основе НЖМД;

• более высокой надежности ТТН, интенсивность отказов которых в 4÷10 раз меньше, чем у НЖМД, что объясняется, в первую очередь, отсутствием у ТТН подвижных механических частей.

В криминалистической практике применительно к машинным носителям информации (МНИ) решаются две основные задачи. Это либо копирование содержимого носителя (полное или выборочное) с последующим исследованием копии на предмет наличия криминалистически значимой информации, либо поиск какой-либо конкретной информации (контекстный поиск) непосредственно на целевом машинном носителе информации с возможным последующим ее копированием.

Таким образом, как в первом, так и во втором случае основным режимом работы целевого МНИ будет чтение.

Моделирование функционирования твердотельного накопителя в режиме чтения на основе информации о модели накопителя (а, следовательно, и спецификации устройства) позволит оценить время, необходимое для получения полной копии содержимого ТТН.

Ключевые слова: *моделирование, дисковая подсистема, копирование, страница чтения, контроллер.*

SIMULATION OF A COMPUTER DISK SUBSYSTEM BASED ON A SOLID STATE DRIVE IN READ MODE

Recently, there has been a noticeable displacement of traditional hard disk drives — HDD (Hard Disk Drive) by solid state drives — SSD (Solid State Drive), built on the basis of integrated circuits (ICs) flash-memory not only from the segment of personal computers, but also from the segment of data centers (DC). This happens for the following reasons [1]:

• the ultimate reduction in the total cost of purchase plus the cost of operation by reducing energy consumption by 60% (for each rack in which the devices were replaced);

• 40 times higher performance of data storage system based on SSD compared to based on HDD;

• higher reliability of SSD, the failure rate of which is 4÷10 times less than that of HDD, which is explained, first of all, by the absence of moving mechanical parts in SSD.

In forensic practice in relation to media type, two main tasks are solved. This is either copying the contents of the media (full or selective) with subsequent examination of the copy for the presence of forensic information, or searching for any specific information (context search) directly on the target media with possible subsequent copying.

Thus, both in the first and in the second case, the main mode of target media operation is reading.

Modeling the functioning of a solid state drive in read mode based on information about the drive model (and, consequently, the device specifications) allow us to estimate the time required to obtain a complete copy of the contents of the hard drive.

Keywords: *modeling, disk subsystem, copying, reading page, controller.*

При считывании данных с ТТН цепь прохождения считанных данных будет включать следующие элементы (рис. 1).

На рис. 1: NAND – устройства flash-памяти; Controller – контроллер SSD; Data Register – регистр данных (страничный); Cache Register

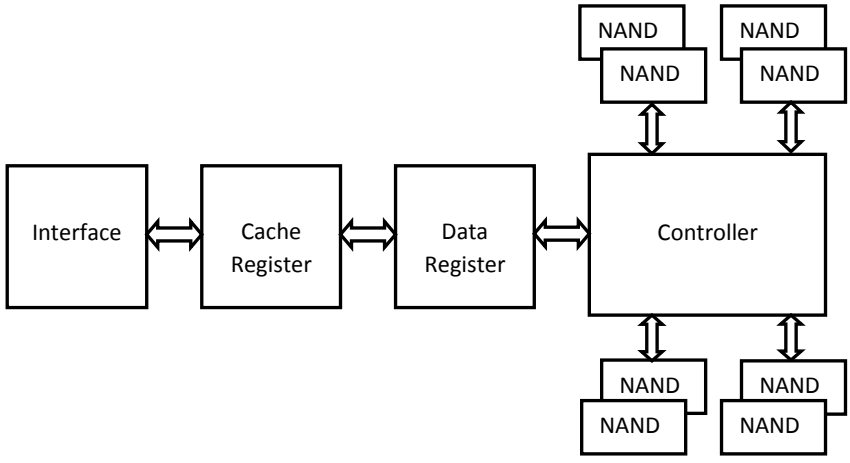

Рис. 1. Цепь прохождения считанных данных в ТТН

– буферная память; Interface – интерфейс накопителя.

Наличие регистра данных связано с особенностью построения ИМС flash-памяти (рис. 2).

Работа с отдельными ячейками ИМС flash-памяти невозможна. Группы ячеек объединяются в страницы чтения/записи. Именно такой объем данных является минимальным для его считывания или записи. Страницы объединяются в более крупный элемент массива – блок стирания. Набор блоков стирания собственно и представляет собой массив ячеек ИМС flash-памяти.

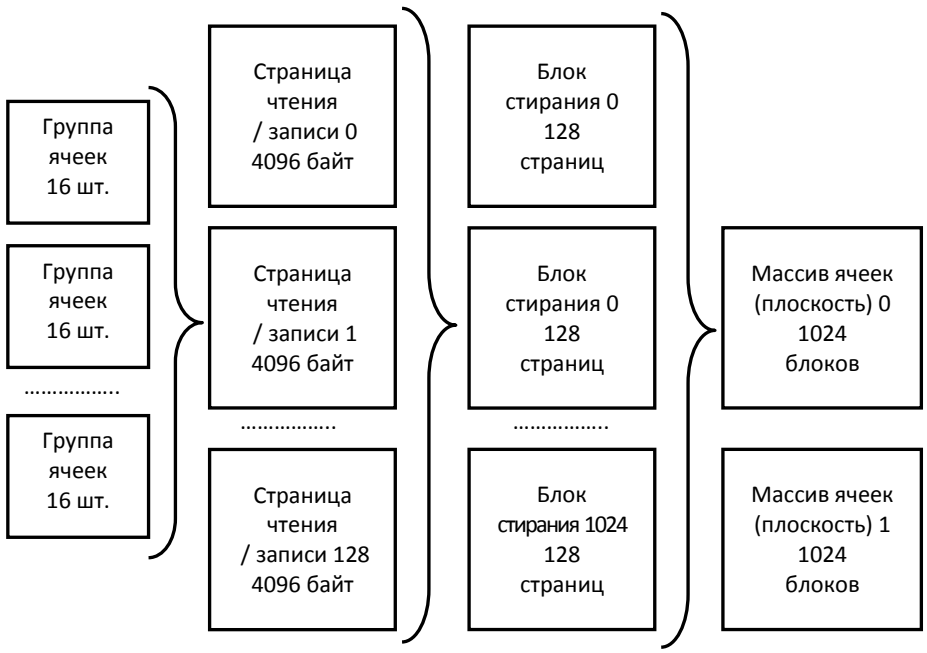

Рис. 2. Массив ячеек ИМС flash-памяти

При считывании данных требуемая страница считывается сначала в регистр данных, и только после этого перемещается в буферную оперативную память, которая также может входить в состав контроллера, либо может быть представлена отдельной ИМС.

В представленном на рис. 1 варианте считывание может осуществляться одновременно по четырем каналам с шириной каждого канала 8 бит (1 байт). Более совершенные контроллеры могут поддерживать 8 каналов с шириной канала 16 бит (2 байта).

Кроме непосредственного использования параллельно 2, 4, 8 каналов [2] существует еще и возможность подключения на каждый канал более одного NAND-устройства. Это может быть две ИМС flash-памяти, либо два NAND-устройства в одном корпусе ИМС (рис. 1). Такое подключение позволяет задействовать еще один механизм ускорения процессов чтения/записи (в первую очередь записи) – чередование (Interleaving).

Пусть C – множество запросов, при которых данные берутся только из кэша, а F – множество запросов, требующих обращения к массиву flash-памяти. Нагрузка представляет собой последовательность запросов из множества $C \cup F$, причем для чтения $C \cap F \neq \varnothing$.

Предположив, что скорость чтения данных из каждого хранилища постоянна и равна v^r_c и v^r_f, можно записать время выполнения одного запроса:

$$t^r_c = s^r_c / v^r_c,\ t^r_f = s^r_f / v^r_f,$$

где s^r_c и s^r_f – количество запрашиваемых байт соответственно из кэша и массива flash-памяти.

В работе [3] применительно к НЖМД время выполнения последовательности запросов чтения представлено как линейная функция трех переменных:

$$T^r = N^r_d * t^r_0 + S^r_d / v^r_0 + S^r_c / v^r_c, \qquad (1)$$

где N^r_d – общее количество дисковых запросов на чтение; S^r_d и S^r_c – общее число байтов, прочитанных за время T^r с пластин жесткого диска и из кэша соответственно; t^r_0 – среднее время поиска.

Данную модель можно адаптировать и для прогнозирования производительности дисковой подсистемы ЭВМ на основе ТТН.

Параметры нагрузки остаются прежними,

т. е. N^r_f – количество за-про¬сов на чтение из flash-памяти; S^r_f – общее число байтов, считанных из flash-памяти; S^r_c – общее число байтов, считанных из кэша.

Коэффициенты модели для ТТН будут иметь тот же физический смысл, но применительно конструкции твердотельного носителя. Первый коэффици-ент модели (1) применительно к НЖМД – среднее время поиска, т. е. за-держка между временной отметкой, как поступил запрос на чтение и отмет-кой, когда началось реальное считывание данных.

Применительно к ТТН данная задержка зависит от технологии изго-товле¬ния flash-памяти, а именно емкости отдельной ячейки памяти. Формат хранения данных в flash-памяти типа NAND медленно эволюционировал к повышению емкости микросхем за счет увеличения количества бит, храни-мых в одной ячейке, что в свою очередь вело к увеличению времени доступа (табл. 1) [4].

На смену первому поколению ячеек SLC (Single-Level Cell), хранивших один бит в ячейке, пришло следующее MLC (Multi-Level Cell) с

Таблица 1

Характеристики ячеек NAND-памяти

Характеристика	SLC	MLC	TLC
Количество циклов стирания/записи	100 000	10 000	5 000
Количество бит в ячейке	1	2	3
Задержка поиска, мкс	–	–	–
Задержка чтения, мкс	25	50	100
Задержка записи, мкс	250	900	1 500
Задержка стирания, мкс	1 500	3 000	5 000

двумя битами в ячейке, а затем TLC (Triple-Level Cell) с тремя битами в ячейке.

При этом необходимо иметь ввиду, что при снятии полной копии будет задействовано конвейерное чтение, которое за счет наличия нескольких каналов позволяет свести к минимуму задержки чтения, а именно задержка будет иметь место только при чтении первой страницы.

Конкретно (упрощенно), происходит следующее (рис. 3, б) [5]:

• команда чтения первой страницы (с указанием адреса);

• большая пауза для получения данных из матрицы;

• команда кэширующего чтения второй страницы (с указанием адреса);

• вычитывание данных из первой страницы. В действительности, данные считываются из буферного регистра (Cache Register), в который они переписались сразу по факту окончания передачи из матрицы в регистр данных. Пока идет процесс вычитывания данных из микросхемы, данные страницы номер два переписываются в освободившийся регистр данных;

• команда кэширующего чтения третьей страницы (с указанием адреса);

• вычитывание второй страницы из буферного регистра и т. д.

Дополнительные накладные расходы ожидания есть только для чтения первой страницы, все остальные идут без пауз – время ожидания выполнения чтения из матрицы flash-памяти (tR) скрадывается временем передачи данных из микросхемы (Data Output).

На рис. 3 представлен вариант чтения страницы объемом 4 КВ, выполненной по технологии MLC, без кэширования (3, а) и с кэшированием (3, б) [5].

Чередование на уровне шины устройства не требует сложных изменений оборудования, а дополнительные накладные расходы невелики. Для устройства с чередованием на уровне шины рост производительности составляет от 55% до 85% [6].

На рис. 4 представлен вариант чтения страницы объемом 4 КВ, выполненной по технологии MLC с одной (4, а) и двумя плоскостями (4, б) [5]. В данном случае уже имеет место интерливинг для двух плоскостей NAND-устройства.

Чередование плоскостей флэш-памяти не требует специальной конструкции оборудования, но аппаратное и программное обеспечение флэш-памяти должно поддерживать плоскости. Такое чередование может повысить производительность от 30% до 80% [6].

Таким образом, первый коэффициент модели (1) можно взять из табл. 1 в зависимости от технологии изготовления ячейки. Пара-

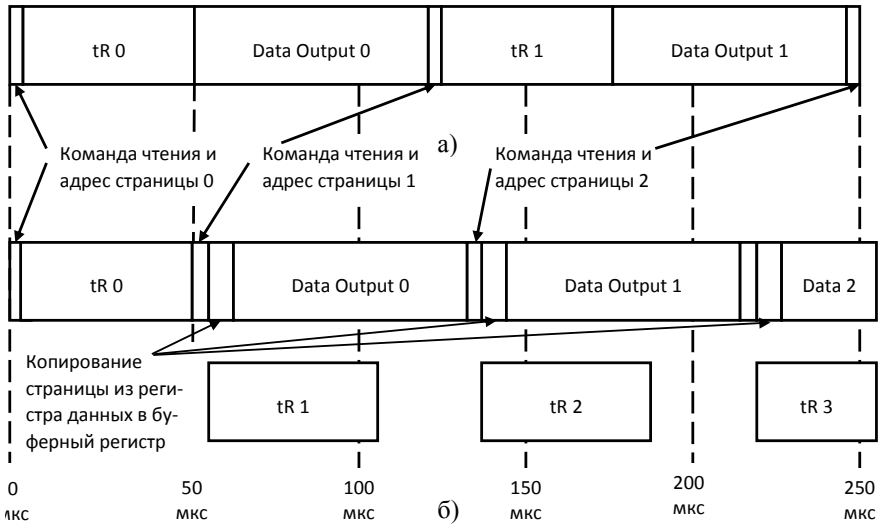

Рис. 3. Чтение страницы 4 КВ MLC: а — без кэширования (скорость чтения 27,3 МБ/с);
б — с кэшированием (скорость чтения 36,5 МБ/с)

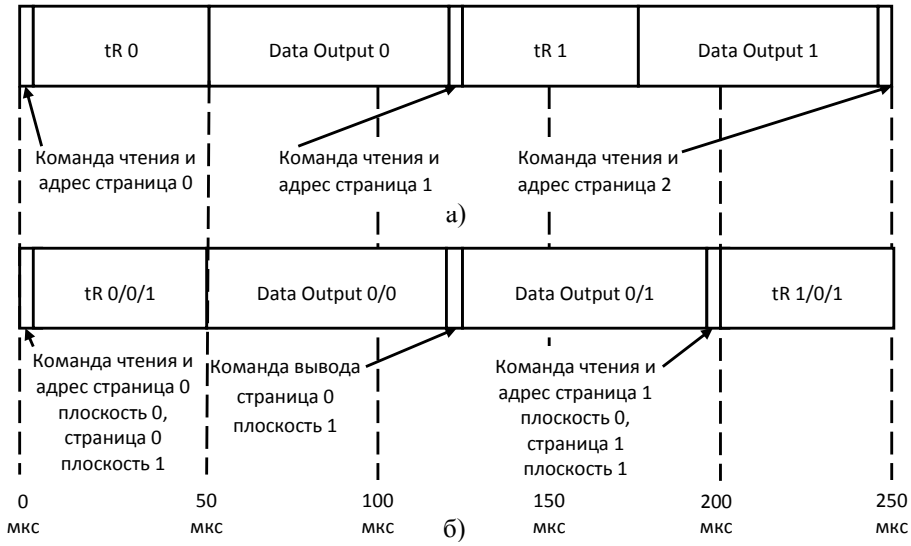

Рис. 4. Чтение страницы 4 КВ MLC: а — NAND-устройство содержит одну плоскость (скорость чтения 27,3 МБ/с);
б — NAND-устройство содержит две плоскости (скорость чтения 32,4 МБ/с)

метр нагрузки – количество запросов на чтение из flash-памяти – будет равен $N^r_f = 1$ из-за особенностей конвейерного чтения.

Второй коэффициент модели (1) для НЖМД представляет собой величину, обратную внутренней скорости передачи данных с пластин жесткого диска во внутренний буфер. По аналогии для ТТН данный коэффициент будет характеризовать скорость передачи данных, считанных из матрицы flash-памяти. Так как считывание данных происходит из нескольких NAND-устройств, то данный коэффициент будет напрямую зависеть от количества каналов, поддерживаемых контроллером SSD, а также процедур чередования, реализованных в накопителе в целом. Кроме того, необходимо учитывать, какие именно процедуры интерливинга будут задействованы исходя из количества и конструкции ИМС flash-памяти и наличие (либо отсутствие) в SSD буферной (кэш) памяти.

Допустим, SSD реализован в виде накопителя, блок-схема которого приведена на рис. 1. Тогда, исходя из количества NAND-устройств (8), если это отдельные ИМС, на каждой шине (канале) будет задействован шинный интерливинг. Если же это 4 ИМС, каждая из которых будет содержать две плоскости flash-памяти, как на рис. 2, то будет задействовано чередование плоскостей. Следовательно, внутреннюю скорость передачи данных можно представить как скорость чтения

страницы v^r_1 (рис. 3, а), умноженную на количество каналов (шин) n, поделенное на коэффициент интерливинга a, так как одномоментно восьмибитная шина может передавать данные только от одного NAND-устройства (ИМС или плоскости), т. е. $\frac{1}{v^r_1 * n/\alpha}$.

Считанные данные будут последовательно перемещаться вначале в регистр данных, а затем в буферную память (см. рис. 1), т. е. через эти элементы будет проходить весь объем считанных данных. Поэтому третье слагаемое в модели (1) можно отбросить, а влияние кэша учесть непосредственно скоростью чтения во втором слагаемом модели (1) (рис. 3, б).

Следовательно, применительно к ТТН время выполнения последовательности запросов чтения может быть представлено как линейная функция двух переменных:

$$Tr = tr0 * Nrf + \frac{1}{v^r_1 * n/\alpha} * S^r_f, \quad (2)$$

Для определения количества каналов, поддерживаемых контроллером SSD, и коэффициента интерливинга, необходимо иметь более обширную информацию, чем та, которая приводится в спецификации на SSD (рис. 5) [7]. Дополнительно могут потребоваться спецификации на контроллер, ИМС flash-памяти, а также информация о наличии буферной памяти (встроенной в контроллер, либо представленной в виде отдельной ИМС).

Specifications

Product Model	SP600
Capacity	32GB/64GB/128GB
Form factor	2.5 inch
NAND Flash	Synchronous multi-Level Cell (MLC) NAND Flash Memory
Controller	JMicron , 66X Series
Dimensions	100 x 69.85 x 7mm (L x W x H)
Weight	68g
Interface	SATA 6Gb/s

Рис. 5. Спецификация на SSD ADATA модель SP600

Как видно из рис. 5, в спецификации о контроллере и используемых ИМС flash-памяти присутствует только самая общая информация, из которой нельзя сделать выводы о количестве каналов, поддерживаемых контроллером, количестве ИМС памяти и количестве NAND-устройств, используемых в SSD.

Вскрытие корпуса накопителя объемом 64 ГБ позволило выяснить наличие контроллера JMF670H (четырехканальный) и 4 ИМС ADATA 600. Поскольку компания ADATA сама микросхем flash-памяти не производит, а закупает у другого производителя (как правило, одного и того же), то пришлось изучить содержимое более объемного ADATA SSD на 128 ГБ, на плате которого имелось 8 ИМС 29F16B08CC (производитель компания Micron). Был сделано предположение, что в SSD на 64 ГБ установлены аналогичные ИМС. Первые три символа – 29F – указывают, что это NAND flash-память, следующие три – 16B – объем 16 ГБ, далее – 08 – разрядность шины 8 бит, символ C – количество бит в ячейке – 2 бита, последний символ C – количество кристаллов в ИМС – 2 кристалла.

Таким образом, имеем четырехканальный контроллер, к которому подключены 4 ИМС flash-памяти компании Micron, каждая из которых имеет 2 кристалла (плоскости), т. е. в SSD реализовано чередование на уровне плоскостей. Какой прирост производительности это дает оценить достаточно сложно, поэтому остановимся на среднем значении 50%, т. е. коэффициент интерливинга принимаем равным a = 1,5.

Осуществим оценку времени, необходимого для получения полной копии SDD, объем которого составляет 64 ГБ или 65536 МБ, скорость считывания страницы 4 КБ 32,4 МБ/с (рис. 4, б) (буферная память отсутствует).

$$T^r = t^r_0 * N^r_f + \frac{1}{v^r_1 * n/\alpha} * S^r_f = 0{,}00005 * 1 + \frac{65536}{32{,}4 * 4/1{,}5} = 758{,}51857 \text{ с} = 12 \text{ мин } 38 \text{ с}.$$

Время полного копирования с использованием программно-аппаратного комплекса (ПАК) PC-3000 составило 11 мин 49 с. Разница между расчетным временем и практическим составляет 49 с.

Для проверки адекватности модели осуществим расчет и практическое копирование еще для двух накопителей разных производителей и объемов.

ТТН Silicon Power CPCC 128 ГБ на контроллере SM2246XT (четырехканальный), 2 ИМС 29F64G08 CM. Первые три символа – 29F – указывают, что это NAND flash-память, следующие три – 64G – объем 64 ГБ, далее – 08 – разрядность шины 8 бит, символ C – количество бит в ячейке – 2 бита, последний символ M – количество кристаллов в ИМС – 4 кристалла.

Контроллер имеет четыре канала, а ИМС всего две, но в каждой по четыре кристалла, т. е. к каждому каналу подключено 2 кристалла одной из ИМС или одна ИМС подключена к двум каналам. Используем тот же коэффициент интерливинга a = 1,5.

Осуществим оценку времени, необходимого для получения полной копии SDD, объем которого составляет 128 ГБ или 114 470 МБ, скорость считывания страницы 4 КБ 36,5 МБ/с (рис. 3, б) (есть ИМС буферной памяти объемом 512 МБ).

$$T^r = t^r_0 * N^r_f + \frac{1}{v^r_1 * n/\alpha} S^r_f = 0{,}00005 * 1 + \frac{114470}{36{,}5 * 4/1{,}5} = 1176{,}10197 \text{ с} = 19 \text{ мин } 36 \text{ с}.$$

Время полного копирования с использованием ПАК PC-3000 составило 18 мин 37 с. Разница между расчетным временем и практическим составляет 59 с.

SSD Plextor PX-256M6S 256 ГБ на контроллере Marvell 88SS9188 (четырехканальный), 8 ИМС TH58TEG8DDKTA20. Расшифровка маркировки ИМС компании Toshiba вызвала проблему, поскольку ни в одном из источников она не приводится, но зато производитель ТТН приводит в спецификации на устройство информацию, достаточную для того, чтобы сделать выводы, какое количество ИМС и NAND-устройств содержится в накопителе — 8 ИМС по 4 кристалла в каждом корпусе (рис. 6) [8].

Осуществим оценку времени, необходимого для получения полной копии SDD, объ-

Производитель	Plextor		
Серия	M6S		
Модельный номер	PX-128M6S	PX-256M6S	PX-512M6S
Форм-фактор	2,5 дюйма		
Интерфейс	SATA 6 Гбит/с		
Ёмкость	128 Гбайт	256 Гбайт	512 Гбайт
Конфигурация			
Микросхемы памяти: тип, интерфейс, техпроцесс, производитель	Toshiba 64 Гбит A19-нм MLC NAND		Toshiba 128 Гбит A19-нм MLC NAND
Микросхемы памяти: число / количество NAND-устройств в чипе	8/2	8/4	8/4
Контроллер	Marvell 88SS9188		
Буфер: тип, объем	DDR3L-1600, 256 Мбайт	DDR3L-1600, 512 Мбайт	DDR3L-1600, 768 Мбайт

Рис. 6. Спецификация на SSD Plextor модель PX-256M6S

ем которого составляет 256 ГБ или 244 191 МБ. Ввиду того, что в накопителе используется как чередование по плоскостям, так и по шинам (8 ИМС на четырехканальный контроллер), увеличим коэффициент интерливинга до a = 1,6, скорость считывания страницы 4 КБ 36,5 МБ/с (рис. 3, б) (есть ИМС буферной памяти объемом 512 МБ).

$$T^r = t^r_0 * N^r_f + \frac{1}{v^r_1 * n/\alpha} S^r_f = 0{,}00005 * 1 + \frac{244191}{36{,}5 * 4/1{,}6} = 2676{,}0658 \text{ с} = 44 \text{ мин } 36 \text{ с}.$$

Время полного копирования с использованием ПАК PC-3000 составило 44 мин 31 с. Разница между расчетным временем и практическим составляет 5 с.

Для наглядности исходные данные и полученные результаты сведены в таблицу (табл. 2).

Выводы

1. Имея информацию о модели целевого накопителя можно предварительно оценить потребное время на получение его полной копии с использованием модели производительности дисковой подсистемы (2).

2. Подбор исходных данных для оценки времени, необходимого для получения полной копии ТТН, является достаточно кропотливым процессом, поскольку информации, которая присутствует в спецификации, как правило, недостаточно для того, чтобы выяс-

Таблица 2

Характеристики ТТН

Характеристика\ ТТН	ADATA	Silicon Power	Plextor
Модель	CP600	CPCC	PX-256M6S
Емкость, Гбайт	64	128	256
Интерфейс	SATA	SATA	SATA
Тип контроллера, количество каналов (шин)	JMF670H 4	SM2246XT 4	Marvell 88SS9188 4
Тип памяти, количество ИМС/ NAND-устройств	MLC 4/2	MLC 2/4	MLC 8/4
Расчетное время копирования, мин	12,64	19,6	44,6
Практическое время копирования, мин	11,82	18,62	44,52
Разница между расчетным и практическим временами, мин	+0,82	+0,98	+0,08

нить, какое количество каналов поддерживает контроллер и какие конструктивные особенности имеют ИМС flash-памяти.

3. Модель (2) позволяет оценить и время, необходимое для копирования определенного объема данных. Однако при этом количество запросов на чтение из flash-памяти N^r_f в первом слагаемом будет отличным от 1. Его значение можно будет определить, разделив объем копируемых данных на объем страницы 4 КБ.

4. Как было указано вначале статьи, количество каналов, поддерживаемых контроллером SSD, может быть более, чем 4 (например, 8, 16); ширина канала также может быть отличной от 8 бит (например, 16, 32). Объем страницы в современных ИМС flash-памяти может быть отличным от стандартных 4 КБ (например, 8, 16). Наконец flash-память, выполненная по технологии MLC, в свое время вытеснившая SLC, сама вытесняется памятью, производимой по технологиям TLC и QLC (Quad-Level Cell), хранящих 3 и 4 бита соответственно. Все это необходимо учитывать при выборе коэффициентов, используемых в модели (2).

5. Так же, как и при работе с НЖМД, возможно считывание содержимого страницы с ошибками, которые не были исправлены ECC (Error-Correcting Code). Но если для НЖМД каждое повторное чтение нестабильного сектора требует полного оборота пластин жесткого диска, то для ТТН повторное чтение страницы может быть сделано практически моментально, даже если необходимо сделать несколько повторов вычитывания данных станицы до того, как декодирование ECC будет успешным (рис. 7) [9] — задержка составляет единицы микросекунд.

Таким образом, если время полного копирования НЖМД в значительной степени зависит от технического состояния механиче-

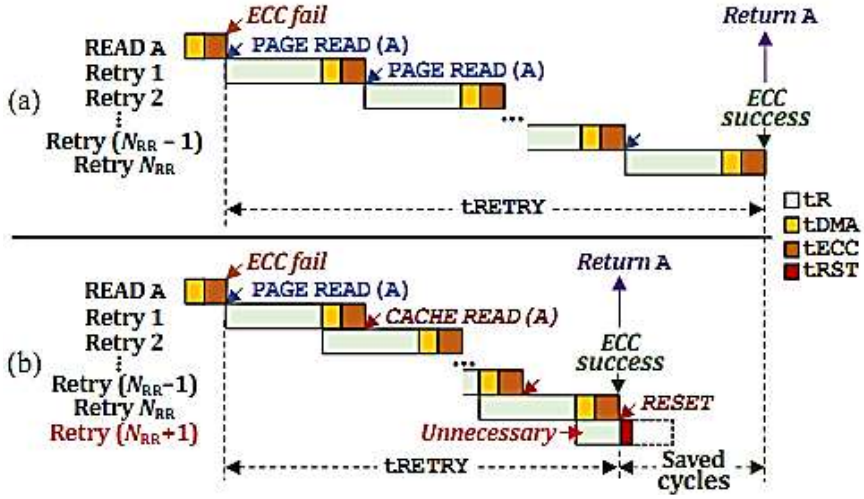

Рис. 7. Повторное вычитывание страницы и декодирование ECC

ской подсистемы накопителя (гермоблок), т. е. от наличия нестабильных блоков, то применительно к ТТН наличие нестабильных страниц не привносит сколько-нибудь значительных задержек в процесс снятия копии.

Литература

1. Жесткие диски (мировой рынок) на 2021/08/09. [Электронный ресурс] — URL: https://www.tadviser.ru/index.php (дата обращения: 04.09.2021)

2. Эволюция SSD: магия меркантологов и ее разоблачение. Longread о проникновении твердотельных накопителей в нашу жизнь. [Электронный ресурс] — URL: https://www.overclockers.ua/storage/ssd-evolution/all (дата обращения: 02.11.2021).

3. Нижник Е. И. Математическая модель нагрузки файловой системы NTFS при активном поиске дисковых данных. [Электронный ресурс] — URL: http://tekhnosfera.com/matematicheskoe-modelirovanie-proizvoditelnosti-faylovyh-sistem (дата обращения: 07.03.2021).

4. Принцип работы, 3 типа памяти и устройство SSD накопителя. [Электронный ресурс] — URL:https://www.moyo.ua/news/chto_takoe_ssd_ disk_

ustroyistvo_i_3_tipa_ pamyati_nakopitelya.html (дата обращения: 16.09.2021).

5. HDD и SSD – единство различий. [Электронный ресурс] — URL: https://overclockers.ru/lab/show/41187/HDD_i_SSD_edinstvo_razlichij (дата обращения: 16.09.2021).

6. Обзор твердотельных накопителей Corsair Force GT Series 240 Гбайт и Corsair Force 3 Series 240 Гбайт. [Электронный ресурс] — URL: https://fcenter.ru/online/hardarticles/hdd/32467/Obzor_tverdotelnyh_nakopitelej_ Corsair_Force_GT_Series_240_Gbajt_i_Corsair_Force_3_Series_240_Gbajt (дата обращения: 16.01.2022).

7. ADATA SP600 Solid State Drive [Электронный ресурс] — URL: https://www.adata.com/upload/downloadfile/120906-datasheet-SP600-EN.pdf (дата обращения: 16.01.2022).

8. Обзор SSD Plextor M6S: семь раз отрежь, потом — померь. [Электронный ресурс] — URL: https://3dnews.ru/821000/obzor-ssd-plextor-m6s-sem-raz-otreg-potom-pomer (дата обращения 16.01.2022).

9. Reducing Solid-State Drive Read Latency by Optimizing Read-Retry. [Электронный ресурс] — URL: http://people.inf.ethz.ch/omutlu/pub/Reducing-SSD-Read-Latency-by-Optimizing-Read-Retry_asplos21.pdf (дата обращения 16.01.2022).

References

1. Zhestkiye diski (mirovoy rynok) na 2021/08/09. [Elektronnyy re-surs] — URL: https://www.tadviser.ru/index.php (data obrashcheniya: 04.09.2021).

2. Evolyutsiya SSD: magiya merkantologov i yeye razoblacheniye. Longread o pro¬niknovenii tverdotel'nykh nakopiteley v nashu zhizn'. [Elektronnyy re-surs] — URL: https://www.overclockers.ua/storage/ssd-evolution/all (data ob-rashcheniya: 02.11.2021).

3. Nizhnik Ye. I. Matematicheskaya model' nagruzki faylovoy sistemy NTFS pri aktivnom poiske diskovykh dannykh. [Elektronnyy resurs] — URL: http://tekhnosfera.com/matematicheskoe-modelirovanie-proizvoditelnosti-faylovyh-sistem (data obrashcheniya: 07.03.2021).

4. Printsip raboty, 3 tipa pamyati i ustroystvo SSD nakopitelya. [Elektronnyy resurs] — URL:https://www.moyo.ua/news/chto_takoe_ssd_ disk_ ustroyistvo_i_3_tipa_ pamyati_nakopitelya.html (data obrashcheniya: 16.09.2021).

5. HDD i SSD – yedinstvo razlichiy. [Elektronnyy resurs] — URL: https://overclockers.ru/lab/show/41187/HDD_i_SSD_edinstvo_razlichij (data obrashcheniya: 16.09.2021).

6. Obzor tverdotel'nykh nakopiteley Corsair Force GT Series 240 Gbayt i Corsair Force 3 Series 240 Gbayt. [Elektronnyy resurs] — URL: https://fcenter.ru/online/hardarticles/hdd/32467/Obzor_tverdotelnyh_nakopitelej_ Corsair_Force_GT_Series_240_Gbajt_i_Corsair_Force_3_Series_240_Gbajt (data obrashcheniya: 16.01.2022).

7. ADATA SP600 Solid State Drive [Elektronnyy resurs] — URL: https://www.adata.com/upload/downloadfile/120906-datasheet-SP600-EN.pdf (data obrashcheniya: 16.01.2022).

8. Obzor SSD Plextor M6S: sem' raz otrezh', potom — pomer'. [Elek-tronnyy resurs] — URL: https://3dnews.ru/821000/obzor-ssd-plextor-m6s-sem-raz-otreg-potom-pomer (data obrashcheniya 16.01.2022).

9. Reducing Solid-State Drive Read Latency by Optimizing Read-Retry. Available at: http://people.inf.ethz.ch/omutlu/pub/Reducing-SSD-Read-Latency-by-Optimizing-Read-Retry_asplos21.pdf (accessed 16 January 2022).

ШАМОНИН Евгений Дмитриевич, кандидат технических наук, доцент кафедры алгебры и фундаментальной информатики, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, Уральский федеральный округ, Свердловская область, Екатеринбург, ул. Мира, 19. E-mail: shamonined@mail.ru

SHAMONIN Evgeniy Dmitrievich, Candidate of Technical Sciences, Associate Professor of Algebra and Fundamental Informatics, Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Ural Federal District, Sverdlovsk Region, Yekaterinburg, 19 Mira St. E-mail: shamonined@mail.ru

УДК 004.056.53

Вестник УрФО № 3(45) / 2022, с. 34–46

Дорофеев К.А.

DOI: 10.14529/secur220304

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ БИОМЕТРИЧЕСКИХ СИСТЕМ РАСПОЗНАВАНИЯ ЛИЦ

В статье рассматриваются современные подходы к решению задачи распознавания лиц, построению биометрических систем идентификации по лицам, а также основные проблемы и уязвимости подобных систем. Особое внимание уделено вопросам безопасности, а также проблемам, связанным с атаками на такие системы: использование подделок, распечатанных фотографий и масок, визуализированных и сгенерированных двумерных и трёхмерных изображений и видео лиц. Рассмотрены современные подходы к решению таких проблем, к противодействию подобным атакам. Также рассмотрены правовые аспекты, приведены законы, регулирующие обработку биометрических данных граждан РФ, и оценены риски атак на биометрические системы.

Основная задача исследования – провести анализ уязвимостей биометрических систем распознавания лиц и указать основные способы устранения этих уязвимостей.

Ключевые слова: *информационная безопасность, биометрия, распознавание лиц, нейронные сети, глубокое обучение, идентификация, аутентификация, правовое регулирование биометрических данных.*

Dorofeev K. A.

COMPARATIVE ANALYSIS OF VULNERABILITIES IN BIOMETRIC FACE RECOGNITION SYSTEMS

The article discusses current approaches to solving the problem of face recognition, the construction of biometric face identification systems, as well as the main problems and vulnerabilities of such systems. Particular attention is paid to security issues and problems associated with attacks on such systems: the use of fakes, printed photos and masks, visualized

and generated two- and three-dimensional images and video of faces. The modern approaches to solving such problems, to counteract such attacks are considered. It also examined the legal aspects and laws regulating the processing of biometric data of Russian federation and assesses the risks of attacks on biometric systems.

The main task of the research is to analyze the vulnerabilities of biometric face recognition systems and indicate the main ways of eliminating these vulnerabilities.

Keywords: *Information security, biometrics, face recognition, neural networks, deep learning, identification, face authentication, legal regulation of biometric data.*

1. Введение

Одной из крайне актуальных задач информационной безопасности является разработка надёжных систем биометрической идентификации, в частности систем, основанных на распознавании лиц. Обширность применения подобного рода систем тяжело переоценить. Зачастую такие системы являются частью больших, масштабных платформ, систем и решений, например, таких, как проектирование умных магазинов без касс. Существует концепция построения умных городов, где одной из важнейших частей является система распознавания лиц [1,2]. Также интерес к надёжным системам распознавания обусловлен высокими финансовыми потерями от несанкционированного доступа, от действий киберпреступников по всему миру.

Сильным фактором развития отрасли стало распространение коронавирусной инфекции (COVID). С одной стороны, общество было заинтересовано в выполнении рекомендательных мер всемирной организации здравоохранения, таких, как социальная дистанция, ношение защитных масок – и здесь помогали системы распознавания. С другой стороны, отрасль столкнулась с актуальными проблемами – распознавание лиц в масках, сильно перекрытых лиц. Это привело к появлению новых подходов, новых архитектур и методов [3,4].

Достигнуты значительные успехи в решении задачи распознавания человека по двумерному и трехмерному изображению лица благодаря применению нейронных сетей глубокого обучения с тремя и более слоями [5-13], которые объединяют в себе как выбор и расчет признаков, так и классификацию. Точность методов глубокого обучения при большом количестве слоев (от 10 до 22) и при очень большой обучающей выборке (миллионы образцов) на некоторых известных базах данных, таких как Labelled Faces in the Wild [14] (LFW) превысила точность распознавания человеком и достигла 99.6% [10-12].

Идентификация человека по лицу – одна из наиболее важных современных задач компьютерного зрения и робототехники, как с теоретической, так и с практической точек зрения. К сожалению, существующие в настоящее время системы автоматического распознавания человека по лицу в неконтролируемых условиях до сих пор имеют достаточно большую ошибку.

2. Двумерные системы распознавания

Самые ранние исследования в области распознавания лиц можно отнести к 1960-м годам [15]. Очевидно, что большинство таких систем представляли из себя реализации классических алгоритмов компьютерного зрения, обработки и поиска ключевых точек в двумерном изображении. С течением времени разрабатывались новые алгоритмы, системы распознавания лиц усложнялись и позволяли решать всё более сложные задачи [16-19].

Большинство современных систем распознавания лиц можно представить, как совокупность основных модулей (этапов обработки кадра):

- обнаружение лица;
- предобработка кадра (фильтрация, выравнивание и пр.);
- извлечение признаков, составление n-мерного шаблона;
- сопоставление или поиск в базе;
- решение дополнительных (вспомогательных) задач распознавания (определение пола, возраста, эмоций, наличие улыбки, наличие маски и пр.).

Каждый из этапов может быть представлен широким диапазоном направлений, конкретных решений и технологий.

Основные подходы к обнаружению лица в кадре:

- применение каскадов классификаторов [20];
- использование гистограмм ориентированных градиентов [21];
- применение локальных бинарных патернов [22];

• использование нейронных сетей [23-30].

Задачи, которые решают при составлении шаблона – извлечение ключевых признаков и классификация. Классические алгоритмы извлечения признаков сосредоточены на обработке постоянных черт лица, например, таких, как брови, глаза, нос, рот. Наиболее качественные дескрипторы: LBP [31], Gabor [32], SIFT [33], HOG [34]. Основная задача классификатора – получить относительные расстояния между чертами лица. К широко используемым в классификаторах алгоритмам можно отнести: метод опорных векторов, метод k – ближайших соседей, случайный лес [35-37]. Отдельно стоит отметить применение нейронных сетей различной архитектуры: свёрточные сети, множественные свёрточные сети, глубокие нейронные сети [38-45].

Остро стоит вопрос с распознаванием поддельных лиц, распечатанных фотографий и масок, визуализированных, а также сгенерированных (например нейронными сетями) двумерных изображений лиц (рис 1).

Современные возможности нейронных

Рис. 1. Примеры атак с использованием распечатанной фотографии и с помощью визуализации изображения на экране смартфона

сетей, в частности глубоких нейронных сетей, не всегда используются во благо. Иногда даже человек не способен отличить настоящую фотографию или видео от сгенерированных, с помощью современных методик синтеза (deepfake) (рис 2).

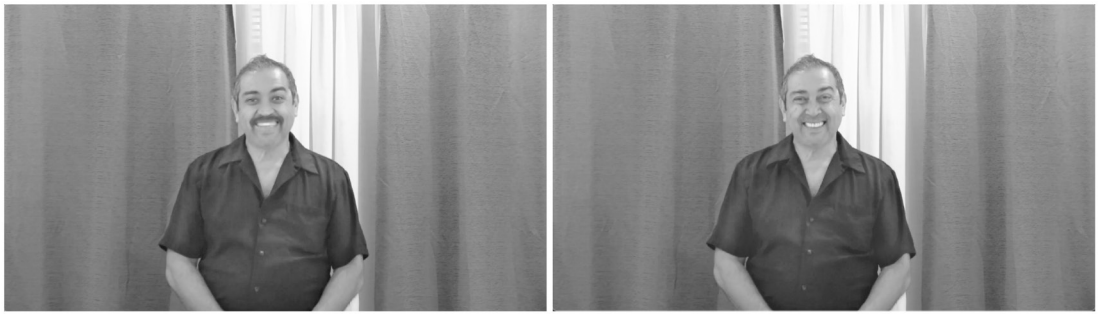

Рис. 2. Настоящее и сгенерированное с помощью deepfake изображения

Традиционные программные методы обнаружения атак с “презентацией” лица основывались на вычислениях параметров, описывающих признаки движения (моргание глаз, движение губ), текстуру лица и качество изображения [46-48]. К сожалению, точность работы подобных методов сильно зависит от тонкой настройки, от человеческого опыта

при извлечении подобного рода информации. Иногда спроектированные пространства признаков не в состоянии отличить подделку от артефактов лица. Именно поэтому внимание сообщества исследователей привлекли нейронные сети, в частности свёрточные сети и сети глубокого обучения [49].

Но несмотря на то, что были достигнуты серьёзные результаты, даже самые современные методы обнаружения атак с "презентацией" лица на основе глубокого обучения показывают неудовлетворительную точность обобщения при подаче изображений, с неизвестными заранее условиями, при работе с группами изображений, полностью отсутствующими в обучающих выборках. Таких примеров достаточно много: этнические и национальные особенности пользователей системы, использование различных датчиков, с которых приходят данные (изображения), отличающееся разрешение изображений/видео, условия окружающей среды (освещение, яркость, контрастность), расстояние между лицом и датчиком. Исследователи стараются решить возникающие проблемы обобщения, можно отметить основные тенденции – использование перекрёстных баз данных [50], применение специальных протоколов перекрёстного обучения и тестирования [51].

Несмотря на ограниченность объёмов обучающих данных есть попытки преодоления подобного рода ограничений:

• глубокое обучение для выявления внутренних различий между реальными и поддельными лицами [52];

• аугментация и искусственный синтез данных [53];

• вспомогательный надзор [53,54];

• адаптация предметной области [55];

• непрерывное обнаружение и обучение на новых типах атак [56].

Yang и другие [53] предложили метод искусственного синтеза данных для имитации спуфинговых атак на основе цифровых носителей, что привело к возможности увеличения объёмов обучающих выборок. Liu и другие [58] предложили увеличить обобщающую способность методов обнаружения "презентации" лица за счёт использования пространственного и временного вспомогательного наблюдения.

Среди последних, пожалуй, самых актуальных работ и исследований стоит отметить [57], авторы которой предложили способы решения некоторых проблем, в частности временной избыточности и межкадровых сдвигов в изображениях, а также представили метод выборки временной последовательности для кодирования и компактного представления видеопотока (рис. 3).

Эффективность такого подхода авторы

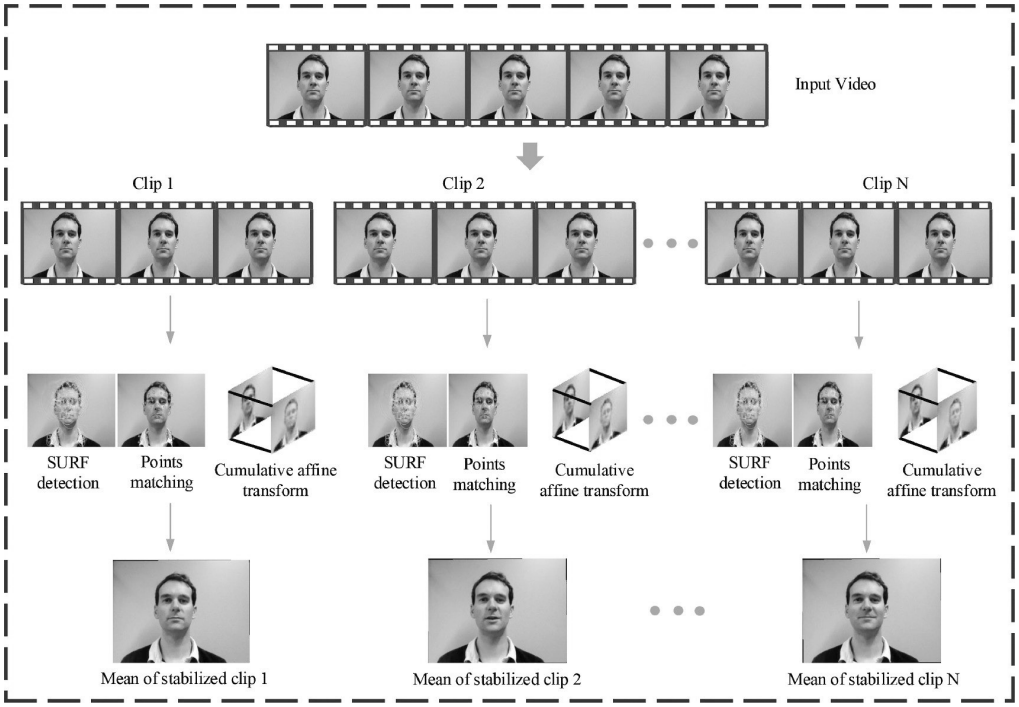

Рис. 3. Метод выборки временной последовательности

продемонстрировали с помощью использования протоколов оценки перекрёстных испытаний базы данных OULU-NPU [51] и нескольких широко используемых конфигураций перекрёстных баз данных. Отдельно стоит отметить, что авторы выложили в открытый доступ исходный код проекта.

Хотя двумерные системы распознавания и достигли серьёзных успехов, на точность распознавания таких систем до сих пор влияют многие факторы и именно поэтому многие исследователи обратились к построению трёхмерных систем распознавания лиц из-за их потенциальных возможностей преодоления присущих 2D систем ограничений и недостатков.

3. Трёхмерные системы распознавания

Для достижения высокой точности и надежности идентификации человека на динамических сценах в реальных условиях использование алгоритмов трехмерного распознавания лиц является перспективным, так как алгоритмы являются инвариантными к изменению освещения, а идентификация личности может быть проведена с разных углов обзора. Алгоритмы трехмерного распознавания используют информацию о форме лица для идентификации отличительных признаков, таких как контур глазниц, носа и подбородка, рис. 4. Однако деформации формы лица при мимических экспрессиях ухудшают качество распознавания [59]. Трехмерное изображение человеческого лица является гораздо более информативным, чем соответствующая двумерная проекция. Из-за сложной топологии формы лица при его динамическом трехмерном описании часто используется деформируемая модель лица [60-63]. С помощью данной модели можно параметрически описать мимические экспрессии человека, и, как следствие, улучшить качество идентификации человека.

Качество алгоритмов трехмерного рас-

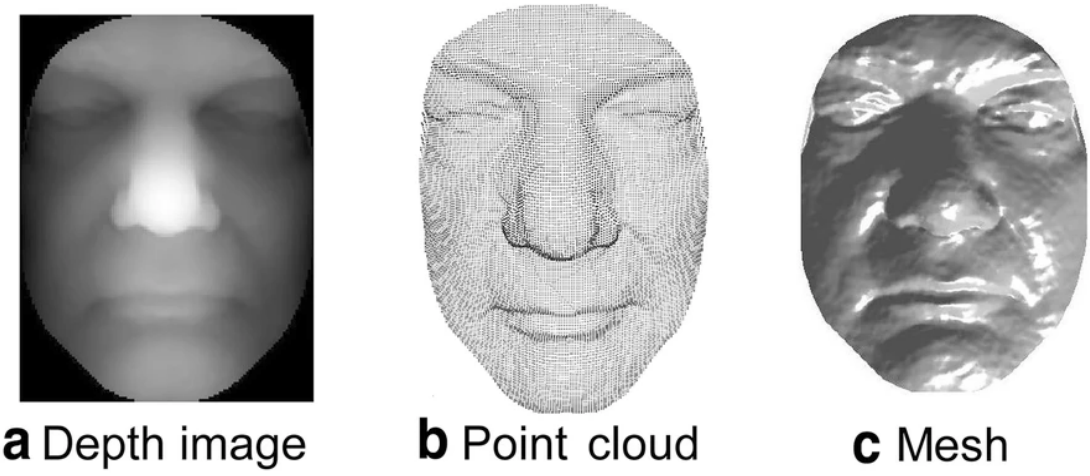

Рис. 4. Пример трёхмерной модели изображения лица

познавания напрямую зависит от точности построения трехмерной модели формы лица человека с помощью регистрации в трехмерном пространстве облаков точек, получаемых от датчиков глубины [64, 65]. Традиционный алгоритм регистрации решает вариационную задачу поиска оптимального геометрического (ортогонального или аффинного) преобразования, который наилучшим образом совмещает два облака точек с заданным соответствием между точками [66]. Выбор вида функционала в задаче оптимизации приводит к различным методам регистрации облаков точек. Наиболее используемыми являются поиск соответствия между парой облаков – точка-точка (point-to-point) и поиск соответствия – точка-плоскость (point-to-plane). Для класса ортогональных преобразований для задачи точка-точка решение в явном виде представлено в классических работах Хорна [67, 68]. Точное решение задачи точка-точка для случая произвольного аффинного преобразования приведено в работе [69]. Вариационная задача точка-плоскость в классе ортогональных преобразований решается с применением итерационного алгоритма Левенберга-Марквардта или методом линеаризации для малых углов [70]. Для вариационной задачи точка-плоскость в классе аффинных преобразований найдено точное

решение [71]. В работе [72] получено приближенное решение задачи точка-плоскость в классе ортогональных преобразований.

Стоит отметить, что метод точка-плоскость является более робастным к шуму датчиков, но для этого метода для класса ортогональных преобразований решение задачи в явном виде пока не найдено. Это усложняет применение метода в задачах, где требуется производить регистрацию в масштабе реального времени. В работе [73] представлен алгоритм динамической регистрации облаков точек, используемый для поиска соответствия между деформируемыми поверхностями. Метод предусматривает разбиение поверхностей на участки, каждый из которых обрабатывается отдельно, а способ объединения результатов регистрации основан на минимизации функционала.

Известно, что использование трехмерной карты окружающего пространства [74,75] существенно улучшает качество распознавания и локализации субъектов на динамических, контекстуально сложных сценах, особенно при частичном или полном закрытии субъектов посторонними предметами. Несмотря на то, что качество карты глубины, получаемое от RGB-D камер, таких, например, как Kinect, в целом хорошее, существуют проблемы с выходной информацией. Так в выходных данных образуются области неопределенности из-за того, что структурированный свет излучения после отражения не попадает на камеру, разрешающая способность измерения глубины сцены падает по квадратичному закону с увеличением глубины сцены [76], а также из-за того, что быстрое движение камеры приводит к потере данных.

В качестве предобработки данных применяются как двумерные, так и трехмерные подходы к задаче регуляризации полной вариации для устранения шума, возникающего при получении трехмерных данных с помощью датчиков глубины. Одним из наиболее эффективных методов фильтрации шума является применение регуляризации полной вариации [77]. В работе [78] описан способ решения задачи регуляризации анизотропной полной вариации в многомерном случае.

Для повышения точности распознавания лиц с использованием векторов признаков (дескрипторов) для предварительного обучения сверточных нейронных сетей на внешних наборах данных применяются различные методы регуляризации. Например, для того, чтобы дескрипторы каждого класса образовывали гиперсферу в многомерном пространстве, был предложен метод center loss [79]. Дескрипторы FaceNet [80] обучаются с помощью минимизации специальной функции потерь (triplet loss), которая приводит к тому, что расстояния между дескрипторами одного человека становятся меньше расстояний между дескрипторами различных людей. Кроме того, в последнее время появились функции потерь, основанные на максимизации зазора между углами, образованными извлекаемыми векторами признаками различных классов, такие, как ArcFace [81]. В то же время на практике замечено, что наиболее точные результаты распознавания лиц получаются с помощью дескрипторов CNC, обученных с помощью оптимизации традиционной функции потерь (softmax loss), если использовать высококачественную большую внешнюю базу данных лиц, такую как VGGFace-2 [82].

Получена количественная оценка точности модели, устойчивости к внешним искажающим факторам, таким как неравномерное и слабое освещение, а также к подвижности человека [83,84]. Для нежесткой математической модели лица, то есть когда лицо подвижно, и его форма может деформироваться, предложен метод построения плотной трехмерной математической модели формы лица по набору изображений и карт глубины, снятых с нескольких RGB-D камер, а также реализована система объединения данных с нескольких камер с использованием модифицированного алгоритма совмещения ICP по динамическому набору облаков точек [85].

При работе с трёхмерными моделями лиц также крайне остро стоит вопрос с распознаванием поддельных лиц, распечатанных трёхмерных масок, визуализированных изображений и видео [88-90], рис. 5. Примеры атак приведены на рис. 6. Разработанные способы обнаружения подделок можно разделить на две основные категории: обработка видимого диапазона, обработка инфракрасного диапазона [87].

Наиболее используемыми характерными чертами лица при обработке видимого диапазона являются текстура [88-90], мимика [91]. Например, совместное использование нескольких дескрипторов локальных двоичных шаблонов (LBP) позволяет обнаружить отличия текстуры между реальным лицом и трёхмерной маской достаточно эффективно

Рис. 5. Примеры напечатанных на трёхмерном принтере масок для лиц

Рис. 6. Примеры атак

[92]. Существуют методы, основанные на применении дистанционной фотоплетизмографии с использованием различных сигналов [93]. Также применяется и анализ поляризации света на коже лица [94]. Стоит отметить, что крупным потенциальным недостатком большинства существующих методов обнаружения подделок с помощью анализа видимого диапазона является чувствительность к окружению (к сцене или фону), к освещению и выражению лица.

В дополнение к видимому спектру многие исследователи рассматривают и инфракрасный спектр. Например, Wang объединил видимый и ближний инфракрасный диапазоны спектра для моделирования характеристик градиента при обнаружении масок из поливинилхлорида, силиконовых масок и фотографий лиц [95]. Такой подход доказал, что разница отражательной способности реальной кожи лица и различных подделок может быть важным фактором при принятии решения. Известны попытки применения глубоких нейронных сетей, а также свёрточных нейронных сетей для анализа мультиспектральных изображений [96-99]. Однако пока рано судить об успешности построенных моделей из-за недостаточного объёма обучающих данных.

Применение трёхмерных моделей при построении современных надёжных систем распознавания является актуальным направлением. Проводятся международные мастер-классы и соревнования по распознаванию подделок, масок [86].

4. Законодательство и правовое регулирование в области обработки и применения биометрических данных

Ключевая законодательная норма, регулирующая правовой режим биометрических данных в Российской Федерации – статья 11 Закона о персональных данных. Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» призван образовать фундамент для Единой биометрической системы, регламентировать связанные с ней процедуры (такие, например, как сбор биометрических данных) и области ее применения – пока что главным образом в финансовых сферах наподобие банковской деятельности. Единая биометрическая система – совместный проект Банка России и «Ро-

стелекома», направленный на сбор биометрической информации и её использование для идентификации пользователей финансовых услуг. Платформа была разработана по инициативе Минкомсвязи и Центрального банка, разработчик и оператор ЕБС — «Ростелеком». В конце 2021 года приобрела статус государственного информационного ресурса.

К основным стандартам отрасли можно отнести: ГОСТ Р 52633.0-2006 (Защита информации, техника защиты информации, требования к средствам высоконадежной биометрической аутентификации), ГОСТ Р 52633.4-2011 (Защита информации, техника защиты информации, интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа), ГОСТ Р 54412-2019 (Информационные технологии, биометрия, общие положения и примеры применения), ГОСТ Р 58624.3-2019 (Информационные технологии, биометрия, обнаружение атаки на биометрическое предъявление).

Самый серьёзный вопрос, возникающий при обсуждении биометрии – риск утечки биометрических данных. К сожалению, утечки происходят из самых разных баз данных, и не так важно, как они защищены от взлома снаружи, поскольку часто это делается изнутри. Компрометация биометрических данных — это самое страшное, что может произойти. Если человек доверил системе свои биометрические данные, и эта система не оправдала его доверия, то у человека в цифровом будущем сломана жизнь. Можно поменять пин-код на карточке, можно поменять паспорт, все что угодно, можно поменять фамилию, но поменять биометрические данные практически невозможно. Задача противодействия подобного рода утечкам является достаточно сложной, объёмной, многофакторной. Один из важнейших факторов - способ представления и хранения биометрических образцов. Обычно в системах хранятся «отпечатки» биометрических данных, то есть наборы зашифрованных данных. Процесс восстановления исходной биометрической информации является вычислительно сложным, зачастую практически невыполнимым.

Многие эксперты отмечают, что, к сожалению, правовое регулирование биометрии в России находится не в идеальном состоянии. Однако процесс формирования единого, структурированного подхода к вопросу регулирования биометрических данных РФ все же уже начался, многие законодательные акты, касающиеся биометрии, сейчас находятся на стадии разработки и конкретизации. Например, 6 апреля текущего года в Государственную Думу был внесён законопроект «О внесении изменений в Федеральный закон о персональных данных, предлагающий регулирование обработки биометрических данных».

5. Выводы

В компьютерном зрении и конкретно в распознавании лиц до сих пор существует много проблем и задач, которые ещё предстоит решить. Использование как двумерных, так и трёхмерных систем распознавания лиц сопряжено с известными проблемами и ошибками. Часть исследователей сосредоточила силы на применении многокомпонентных, гибридных, мультимодальных системах [100-102]. Среди основных направлений, трендов и задач для будущих исследований в отрасли можно указать следующее:

- повышение точности распознавания в сложных условиях;
- построение надёжных алгоритмов и систем обнаружения распечатанных, поддельных и сгенерированных изображений и видео;
- упрощение интерфейсной части подобного рода систем, повышение простоты развёртывания, использования и обслуживания таких систем;
- решение проблемы предвзятости и повышение релевантности систем, расширение обучающих баз в контексте использования изображений людей из различных рас и национальностей, разного цвета кожи и других особенностей;
- распознавание лиц в маске, сильно перекрытых лиц;
- решение и обсуждение этических проблем биометрии, влияние систем распознавания на личную жизнь;
- внедрение систем распознавания в повседневную жизнь, в узкие отрасли: в ритейл системы, в системы оплаты, использование распознавания при мониторинге водителя, управляющего транспортным средством и прочее.

Литература / References

1. G. Praveen, J. Dakala, Face Recognition: Challenges and Issues in Smart City/Environments, Conference: 2020 International Conference on Communication Systems and Networks, pp. 791–793, 2020.

2. M. Bansal, D. Sharma, Facial Recognition System for Security Resolutions in Smart City, International Journal of Advanced Research in Engineering and Technology, 11(10), pp. 146–151, 2020.

3. G. Jeevan, G. Zacharias, M. Nair, J. Rajan, "An empirical study of the impact of masks on face recognition", Pattern Recognition, pp. 108308, 2022.

4. N. Ullah, A. Javed, M. Ghazanfar, A. Alsufyani, S. Bourouis, "A novel DeepMaskNet model for face mask detection and masked facial recognition", Journal of King Saud University – Computer and Information Sciences, 2022.

5. I. Goodfellow, Y. Bengio, A. Courville, A. Deep learning. Cambridge, MA: MIT Press (2016).

6. Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, M.S. Lew, "Deep learning for visual understanding: A review," Neurocomputing, 187, 27–48 (2016).

7. R. He, X. Zhang, S. Ren, J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," Proc. IEEE International Conference on Computer Vision, pp. 1026–1034 (2015).

8. Y. Taigman, M. Yang, M. Ranzato, L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 1701–1708 (2014).

9. Y. Sun, X. Wang, X. Tang, X., "Deeply learned face representations are sparse, selective, and robust," Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 2892–2900 (2015).

10. Y. Sun, D. Liang, X. Wang, X. Tang, X., "Deepid3: Face recognition with very deep neural networks," arXiv 1502.00873.

11. E. Zhou, Z. Cao, Q. Yin, "Naive-deep face recognition: Touching the limit of LFW benchmark or not?" arXiv 1501.04690.

12. F. Schroff, D. Kalenichenko, J. Philbin, J.,"Facenet: A unified embedding for face recognition and clustering," Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 815–823 (2015).

13. W. Rawat, Z. Wang, "Deep convolutional neural networks for image classification: A comprehensive review," Neural Computation, June 2017. DOI: 10.1162/NECO_a_00990

14. G.B. Huang, M. Ramesh, T. Berg, E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," Technical Report 07-49. Amherst: University of Massachusetts.

15. W. W., Bledsoe, "The Model Method in Facial Recognition," Technical Report, PRI 15, Panoramic Research, Inc., Palo Alto, California, 1964.

16. Pentland MT (1991) Face recognition using eigenfaces. Computer vision and pattern recognition. pp. 586–591.

17. Belhumeur PN, Hespanha DJKJP (1997) Eigenfaces vs. fisherfaces: recognition using class specific linear projection. Trans Pattern Anal Mach Intell 19:711–720.

18. Frey BJ, Colmenarez TSH A (1998) Mixtures of local linear subspaces for face recognition. In: Computer vision and pattern recognition.

19. Moghaddam B, Jebara APT (2000) Bayesian face recognition. Pattern Recognit 33:1771–1782.

20. Viola, P.; Jones, M.J. Robust Real-Time Face Detection. Int. J. Comput. Vis. 2004, 57, 137–154.

21. Dalal, N.; Triggs, B. Histograms of Oriented Gradients for Human Detection. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Diego, CA, USA, 20–25 June 2005.

22. Ahonen, T.; Hadid, A.; Pietikainen, M. Face Description with Local Binary Patterns: Application to Face Recognition. IEEE Trans. Pattern Anal. Mach. Intell. 2006, 28, 2037–2041.

23. Deng, J.; Guo, J.; Ververas, E.; Kotsia, I.; Zafeiriou, S. RetinaFace: Single-Shot Multi-Level Face Localisation in the Wild. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA, 13–19 June 2020; pp. 5202–5211.

24. Zhang, K.; Zhang, Z.; Li, Z.; Qiao, Y. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. IEEE Signal Process. Lett. 2016, 23, 1499–1503.

25. Jiang, H.; Learned-Miller, E. Face Detection with the Faster R-CNN. In Proceedings of the 12th IEEE International Conference on Automatic Face & Gesture Recognition, Washington, DC, USA, 30 May–3 June 2017.

26. Tang, X.; Du, D.K.; He, Z.; Liu, J. PyramidBox: A Context-Assisted Single Shot Face Detector. In Computer Vision—ECCV 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 812–828.

27. Zhang, S.; Chi, C.; Lei, Z.; Li, S.Z. RefineFace: Refinement Neural Network for High Performance Face Detection. arXiv 2019, arXiv:1909.04376v1.

28. Jang, Y.; Gunes, H.; Patras, I. Registration-free Face-SSD: Single shot analysis of smiles, facial attributes, and affect in the wild. Comput. Vis. Image Underst. 2019, 182, 17–29.

29. Yashunin, D.; Baydasov, T.; Vlasov, R. MaskFace: Multi-task face and landmark detector. arXiv 2020, arXiv:2005.09412v1.

30. Chen, W.; Huang, H.; Peng, S.; Zhou, C.; Zhang, C. YOLO-face: A real-time face detector. Vis. Comput. 2020, 37, 805–813.

31. Yang, B.; Chen, S. A comparative study on local binary pattern (LBP) based face recognition: LBP histogram versus LBP image. Neurocomputing 2013, 120, 365–379.

32. Vinay, A.; Shekhar, V.; Murthy, K.B.; Natarajan, S. Face Recognition Using Gabor Wavelet Features with PCA and KPCA—A Comparative Study. Procedia Comput. Sci. 2015, 57, 650–659.

33. Bakhshi, Y.; Kaur, S.; Verma, P. Face Recognition using SIFT, SURF and PCA for Invariant Faces. Int. J. Eng. Trends Technol. 2016, 34, 39–42.

34. Dadi, H.S.; Pillutla, G.K.M. Improved Face Recognition Rate Using HOG Features and SVM Classifier. IOSR J. Electron. Commun. Eng. 2016, 11, 34–44.

35. Kremic, E.; Subasi, A. Performance of random forest and SVM in face recognition. Int. Arab J. Inf. Technol. 2016, 13, 287–293.

36. Dadi, H.S.; Pillutla, G.K.M.; Makkena, M.L. Face Recognition and Human Tracking Using GMM, HOG and SVM in Surveillance Videos. Ann. Data Sci. 2017, 5, 157–179.

37. Tee, T.X.; Khoo, H.K. Facial Recognition Using Enhanced Facial Features K-Nearest Neighbor (k-NN) for Attendance System. In Proceedings of the 2nd International Conference on Information Technology and Computer Communications, Kuala Lumpur, Malaysia, 12–14 August 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 14–18.

38. Huang, G.B.; Ramesh, M.; Berg, T.; Learned-Miller, E. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments; Technical Report 07-49; University of Massachusetts: Amherst, MA, USA, 2007.

39. Schroff, F.; Kalenichenko, D.; Philbin, J. FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 7–12 June 2015.

40. Sun, Y.; Liang, D.; Wang, X.; Tang, X. DeepID3: Face Recognition with Very Deep Neural Networks. arXiv 2015, arXiv:1502.00873v1.

41. Ranjan, R.; Castillo, C.D.; Chellappa, R. L2-constrained Softmax Loss for Discriminative Face Verification. arXiv 2017, arXiv:1703.09507.

42. Wang, H.; Wang, Y.; Zhou, Z.; Ji, X.; Gong, D.; Zhou, J.; Li, Z.; Liu, W. CosFace: Large Margin Cosine Loss for Deep Face Recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018.

43. Zheng, Y.; Pal, D.K.; Savvides, M. Ring loss: Convex Feature Normalization for Face Recognition. arXiv 2018, arXiv:1803.00130.

44. Deng, J.; Guo, J.; Xue, N.; Zafeiriou, S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019.

45. Alghaili, M.; Li, Z.; Ali, H.A.R. FaceFilter: Face Identification with Deep Learning and Filter Algorithm. Sci. Program. 2020, 2020, 7846264.

46. K. Kollreider, H. Fronthaler, M.I. Faraj, J. Bigun Real-time face detection and motion analysis with application in liveness assessment IEEE Trans. Inf. Forensics Secur., 2 (3) (2007), pp. 548-558.

47. Z. Boulkenafet, J. Komulainen, A. Hadid Face spoofing detection using colour texture analysis IEEE Trans. Inf. Forensics Secur., 11 (8) (2016), pp. 1818–1830.

48. D. Wen, H. Han, A.K. Jain Face spoof detection with image distortion analysis IEEE Trans. Inf. Forensics Secur., 10 (4) (2015), pp. 746–761.

49. Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, G. Zhao, Deep learning for face anti-spoofing: a survey, arXiv preprint: 2106.14948(2021b).

50. T. de Freitas Pereira, A. Anjos, J.M. De Martino, S. Marcel Can face anti-spoofing countermeasures work in a real world scenario? International Conference on Biometrics (ICB) (2013).

51. Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, A. Hadid OULU-NPU: a mobile face presentation attack database with real-world variations IEEE International Conference on Automatic Face & Gesture Recognition (FG) (2017), pp. 612–618.

52. A. Jourabloo, Y. Liu, X. Liu Face de-spoofing: anti-spoofing via noise modeling European Conference on Computer Vision (ECCV) (2018), pp. 290–306.

53. X. Yang, W. Luo, L. Bao, Y. Gao, D. Gong, S. Zheng, Z. Li, W. Liu Face anti-spoofing: model matters, so does data IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019), pp. 3507–3516.

54. Z. Yu, J. Wan, Y. Qin, X. Li, S.Z. Li, G. Zhao NAS-FAS: static-dynamic central difference network search for face anti-spoofing IEEE Trans. Pattern Anal. Mach. Intell., 43 (9) (2021), pp. 3005–3023.

55. A. Mohammadi, S. Bhattacharjee, S. Marcel Domain adaptation for generalization of face presentation attack detection in mobile settengs with minimal information IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020).

56. M. Rostami, L. Spinoulas, M. Hussein, J. Mathai, W. Abd-Almageed Detection and continual learning of novel face presentation attacks International Conference on Computer Vision (ICCV) (2021).

57. U. Muhammad, Z. Yu, J. Komulainen, Self-supervised 2D face presentation attack detection via temporal sequence sampling Pattern Recognition Letters, Volume 156, April 2022, Pages 15–22.

58. Y. Liu, A. Jourabloo, X. Liu Learning deep models for face anti-spoofing: Binary or auxiliary supervision IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2018), pp. 389–398.

59. G. Rajamanoharan, S. Zafeiriou, M. Pantic, L. Yin, "Static and dynamic 3D facial expression recognition: A comprehensive survey," Image Vis. Comput., Vol. 30 (10), pp. 683–697 (2012).

60. G. Pan, X. Zhang, Y. Wang, Z. Hu, X. Zheng, Z. Wu, "Establishing point correspondence of 3D faces via sparse facial deformable model," IEEE Trans. Image Process., Vol. 22 (11), pp. 4170–4181 (2013).

61. C. Cao, Q. Hou, K. Zhou, "Displaced dynamic expression regression for real-time facial tracking and animation," ACM Trans. Graph., Vol. 33 (4), pp. 43:1–43:10 (2014).

62. X. Zhang, L. Yin, J.F. Cohn, S. Canavan, M. Reale, A. Horowitz, P. Liu, J.M. Girard, "BP4D Spontaneous: a high-resolution spontaneous 3D dynamic facial expression database," Image Vis. Comput., Vol. 32 (10), pp. 692–706 (2014).

63. X. Li, Q. Ruan, Y. Jin, G. An, R. Zhao, "Fully automatic 3D facial expression recognition using polytypic multi-block local binary patterns," Signal Processing, Vol. 108, pp. 297–308 (2015).

64. G. Tam, Z.-Q. Cheng, Y.-K. Lai, F. Langbein, Y. Liu, D. Marshall, R. Martin, X.-F. Sun, P. Rosin, "Registration of 3D point clouds and meshes: A survey from rigid to nonrigid," IEEE Trans. Vis. Comput. Graph., Vol. 19 (7), pp. 1199–1217 (2013).

65. S. Cheng, I. Marras, S. Zafeiriou, M. Pantic, "Statistical non-rigid ICP algorithm and its application to 3D face alignment," Image Vis. Comput., Vol. 58, pp. 3–12 (2017).

66. P. Besl and N. McKay, "A method for registration of 3-D shapes," IEEE Transactions of Pattern Analysis and Machine Intelligence, Vol. 14 (2), pp. 239–256 (1992).

67. B. Horn, "Closed-Form Solution of Absolute Orientation Using Unit Quaternions," Journal of the Optical Society of America A, Vol. 4(4), pp. 629–642 (1987).

68. B. Horn B., H. Hilden and S. Negahdaripour S., "Closed-form Solution of Absolute Orientation Using Orthonormal Matrices," Journal of the Optical Society of America A, Vol. 5 (7), pp. 1127–1135 (1988).

69. S. Du, N. Zheng, S. Ying and J. Liu, "Affine iterative closest point algorithm for point set registration," Pattern Recognition Letters, Vol. 31, pp. 791–799 (2010).

70. K.L. Low, "Linear least-squares optimization for point-to-plane ICP surface registration," Technical Report TR04-004, Department of Computer Science, University of North Carolina at Chapel Hill, 2004.

71. Makovetskii A., Voronin S., Kober V. and Tihonkih D., "An efficient point-to-plane registration algorithm for affine transformations," Proc. SPIE 10396, Applications of Digital Image Processing XL, pp. 103962J (2017).

72. K. Khoshelham, "Closed-form solutions for estimating a rigid motion from plane correspondences extracted from point clouds," ISPRS Journal of Photogrammetry and Remote Sensing, Vol. 114, pp. 78–91 (2016).

73. S. Cheng, I. Marras and S. Zafeiriou, "Active nonrigid ICP algorithm," Proc. 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition, pp. 1–8 (2015).

74. J.A. Gonzalez-Fraga, V.H. Diaz-Ramirez, V. Kober, J.J. Tapia-Higuera, O. Alvarez-Xochihua, "An efficient algorithm for matching of SLAM video sequences," Proc. SPIE's 61 Annual Meeting: Applications of Digital Image Processing XXXIX, Vol. 9971, pp. 99712Z-10 (2016).

75. J.A. Gonzalez-Fraga, V. Kober, V.H. Diaz-Ramirez, "Accurate generation of the 3d map of environment with a rgb-d camera," Proc.SPIE. Vol. 10396. pp. 10396–7 (2017).

76. K. Khoshelham, S.O. Elberink, "Accuracy and resolution of kinect depth data for indoor mapping applications," Sensors. Vol. 12(2), pp. 1437–1454 (2012).

77. A. Chambolle and T. Pock, "An introduction to continuous optimization for imaging," Acta Numerica, Vol. 25, pp, 161–319 (2016).

78. S. Yang, J. Wang, W. Fan, X. Zhang, P. Wonka and J. Ye, "An efficient ADMM algorithm for multidimensional anisotropic total variation regularization problems," Proc. 19th ACM SIGKDD International conference on Knowledge discovery and data mining, pp. 641–64 (2013).

79. Wen, Y., Zhang, K., Li, Z., and Qiao, Y. A discriminative feature learning approach for deep face recognition. In European Conference on Computer Vision, pages 499–515. Springer (2016).

80. Schroff, F., Kalenichenko, D., and Philbin, J. FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pages 815–823 (2015).

81. Deng, J., Guo, J., Xue, N., and Zafeiriou, S. ArcFace: Additive angular margin loss for deep face recognition. arXiv preprint arXiv:1801.07698 (2018).

82. Cao, Q., Shen, L., Xie, W., Parkhi, O. M., and Zisserman, A. (2018). VGGFace2: A dataset for recognising faces across pose and age. In Proceedings of the International Conference on Automatic Face & Gesture Recognition (FG 2018), pages 67–74. IEEE

83. Ruchay, A.N., Dorofeev, K.A., Kober, A.V. Accurate reconstruction of the 3D indoor environment map with a RGB-D camera based on multiple ICP // CEUR Workshop Proceedings, 2210, 2018. Pp. 300–308.

84. Ruchay, A.N., Dorofeev, K.A., Kober, A.V. Accuracy analysis of 3D object reconstruction using RGB-D sensor // CEUR Workshop Proceedings, 2210, 2018. pp. 82–88.

85. Ruchay, A.N., Dorofeev, K.A., Kolpakov, V.I. Fusion of information from multiple kinect sensors for 3D object reconstruction // Computer Optics, 42 (5), 2018. pp. 898–903.

86. 3rd Chalearn Face Anti-spoofing Workshop and Challenge. Workshop Schedule (11 October, 2021).

87. P. Sun, D. Zeng, X. LI, L. Yang, L. Li, Z. Chen, F. Chen. A 3D Mask Presentation Attack Detection Method Based on Polarization Medium Wave Infrared Imaging // Symmetry, 12(3), 2020.

88. Z. Boulkenafet, J. Komulainen, A. Hadid. Face spoofing detection using colour texture analysis. IEEE Trans. Inf. Forensics Secur. 2016, 11, 1818–1830.

89. D. Wen, H. Han, A. Jain. Face spoof detection with image distortion analysis. IEEE Trans. Inf. Forensics. Secur. 2015, 10, 746–761.

90. A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa, A. Noore. Face Presentation Attack with Latex Masks in Multispectral Videos. In Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition Workships, Honolulu, HI, USA, 21–26 July 2017; pp. 275–283.

91. S. Bharadwaj, T. Dhamecha, M. Vatsa, R. Singh. Computationally Efficient Face Spoofing Detection with Motion Magnification. In Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition Workships, Portland, OR, USA, 23–28 June 2013; pp. 105–110.

92. N. Erdogmus, S. Marcel. Spoofing face recognition with 3D masks. IEEE Trans. Inf. Forensics Secur. 2014, 9, 1084–1097.

93. S. Liu, P. Yuen, S. Zhang, G. Zhao. 3D mask face anti-spoofing with remote photoplethysmography. Lect. Notes Comput. Sci. 2016, 9911, 85–100.

94. A. Abd, H. Wei, J. Ferryman. Face Anti-Spoofing Countermeasure: Efficient 2D Materials Classification Using Polarization Imaging. In Proceedings of the IEEE International Workshop on Biometrics and Forensics, Coventry, UK, 4–5 April 2017.

95. Y. Wang, X. Hao, Y. Hou, C. Guo. A New Multispectral Method for Face Liveness Detection. In Proceedings of the Second IAPR Asian Conference on Pattern Recognition, Naha, Japan, 5–8 November 2013; pp. 922–926.

96. J. Liu, A. Kumar. Detecting Presentation Attacks from 3D Face Masks under Multispectral Imaging. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops,

Salt Lake City, UT, USA, 18–22 June 2018; pp. 47–52.

97. A. Krizhevsky, I. Sutskever, G. Hinton. ImageNet Classification with Deep Convolutional Neural Networks; NIPS. Curran Associates Inc.: New York, NY, USA, 2012; Volume 60, pp. 84–90.

98. K. Kotwal, S. Bhattacharjee, S. Marcel. Multispectral Deep Embeddings as a Countermeasure to Custom Silicone Mask Presentation Attacks. IEEE Trans. Biom. Behav. Identity Sci. 2019, 1, 238–251.

99. X. Tan, Y. Li, J. Liu, L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. Lect. Notes Comput. Sci. 2010, 6316, 504–517.

100. Elaggoune, Hocine & Belahcene, Mebarka & Bourennane, Salah. (2022). Hybrid descriptor and optimized CNN with transfer learning for face recognition. Multimedia Tools and Applications. 81. 10.1007/s11042-021-11849-1.

101. Sumegh Tharewal, Timothy Malche, Pradeep Kumar Tiwari, Mohamed Yaseen Jabarulla, Abeer Ali Alnuaim, Almetwally M. Mostafa, Mohammad Aman Ullah, "Score-Level Fusion of 3D Face and 3D Ear for

Multimodal Biometric Human Recognition", Computational Intelligence and Neuroscience, vol. 2022, Article ID 3019194, 9 pages, 2022.

102. Szczuko, P.; Harasimiuk, A.; Czyżewski, A. Evaluation of Decision Fusion Methods for Multimodal Biometrics in the Banking Application. Sensors 2022, 22, 2356.

ДОРОФЕЕВ Константин Андреевич, старший преподаватель кафедры компьютерной безопасности и прикладной алгебры Челябинского государственного университета. 454001, г. Челябинск, ул. Бр. Кашириных, 129. E-mail: kostuan1989@mail.ru

DOROFEEV Konstantin, Senior Lecturer of the Department of Computer Security and Applied Algebra, Chelyabinsk State University. 129 Br. Kashirinykh St., Chelyabinsk, 454001. E-mail: kostuan1989@mail.ru

УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 47–53

Сергеев С.С., Баранкова И.И.

DOI: 10.14529/secur220305

МЕТОДИКА ПОСТРОЕНИЯ ГРАФА АТАК ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Нарушение информационной безопасности может быть вызвано рядом причин: наличием уязвимостей в операционных системах и приложениях; неправильной настройкой системы контроля доступа; некорректной настройкой аппаратного и программного обеспечения (далее – ПО); наличием уязвимых сервисов и вредоносного ПО. Используя различные комбинации существующих уязвимостей и слабых мест злоумышленники в зависимости от своих целей могут реализовывать самые разные стратегии атак. Эти стратегии могут быть нацелены на различные критически важные сетевые ресурсы и включают в себя многоэтапные цепочки атак. Поэтому для снижения ущерба от таких инцидентов необходимо обеспечить предотвращение и выявление угроз безопасности, защиту от их воздействия и реагирование на них. Для мониторинга систем можно воспользоваться моделированием, позволяющим получить описание системы и впоследствии производить количественные и качественные оценки ее показателей.

В данной работе будут рассмотрены разработанные подходы и рекомендации для построения графов атак для объектов критической информационной инфраструктуры.

Ключевые слова: *информационная безопасность, критическая информационная инфраструктура, объекты критической информационной инфраструктуры, моделирование, граф атак, система защиты информации.*

Sergeev S.S., Barankova I.I.

METHODOLOGY FOR CONSTRUCTING ATTACK GRAPH FOR OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Violation of information security can be caused by a number of reasons: the presence of vulnerabilities in operating systems and applications; incorrect configuration of the access

control system; incorrect configuration of hardware and software (hereinafter referred to as software); the presence of vulnerable services and malware. Using various combinations of existing vulnerabilities and weaknesses, attackers, depending on their goals, can implement a variety of attack strategies. These strategies can target a variety of critical network resources and include multi-stage attack chains. Therefore, in order to reduce the damage from such incidents, it is necessary to ensure the prevention and detection of security threats, protection from their impact and response to them. To monitor systems, you can use modeling, which allows you to get a description of the system and subsequently make quantitative and qualitative assessments of its performance.

This article will consider the developed approaches and recommendations for building attack graphs for critical information infrastructure objects.

Keywords: *information security, critical information infrastructure, objects of critical information infrastructure, modeling, attack graph, information security system.*

Информационные активы предприятия подвержены рискам угроз кибербезопасности из-за использования злоумышленниками некоторых известных уязвимостей. Для снижения ущерба от таких инцидентов необходимо обеспечить предупреждение и выявление угроз безопасности, защиту от их воздействия и реагирование на них. Защита информации, как правило, сочетает в себе использование технических средств и организационных мер. Для мониторинга систем можно использовать математическое моделирование, позволяющее получить формальное описание системы и впоследствии производить количественные и качественные оценки ее показателей.

Выделяются следующие теории, которые могут быть положены в основу моделей СЗИ: теории вероятностей и случайных процессов, теории графов, автоматов и сетей Петри, теория нечетких множеств, теории игр и конфликтов, теория катастроф, эволюционное моделирование, формально-эвристический подход, энтропийный подход.

В данной работе в основу моделирования системы защиты положена теория графов. Алгоритм формирования графа атак предназначен для создания графа атак, описывающего всевозможные варианты реализации атакующих действий нарушителем с учетом его первоначального положения, уровня знаний и умений, исходной конфигурации компьютерной сети и реализуемой в ней политики безопасности. На основе общего графа атак производится анализ защищенности информационной системы, выявляются «узкие» места, формируются рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности и созданию эффективной системы защиты информации [1].

Под эффективностью понимается следование принципу «разумной достаточности», который можно описать следующими утверждениями:

– нельзя создать абсолютно непреодолимую защиту;

– необходимо соблюдать баланс между затратами на защиту и получаемым эффектом;

– стоимость средств защиты не должна превышать стоимости активов;

– затраты нарушителя на несанкционированный доступ к активам должны превосходить эффект в соответствующем выражении, получаемый злоумышленником при осуществлении такого доступа [2].

Граф атак – это визуальное средство, используемое для документирования известных угроз безопасности конкретной архитектуры, он описывает пути, по которым злоумышленники могут достичь своих целей. Применение графов атак позволяет несколько упростить задачу аналитиков при исследовании проблемы безопасности и защищенности [3].

Основной целью данной работы является разработка общих подходов и рекомендаций для построения графов атак для объектов критической информационной инфраструктуры.

Ниже представлены дорожная карта, отображающая этапы моделирования графа атак для объектов КИИ (рис.1).

Для моделирования системы защиты информации и построения графа атак первым этапом необходимо определить структуру объекта, состав технических, программных и программно-аппаратных средств, используемых на объекте КИИ. Также необходимо построить функциональную схему и схему сети

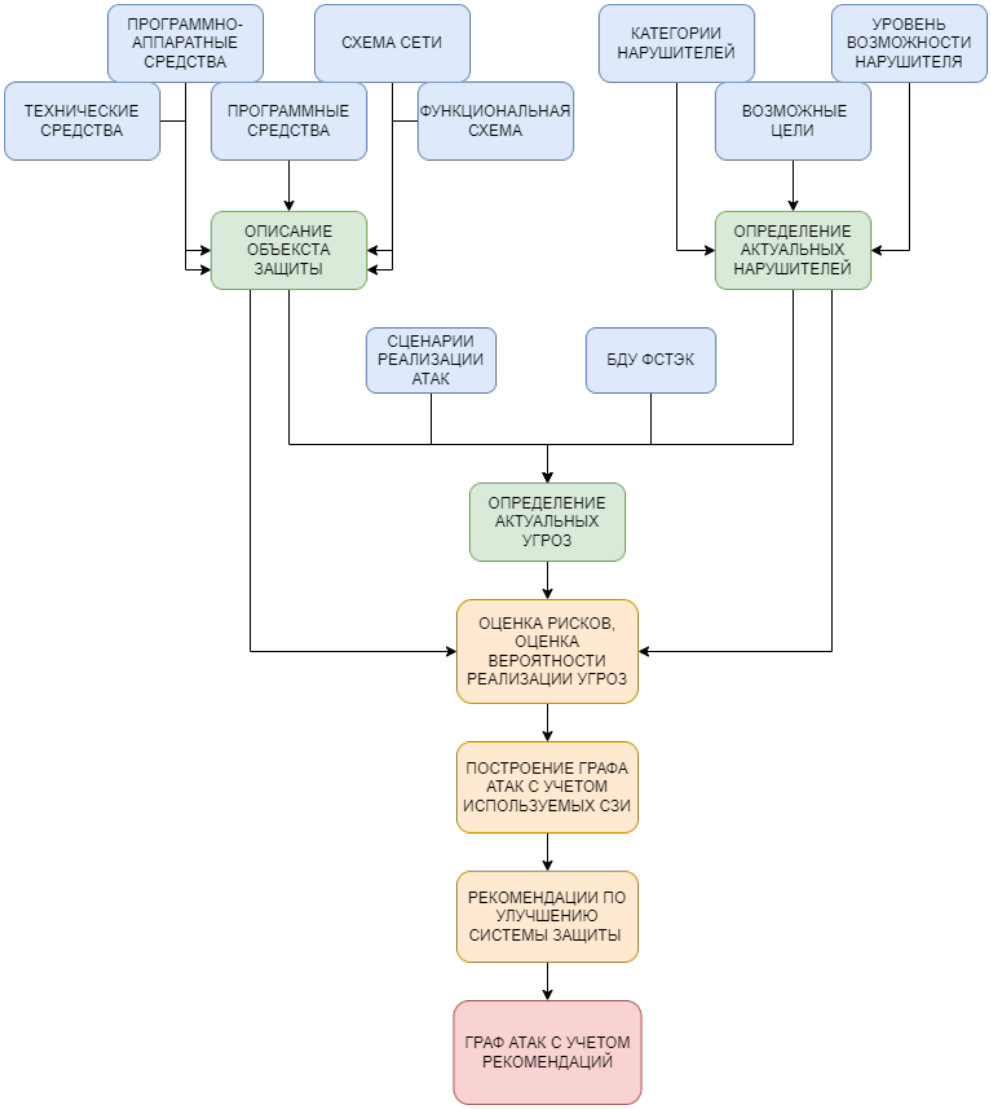

Рис. 1. Дорожная карта построения графа атак для объектов КИИ

объекта. На рисунках 2, 3 приведены примеры, как могут выглядеть функциональная схема и схема сети соответственно.

Следующий этап - выявление возможных нарушителей информационной безопасности в соответствии с Методическим документом «Методика оценки угроз информационной безопасности» (утверждена ФСТЭК России 5 февраля 2021 г.). При определении потенциальных нарушителей следует обратить внимание на следующие категории нарушителей: спецслужбы иностранных государств, террористические группы, преступные группы, хакеры, конкурирующие организации, разработчики программного/программно-аппаратного обеспечения, поставщики программного обеспечения, программно-аппаратных средств, обеспечивающих систем, поставщики услуг связи, вычислительных услуг, лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора, авторизованные пользователи, системные администраторы и администраторы безопасности, бывшие сотрудники [4].

Далее при оценке угроз информационной безопасности должны быть определены возможные пути реализации угроз актуальными нарушителями - актуальные способы реализации угроз информационной безопасности.

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации. Сценарии реализации угроз информационной безопасности должны быть определены для соответствующих способов реализации угроз безопасности информации и применительно к объектам

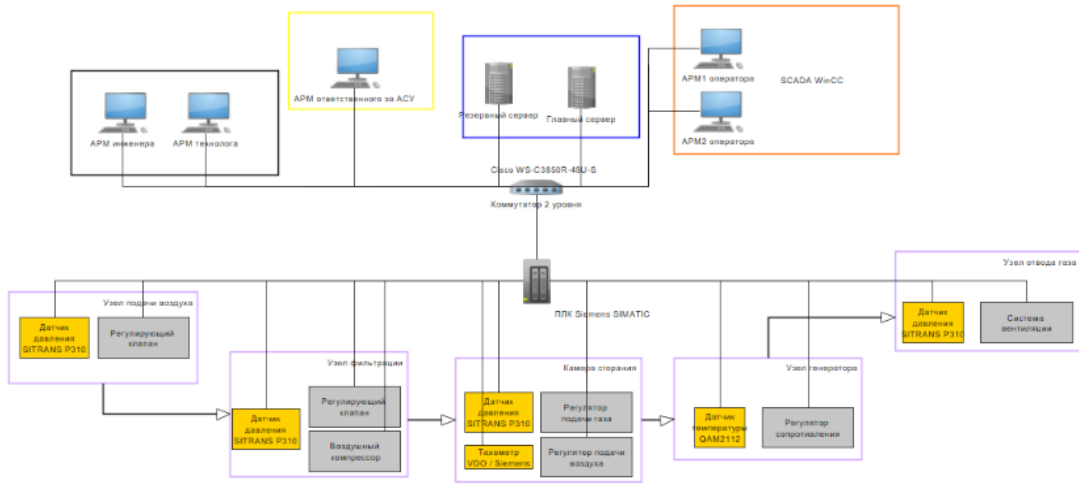

Рис. 2. Пример функциональной схемы АСУ ТП ГТЭС

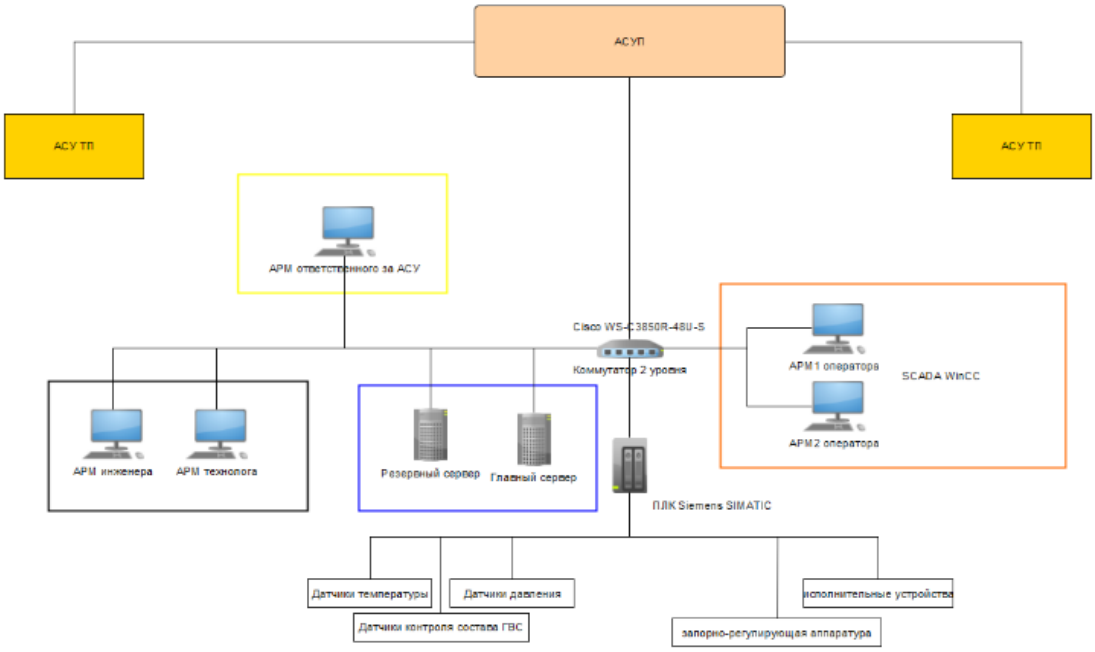

Рис. 3. Пример схемы сети АСУ ТП ГТЭС

воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Следующим важным этапом является оценка рисков. От того, насколько правильно будут оценены риски зависит и эффективность системы информационной безопасности предприятия в целом. Одними из самых распространенных методик управления рисками информационной безопасности являются CRAMM, COBIT for Risk, FRAP, Octave и Microsoft. В [5] приведен краткий обзор методик оценки рисков.

Когда определены актуальные нарушители и их возможности, актуальные угрозы и уязвимости, выполнена оценка рисков, можно строить граф атак.

Алгоритм формирования общего графа атак основан на реализации следующей последовательности действий:

(1) Сбор информации о системах и сетях;

(2) Получение первоначального доступа к компонентам систем и сетей;

(3) Внедрение и исполнение вредоносного программного обеспечения в системах и сетях;

(4) Закрепление в системе или сети;
(5) Управление вредоносным программным обеспечением или компонентами, к которым ранее был получен доступ;

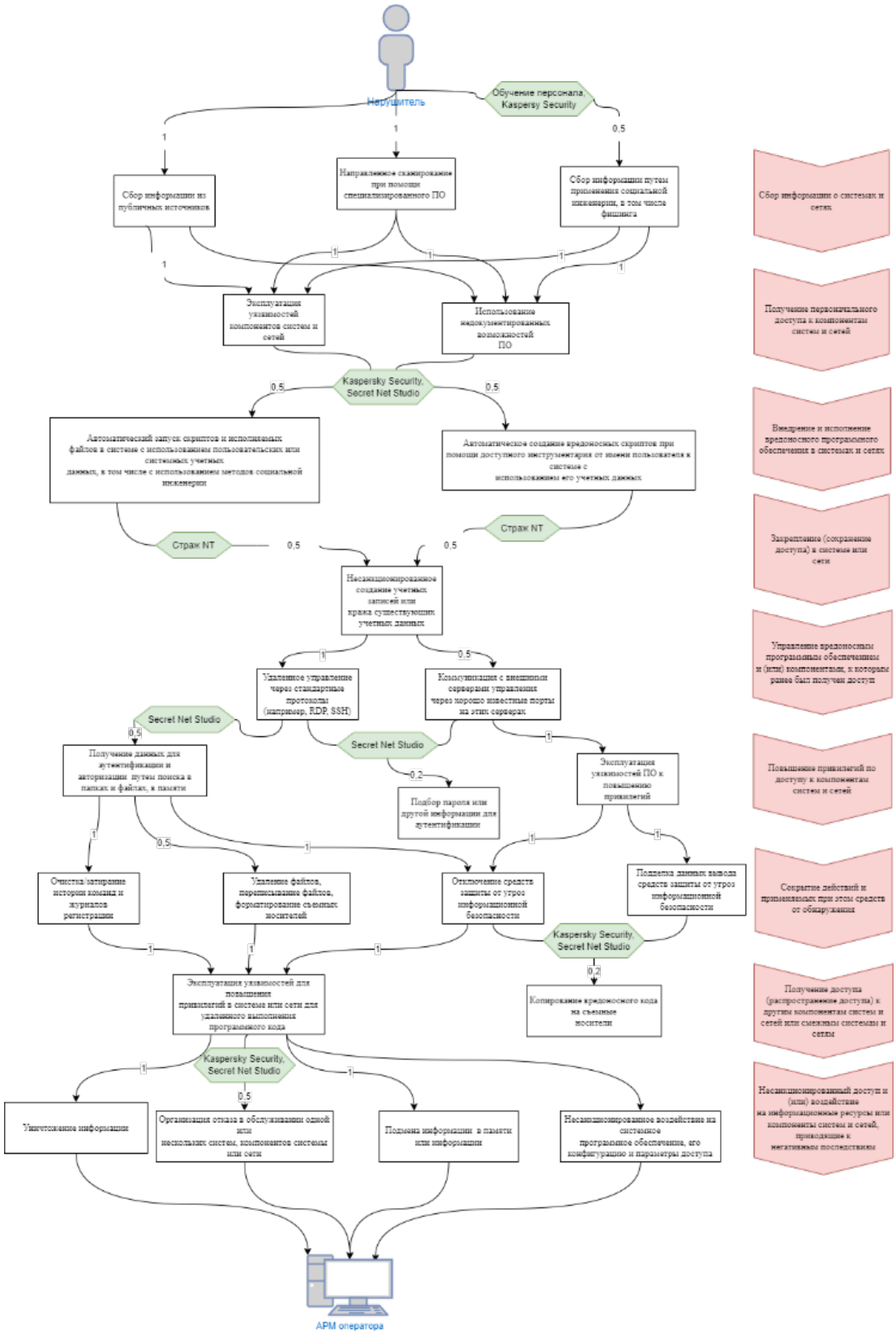

Рис. 4. Граф атак

(6) Повышение привилегий по доступу к компонентам систем и сетей;

(7) Сокрытия действий и применяемых при этом средств от обнаружения;

(8) Получение доступа (распространение доступа) к другим компонентам систем и сетей;

(9) Несанкционированный доступ и негативные воздействие на информационные ресурсы или компоненты систем, сетей [4].

Граф атак нарушителя на АРМ оператора, учитываемый все используемые средства защиты на предприятии приведен на рисунке 4.

На основе построенного графа атак необходимо рассмотреть наиболее вероятно реализуемые сценарии атак и оценить ущерб от их реализации, тем самым определив уязвимые места в системе для дальнейшего формирования рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности и минимизации рисков от происшествий. При формировании рекомендаций по улучшению системы защиты на объектах КИИ также следует учитывать состав мер по обеспечению безопасности для значимого объекта КИИ соответствующей категории значимости, указанный в [6].

Предложенный подход доступно и в полной мере отображает все этапы процесса моделирования системы защиты информации и может быть использован для построения графов атак и выработки рекомендаций для объектов критической информационной инфраструктуры, позволяющие определить уязвимые места в системе и создать эффективную систему защиты информации.

Литература

1. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Построение графа атак для анализа защищенности компьютерных сетей// Символ науки: международный научный журнал. 2016. № 7-2(19). С. 31–32.

2. Курилов Ф.М. Моделирование систем защиты информации. Приложение теории графов / Ф.М. Курилов. – Текст: непосредственный // Технические науки: теория и практика: материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). – Чита: Издательство Молодой ученый, 2016. – С. 6–9.

3. Баранкова И.И., Михайлова У.В., Афанасьева М.В. Минимизация рисков информационной безопасности на основе моделирования угроз безопасности// Динамика систем, механизмов и машин. 2019. №4. С. 60–66

4. Методический документ методика оценки угроз безопасности информации [Текст], Утвержден ФСТЭК России 5 февраля 2021 г. – 2021. – 83 с.

5. Гаврилов А.В., Сизов В.А., Ярошенко Е.В. Методика оценки рисков информационной безопасности предприятия с использованием CASE-технологий// Open education. 2021. № 5. С. 41–49.

6. Приказ ФСТЭК России N 239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации" [Текст], Утвержден ФСТЭК России 25 декабря 2017 г. – 2017. – 37 с.

References

1. Alekseev D.M., Ivanenko K.N., Ubiraylo V.N. Postroenie grafa atak dlya analiza zashchishchennosti komp'yuternykh setey// Simvol nauki: mezhdunarodnyy nauchnyy zhurnal. 2016. № 7-2(19). P. 31–32.

2. Kurilov F.M. Modelirovanie sistem zashchity informatsii. Prilozhenie teorii grafov / F.M. Kurilov. – Tekst: neposredstvennyy // Tekhnicheskie nauki: teoriya i praktika: materialy III Mezhdunar. nauch. konf. (g. Chita, aprel' 2016 g.). – Chita: Izdatel'stvo Molodoy uchenyy, 2016. – P. 6–9.

3. Barankova I.I., Mikhaylova U.V., Afanas'eva M.V. Minimizatsiya riskov informatsionnoy bezopasnosti na osnove modelirovaniya ugroz bezopasnosti// Dinamika sistem, mekhanizmov i mashin. 2019. №4. P. 60–66.

4. Metodicheskiy dokument metodika otsenki ugroz bezopasnosti informatsii [Tekst], Utverzhden FSTEK Rossii 5 fevralya 2021 g. – 2021. – 83 p.

5. Gavrilov A.V., Sizov V.A., Yaroshenko E.V. Metodika otsenki riskov informatsionnoy bezopasnosti predpriyatiya s ispol'zovaniem CASE-tekhnologiy// Open education. 2021. № 5. P. 41–49.

6. Prikaz FSTEK Rossii N 239 "Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury rossiyskoy federatsii" [Tekst], Utverzhden FSTEK Rossii 25 dekabrya 2017 g. – 2017. – 37 p.

СЕРГЕЕВ Сергей Сергеевич, студент 5 курса по специальности «Информационная безопасность автоматизированных систем», ФГБОУ ВО «Магнитогорский государственный техни-

ческий университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: sergeyjek@yandex.ru

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

SERGEEV Sergey Sergeevich, 5th year student majoring in "Information Security of Automated Systems", Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: sergeyjek@yandex.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru

УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 54–61

Собина А.А., Лизовенко О.А., Пономарева О.А., Чернова О.В.

DOI: 10.14529/secur220306

ПОДХОДЫ К ОЦЕНКЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОФИЦИАЛЬНОГО ВЕБ-САЙТА ОРГАНИЗАЦИИ

В статье представлены подходы к оценке угроз безопасности информации в том случае, когда владелец информационного ресурса обладает правом самостоятельно выбирать способ такой оценки. Официальный веб-сайт коммерческой организации, представленный в статье, не относится к информационным системам, для которых нормативно установлен порядок оценки угроз безопасности информации, в том числе: информационным системам персональных данных, государственным (муниципальным) информационным системам и пр. Для подготовки статьи были изучены соответствующие нормативные правовые акты и методические документы федеральных органов исполнительной власти Российской Федерации, международные стандарты. В качестве основы взяты методический документ «Методика оценки угроз безопасности информации» (05.02.2021 г.) и стандарт ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». В процессе подготовки статьи авторами разработаны наглядные схемы, отражающие основные этапы оценки угроз безопасности информации (оценки рисков). Указанные этапы реализованы для рассматриваемой информационной системы.

Ключевые слова: *угрозы безопасности информации, модель угроз безопасности информации, оценка угроз, ИСО, веб-сайт.*

Sobina A.A., Lizovenko O.A., Ponomareva O.A., Chernova O.V.

APPROACHES TO INFORMATION SECURITY THREATS ASSESSMENT FOR THE OFFICIAL WEBSITE OF THE ORGANIZATION

The article provides approaches to the information security threats assessment in the case when the owner of an information resource has the right to choose an approach to the assessment. The official website of the organization presented in the article is not an information system that implies a strict approach to information security threats assessment because the information system does not process personal data, state information resources and other similar data. To prepare the article, regulatory and methodological documents of the federal

executive authorities of the Russian Federation, international standards were studied. As the basis, methodological document «Methodology for assessing threats to information security» (February 5, 2021) and standard ISO/IEC 27005 «Information technology. Security techniques. Information Security Risk Management» were taken. The authors have prepared schemes with the main stages of information security threat assessment (risk assessment). Each described stage is implemented for the considered information system.

Keywords: *information security threats, information security threat model, threats assessment, ISO, website.*

1. Введение

Одним из важнейших этапов создания системы защиты информации (защищенной информационной системы) является определение угроз безопасности информации (далее – УБИ), реализация которых может привести к нарушению безопасности информации (оценка угроз), и разработка на их основе модели угроз безопасности информации.

Корректно разработанная модель угроз безопасности информации информационной системы (далее – модель угроз) позволит выбрать оптимальные технические и организационные меры защиты информации и создать эффективную систему защиты информации [1]. Организационные и технические меры должны блокировать (нейтрализовать) актуальные УБИ, представленные в модели угроз.

В случае недостаточности выбранных мер реализация УБИ может привести к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора информационной системы, а в случае обработки персональных данных – для субъектов персональных данных.

Кроме того, обязанность оператора информационной системы (либо владельца информации, заказчика, заключившего контракт на создание информационной системы) определять (оценивать) УБИ предусмотрена нормативными правовыми актами Российской Федерации. Нормативные правовые акты, регламентирующие оценку УБИ, разрабатываются федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

В рамках настоящей статьи не будут рассмотрены аспекты оценки УБИ:

– связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации;

– связанных с техническими каналами утечки информации;

– в финансовой сфере (для финансовых организаций).

2. Подход к оценке угроз безопасности информации в соответствии с требованиями регулятора

Для определения УБИ, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, а также для некоторых других категорий информационных систем, должен использоваться методический документ «Методика оценки угроз безопасности информации», утвержденный 05.02.2021 г. (далее – Методика оценки, методический документ).

Этапы оценки УБИ, представленные в методическом документе, приведены на рис. 1.

Методическим документом определены форма, порядок разработки и актуализации модели угроз.

3. Иностранные (международные) подходы к оценке угроз безопасности информации

Для эффективного управления рисками информационной безопасности разработаны специальные методики, представленные, например, в международных стандартах ISO 15408, ISO 17799 (BS7799), ISO 27000, BSI; а также национальных стандартах NIST 800-'30, SAC, COSO, SAS 55/78 и др. [2].

Как правило, в зарубежных (международных) стандартах и методиках оценка УБИ является составной частью оценки рисков информационной безопасности. Риск информационной безопасности – это потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

В рамках настоящей статьи рассматривается стандарт ГОСТ Р ИСО/МЭК 27005–2010 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Менеджмент риска информационной безопасности» (далее –

ИСО/МЭК 27005), так как он переведен на русский язык, утвержден Федеральным агентством по техническому регулированию и метрологии и введен в действие в качестве национального стандарта Российской Федерации.

ИСО/МЭК 27005 представляет руководство по управлению рисками информационной безопасности (далее – ИБ) и предназначен для помощи в реализации процессов информационной безопасности на основе подхода, связанного с менеджментом риска.

Примеры использования ИСО/МЭК 27005 представлены, например, в [3], [4], [5], [6].

Отдельные этапы оценки риска ИБ, представленные в ИСО/МЭК 27005, приведены на рисунке 2.

Оцененные риски ИБ требуют обработки: снижения, сохранения, предотвращения, переноса риска. Если уровень риска соответствует критериям принятия риска, то отсутствует необходимость в реализации дополнительных мер, и риск может быть сохранен (принят).

Таким образом, если проводить параллель с Методикой оценки, соотношение уровня риска ИБ критериям принятия риска – индикатор актуальности (неактуальности) УБИ, соответствующей данному риску.

4. Пример практического применения подходов к оценке угроз безопасности информации

4.1. Исходные данные для оценки

Подходы к оценке угроз (рисков) рассмотрены на примере информационной системы, представляющей собой официальный сайт коммерческой организации (далее – ИС). Указанная организация обладает правом выбора подхода к оценке УБИ, так на рассматриваемый веб-сайт не распространяются требования регулятора.

Сайт размещен на сервере организации и поддерживается ее сотрудниками, а его содержание представляет собой исключительно справочную информацию (каталог услуг, новости, информация о партнерах и клиентах, контакты, вакансии). Кроме того, на сайте нет платежного механизма, формы обратной связи и личного кабинета для клиентов.

4.2. Методика оценки

Этапы оценки УБИ приведены на рисунке 1.

Рис. 1

Рис. 2

В качестве негативных последствий реализации (возникновения) УБИ можно обозначить:

– размещение недостоверной информации на веб-ресурсе организации;

– использование веб-ресурса с целью распространения и управления вредоносным программным обеспечением;

– нарушение функционирования веб-ресурса;

– нарушение деловой репутации.

Объекты воздействия УБИ:

– информация (обрабатываемая в ИС, учетные данные);

– автоматизированное рабочее место администратора сайта;

– сервер;

– системное программное обеспечение;

– прикладное программное обеспечение (обеспечивающее функционирование сайта, веб-браузер);

– телекоммуникационное оборудование;

– обеспечивающие системы (электропитание, кондиционирование);

– каналы связи;

– пользователь (администратор сайта).

Нарушители признаются актуальными, если возможные цели реализации ими УБИ могут привести к определенным для ИС негативным последствиям и соответствующим рискам (видам ущерба). Таким образом, для рассматриваемой ИС актуальными являются следующие виды нарушителей:

– отдельные физические лица (хакеры);

– конкурирующие организации;

– администратор информационной системы;

– бывшие (уволенные) работники (пользователи).

Были учтены следующие цели реализации УБИ, которые могут привести к негативным последствиям:

– получение конкурентных преимуществ;

– любопытство или желание самореализации (подтверждение статуса);

– непреднамеренные, неосторожные или неквалифицированные действия;

– месть за ранее совершенные действия.

Способы реализации УБИ:

– атака типа «отказ в обслуживании»;

– использование уязвимостей прикладного программного обеспечения, используемого для обработки данных;

– действия пользователей (ошибочные или целенаправленные), приводящие к деструктивным последствиям;

– повреждение (вывод из строя) технических средств.

УБИ возможна, если для нее имеются нарушитель, объект воздействия, способ реализации, и ее реализация может привести к негативным последствиям. Перечень возможных угроз формируется из общего перечня УБИ, приведенного в Банке данных угроз (https://bdu.fstec.ru/), путем исключения УБИ, не удовлетворяющих данному условию (например, для исключаемой угрозы УБИ.110 объект воздействия – ресурсные центры грид-системы, которых в ИС нет).

Для каждой из возможных УБИ определяются сценарии реализации на основании представленных в Методике оценки техник и тактик. Чтобы определить все возможные сценарии атак, техники и тактики, получить дополнительную информацию о возможных уязвимостях, способах реализации компьютерных атак могут использоваться Банк данных угроз (https://bdu.fstec.ru/) и другие источники [7].

Например, рассмотрим УБИ.100 «Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб», которая реализуется следующим сценарием: тактика Т1, техника Т1.4 (направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств). Таким образом, данная УБИ должна быть признана актуальной и включена в модель угроз рассматриваемой ИС.

4.3. ИСО/МЭК 27005

Основные этапы оценки риска ИБ приведены на рисунке 2.

До процедуры оценки риска ИБ должны быть определены основные критерии, сфера действия и границы, структура процесса менеджмента риска ИБ.

На первом этапе оценки риска ИБ определяются активы. Активы в ИСО/МЭК 27005 понимаются шире, чем объекты воздействия в Методике оценки.

Основные и вспомогательные активы в рамках ИС, их ценность (по десятибалльной шкале) приведены в таблице 1.

В качестве перечня угроз и их источников принят полный набор данных из приложения С к ИСО/МЭК 27005, за исключением угроз и источников угроз, указанных в таблице 2.

Далее необходимо установить, какие организационные и технические меры реализованы ранее. В организации реализованы следующие меры:

Таблица 1

Активы

Наименование актива	Владелец	Значимость
Бизнес-процесс – размещения информации на официальном сайте с целью обеспечения информационной открытости организации	Руководитель организации	8
Информация	Руководитель организации	6
Автоматизированное рабочее место администратора сайта	Администратор сайта	5
Сервер	Руководитель отдела ИТ	7
Системное программное обеспечение	Администратор сайта	5
Прикладное программное обеспечение	Администратор сайта	5
Телекоммуникационное оборудование	Руководитель отдела ИТ	4
Обеспечивающие системы (электропитание, кондиционирование)	Руководитель отдела ИТ	6
Каналы связи	Руководитель отдела ИТ	4
Пользователь (администратор сайта)	Руководитель организации	4
Помещение серверной и кабинет отдела информационных технологий	Руководитель отдела ИТ	3

Таблица 2

Исключаемые угрозы и их источники

Исключаемая угроза/источник угрозы	Обоснование
Класс угроз, связанных с природными явлениями	Вулканическая и сейсмическая активность в регионе отсутствуют. Помещения расположены на 9 этаже из 14
Перехват компрометирующих сигналов помех	Помехи не используются
Прослушивание	Акустическая информация не обрабатывается
Кража носителей или документов	Защищаемая информация не хранится на отдельных (не встроенных) носителях и в бумажном виде
Поиск повторно используемых или забракованных носителей	Защищаемая информация не хранится на отдельных (не встроенных) носителях и в бумажном виде
Данные из ненадежных источников	Не обрабатывается информация, влияющая на принятие решений
Определение местонахождения	Местонахождение не является конфиденциальной информацией
Террорист	Не соответствует мотивация
Промышленный шпионаж	Не соответствует мотивация

– доступ в крыло на этаже, которое занимает организация, ограничен: установлена металлическая дверь с магнитным замком;

– внедрена система видеонаблюдения;

– внедрена система охранно-пожарной сигнализации с выводом на пункт охраны;

– все помещения оборудованы запираемыми дверьми;

– должностные инструкции сотрудников включают положения по обеспечению ИБ, сотрудники проходят периодическое обучение;

– используются средства антивирусной защиты на всех рабочих станциях;

– используется межсетевой экран на границе с сетью общего доступа;

– серверный сегмент выделен в отдельную виртуальную локальную сеть (VLAN).

Технические уязвимости могут быть определены с использованием автоматизированных инструментальных средств поиска уязвимостей, тестирования и оценки, тестирования на проникновение, проверки кода.

Среди уязвимостей для организации также характерны:

– плохой менеджмент паролей;

– отсутствие резервных копий;

– единая точка отказа;

– отсутствие формального процесса для пересмотра прав пользователей.

Негативные последствия для реализации определяются в виде перечней сценариев инцидентов. Сценарий инцидента – это описание угрозы, использующей определенную уязвимость или совокупность уязвимостей в инциденте ИБ.

Таким образом, для организации, учитывая исходные данные, можно привести следующие сценарии:

a) угроза фальсификации прав, использующая уязвимости, связанные с плохим менеджментом паролей, отсутствием формального процесса для пересмотра прав пользователей, может привести к размещению недостоверной информации на веб-ресурсе организации;

b) угроза отказа телекоммуникационного оборудования, использующая уязвимость, связанную с единой точкой отказа, может привести к нарушению функционирования веб-ресурса;

c) угроза тайных действий с программными средствами, использующая уязвимость, связанную с отсутствием резервных копий, может привести к использованию веб-ресурса с целью распространения и управления вредоносным программным обеспечением.

Оценка последствий осуществляется с учетом ценности активов, которые оказываются затронуты инцидентом. Результаты оценки приведены в таблице 3.

Установление значений уровней рисков производится для всех значимых сценариев инцидентов. В стандарте приведены примеры различных методов и подходов к установлению значений рисков ИБ.

В организации используется подход, приведенный в таблице 4.

Перечень рассмотренных рисков с уровнями присвоенных значений и назначенными приоритетами приведен в таблице 5.

В зависимости от принятых в организа-

Таблица 3

Сравнение сценариев

Сценарий	Ценность	Вероятность
a)	12	Низкая
b)	15	Высокая
c)	8	Средняя

Таблица 4

Критерии оценки

Уровень риска		Вероятность реализации		
		Низкая	Средняя	Высокая
Ценность	1-4	1	3	6
	5-9	2	4	7
	10-14	3	5	8
	15-19	4	6	9
	20+	5	7	10

Таблица 5

Рассмотренные риски

Сценарий	Уровень риска	Ранжирование угроз
a)	3	3
b)	9	1
c)	4	2

ции критериев принятия риска, риск ИБ может быть сохранен (принят) либо потребовать дальнейшей обработки. Предположим, что в организации приемлемый уровень риска – 3.

Таким образом, требуют дальнейшей обработки риски ИБ, описанные сценариями b) и c). В сценариях реализации отражены соответствующие УБИ. Должны быть выбраны меры и средства контроля и управления для снижения, предотвращения или переноса указанных рисков.

5. Заключение

Авторами проанализированы подходы к оценке УБИ и рисков информационной безопасности, изложенные в документах:

– методический документ «Методика оценки угроз безопасности информации», утвержденный 05.02.2021 г.;

– ГОСТ Р ИСО/МЭК 27005–2010 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Менеджмент риска информационной безопасности».

Объем данной статьи не позволяет отразить все практические аспекты оценки УБИ и рисков информационной безопасности или провести более детальное сравнение приведенных выше документов. Поэтому данные вопросы будут рассмотрены в последующих работах.

Литература / References

1. O. Kalugina, I. Barankova and U. Mikhailova, «Development of a Tool for Modeling Security Threats of an Enterprise Information System», 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, P. 1–5, DOI: 10.1109/ICECCE49384.2020.9179449.

2. S. S. Sokolov, O. M. Alimov, M. G. Golubeva, V. G. Burlov and N. M. Vikhrov, «The automating process of information security management», 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018, P. 124–127, DOI: 10.1109/EIConRus.2018.8317045.

3. M. M. Putra and K. Mutijarsa, «Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005», 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), 2021, P. 14–19, DOI: 10.1109/EIConCIT50028.2021.9431865.

4. S. Jaya Putra, M. Nur Gunawan, A. Falach Sobri, J. Muslimin, Amilin and D. Saepudin, «Information

Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company», 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020, P. 1–5, doi: 10.1109/CITSM50537.2020.9268845.

5. S. Prasetyo and Y. G. Sucahyo, «Information security risk management planning: A case study at application module of state asset directorate general of state asset ministry of finance», 2014 International Conference on Advanced Computer Science and Information System, 2014, P. 96–101, doi: 10.1109/ICACSIS.2014.7065875.

6. A. Alwi and K. A. Zainol Ariffin, «Information Security Risk Assessment for the Malaysian Aeronautical Information Management System», 2018 Cyber Resilience Conference (CRC), 2018, P. 1–4, doi: 10.1109/CR.2018.8626841.

7. V. Vasilyev, A. Kirillova, A. Vulfin and A. Nikonov, «Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score», 2021 International Conference on Information Technology and Nanotechnology (ITNT), 2021, P. 1–6, DOI: 10.1109/ITNT52450.2021.9649191.

СОБИНА Алена Александровна, магистрант Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: micropipe@gmail.com.

ЛИЗОВЕНКО Ольга Александровна, магистрант Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: lanuri@yandex.ru.

ПОНОМАРЕВА Ольга Алексеевна, Кандидат технических наук, Старший преподаватель Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: o.a.ponomareva@urfu.ru.

ЧЕРНОВА Ольга Вячеславовна, старший преподаватель Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: o.v.chernova@urfu.ru.

SOBINA Alena Aleksandrovna, Master's student of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: makkuropip@gmail.com.

LIZOVENKO Olga Aleksandrovna, Master's student of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: lanuri@yandex.ru.

PONOMAREVA Olga Alekseevna, Candidate of Technical Sciences, Senior Lecturer of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: o.a.ponomareva@urfu.ru.

CHERNOVA Olga Vjacheslavovna, Senior Lecturer of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: o.v.chernova@urfu.ru.

УДК 004.67 Вестник УрФО № 3(45) / 2022, с. 62–68

Шпак В.А., Михайлова У.В., Баранкова И.И.

DOI: 10.14529/secur220307

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ОЦЕНКИ И АНАЛИЗА АКУСТИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ

Защита выделенного или защищаемого помещения должна состоять из комплекса организационных, технических и иных мер предотвращающих несанкционированное получения или воздействия злоумышленником на защищаемую информацию. Оценка эффективности защищенности помещений по акустическому и виброакустическому каналам утечки информации определяется методическими документами ФСТЭК России. В статье рассматривается оценка утечки информации по акустическому каналу, приведены проблемы современных технических средств анализа исследуемого ТКУИ. Для этого разработан программно-аппаратный продукт, позволяющий проводить оценку показателей акустической защищенности ограждающих конструкций помещения и выводить результаты в виде отчета.

Ключевые слова: *информационная безопасность, утечка речевой информации, акустический канал, анализ звукоизоляционных свойств, ограждающие конструкции, оценка, защита информации, программно-технические каналы утечки информации.*

Shpak V.A., Mikhailova U.V., Barankova I.I.

DEVELOPMENT OF SOFTWARE AND HARDWARE COMPLEX FOR EVALUATION AND ANALYSIS OF ACOUSTIC CHANNEL OF INFORMATION LOSS

Protection of dedicated or protected premises should consist of a set of organizational, technical and other measures that prevent unauthorized receipt or impact by an attacker on protected information. Evaluation of the effectiveness of the security of premises by acoustic and vibroacoustic channels of information leakage is determined by the methodological documents of the FSTEC of Russia. The article discusses the assessment of information leakage through the acoustic channel, presents the problems of modern technical means for analyzing

the studied channel of information loss. For this, a software and hardware product has been developed that allows evaluating the acoustic protection indicators of building envelopes and displaying the results in the form of a report.

Keywords: *information security, speech information leakage, acoustic channel, analysis of sound insulation properties, enclosing structures, assessment, information protection, software and hardware channels of information leakage.*

Защита акустической (речевой) информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта или учреждения. Для перехвата речевой информации предполагаемый «противник» может использовать каналы непреднамеренного прослушивания речи (без использования технических средств), а также широкий арсенал портативных средств акустической речевой разведки, позволяющих перехватывать речевую информацию по прямому акустическому, виброакустическому, электроакустическому и оптико-электронному (акустооптическому) каналам [1].

Выделенными (защищаемыми) помещениями называют помещения (служебные кабинеты, конференц-залы и т.п.), специально предназначенные для проведения различных конфиденциальных мероприятий (совещаний, обсуждений, переговоров и т.п.). Защите подлежит как само помещение, так и технические средства, расположенные в этом помещении, а именно основные технические средства и системы (ОТСС) и вспомогательные технические средства и системы (ВТСС). Кроме того, предусматриваются меры защиты от различных технических средств разведки, которые могут быть использованы злоумышленником для несанкционированного получения или воздействия на защищаемую информацию [2].

Совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация, и физической среды, в которой распространяется информационный сигнал, называется техническим каналом утечки информации (рис. 1) [3].

На данный момент существует и исполь-

Рис. 1. Общая схема технического канала утечки информации

зуется множество готовых средств оценки и анализа вибро- и акустического канала утечки информации, таких семейств как «Спрут», «Шепот», «Аврора» и проч. Такие средства обеспечивают полную достоверность измерений и расчетов согласно существующему сборнику нормативно-методических документов ФСТЭК России, однако их преследует ряд недостатков. К таким недостаткам относятся сложность при разворачивании средства в рабочее состояние из-за проводного подключения компонентов комплекса и отсутствие функции автоматического формирования отчета акустической защищенности защищаемых помещений.

Для решения первого недостатка существующих средств оценки и анализа акустического канала утечки информации была разработана схема шумомера (рис. 2). Данная схема построена на основе операционного усилителя LM386 и отличается наличием фильтров низких и верхних частот, позволяющих проводить проверку как на пяти октавах, так и на семи. Коэффициент усиления микросхемы LM386 можно регулировать подстрочным резистором RP2. Собранная схема подключается к микроконтроллеру Arduino Nano. Беспроводная связь с устройством управления комплексом обеспечивается за счет Wi-Fi модуля ESP 12e. Собранный шумо-

мер энергетически автономен благодаря Li-ion аккумулятору.

В качестве генератора шума в разрабатываемом комплексе временно используется портативная беспроводная акустическая колонка JBL Flip 5. К ее преимуществам относятся компактность, автономность, наличие ударопрочного корпуса, однако использование генератора шума, не предназначенного для проверки защищаемых помещений, требует дополнительной настройки в эквалайзере из-за неровной амплитудно-частотной характеристики тестового сигнала [4].

Очень важно правильно интерпретировать данные полученные с АЦП, поскольку значения уровня звукового давления имеют нелинейную зависимость от имеющихся значений АЦП с выхода аналогового контакта Arduino. Для этого нужно откалибровать шумомер по эталонному измерителю шума CEM DT-8851. Для наиболее точной калибровки нужно произвести несколько измерений на каждой октаве для обоих шумомеров. На основе полученных данных можно провести корреляцию между значениями методом линейной регрессии.

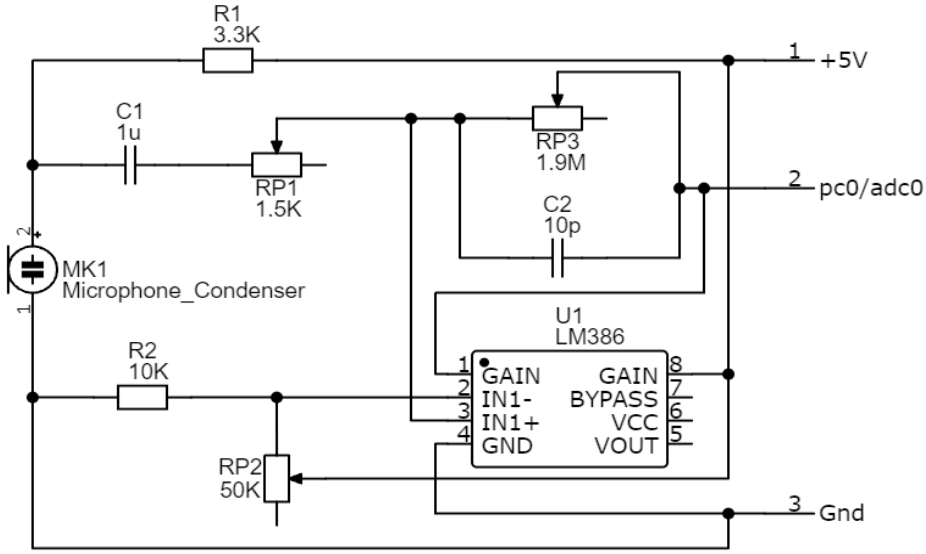

Рис. 2. Схема шумомера

Управление шумомером и его режимами работы осуществляется посредством разработанного программного продукта для оценки изоляционных свойств ограждающих конструкций. Данное ПО было разработано в программной среде C#. Для работы приложения в качестве полноценного комплекса необходимо и достаточно использовать ноутбук с ОС Windows 7 и .NET Framework 5.0. В программе реализована форма для указания основных сведений об исследуемом объекте (рис. 3).

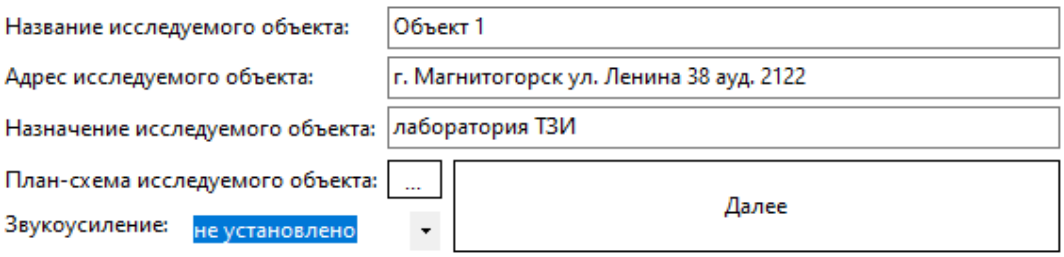

Рис. 3. Стартовая форма ПО

Одно из преимуществ разрабатываемого ПО, по сравнению с существующими аналогами — наличие графического редактора (рис. 4) для расстановки контрольных точек (КТ) на техническом плане исследуемого помещения. КТ поделены на типы ограждающих конструкций (окна, стены и т.д.), каждый из которых поделен на различные виды типовых конструкций. Типовые виды ограждающих конструкций взяты из методики ФСТЭК России. В окне расстановки КТ каждый тип ограждающих конструкций обозначен своим

цветом: стены и сплошные перегородки кирпичного цвета, двери — коричневые, перекрытия — серые, а окна — голубые. Помимо вида и типа для каждой КТ можно настраивать толщину и прочие особенности конструкций, характерные для того или иного типа ограждающей конструкции.

После задания КТ в графическом редакторе и расстановки измерительного оборудования у КТ №1 в положение согласно методике ФСТЭК России, проводится автоматическое сканирование ограждающей конструкции. После окончания комплекса измерений в одной КТ приложение предложит оператору устройства управления комплексом переставить измерительное оборудование в другую КТ. Измерения должны проводиться при минимально возможных уровнях акустических и вибрационных шумов.

На основе выполненных измерений про-

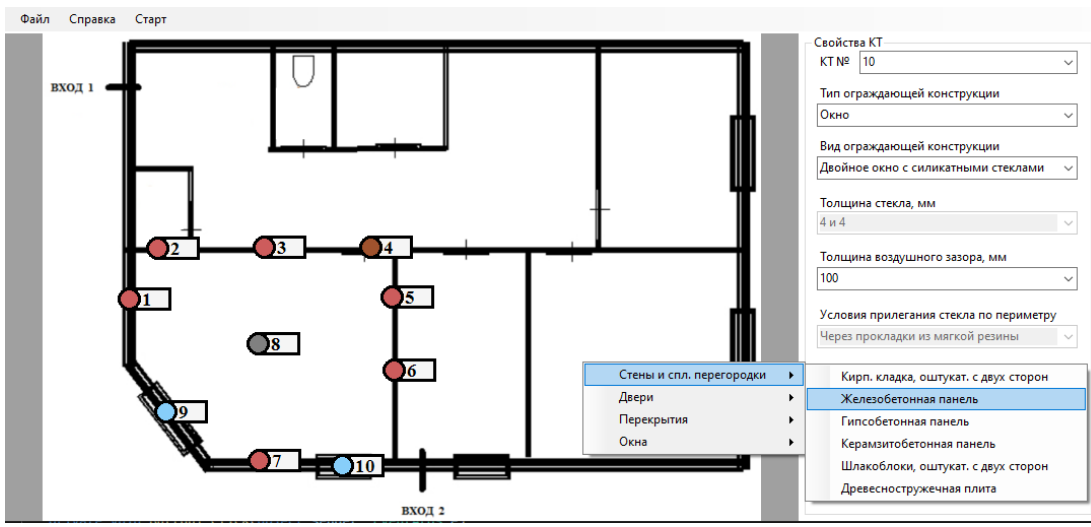

Рис. 4. Окно расстановки КТ

Результат сканирования

Файл Справка

КТ	Среднегеометрическая частота, Гц	Измеренный уровень акуст. шума в КТ, Дб	Уровень измеренного суммарного сигнала, Дб	Расчетный уровень акустического сигнала в КТ, Дб	Измеренный уровень акустического сигнала в помещении	Октавные уровни звукоизоляции в контрольной точке, Дб
1	250	36	39,1	3,1	70	66,9
(Железобетонная панель 100 мм.)	500	36	37,5	1,5	70	68,5
	1000	36	37,5	1,5	70	68,5
	2000	36	38,3	2,3	70	67,7
	4000	36	40,5	4,5	70	65,5
	8000	36	37,7	1,7	70	70,3
2	250	38	37,8	1,8	72	70,2
(Железобетонная панель 100 мм.)	500	38	38,2	2,2	72	69,8
	1000	38	37,8	1,8	72	70,2
	2000	38	38	2	72	70
	4000	38	53,4	15,4	72	54,6
	8000	38	46,8	8,8	72	61,2
3	250	36	60	22	70	48
(Железобетонная панель 100 мм.)	500	36	53	15	70	55

Рис. 5. Окно результатов сканирования

водятся расчеты звукоизоляции ограждающих конструкций на исследуемом объекте согласно методике ФСТЭК России. Результат расчетов выводится в таблицу на пользовательскую форму (рис. 5).

Итоговая схема работы комплекса указана на рис. 6. Устройство управления комплексом по Bluetooth передает на генератор шума тест-сигнал. Генератор шума излучает полученный акустический сигнал через ограждающую конструкцию в месте установки КТ. Шум, прошедший ограждающую конструк-

Рис. 6. Общий принцип работы комплекса

цию улавливается шумомером, обрабатывается АЦП и по сети Wi-Fi передается на устройство управления комплексом. Последний этап — устройство управления комплексом по полученному уровню звукового давления рассчитывает звукопоглощающие свойства исследуемой ограждающей конструкции согласно нормативно-методическому документу по противодействию акустической речевой разведке.

По полученным результатам составляется отчет в PDF формате. В отчет входят: информация об исполнителе проверки помещения, адресе и функциональном назначении помещения, план помещения с расставленными на нем КТ, таблица с проведенными измерениями и расчетами для каждой КТ, а также заключение о соответствии помещения требованиям безопасности.

Выполнив оценку работы разрабатываемого средства оценки и анализа акустического канала утечки информации можно составить заключение о том, что данный программно-аппаратный продукт, выполняя измерения, получает достоверные данные, а также упрощает процедуру анализа полученных данных. Комплекс легко разворачивать в рабочее состояние благодаря полностью беспроводному подключению компонентов. Положительными отличительными особенностями программной части комплекса являются наличие функций графического редактора расстановки КТ и создания автоматического развернутого отчета акустической защищенности защищаемых помещений, оформленного согласно требованиям ФСТЭК России, в PDF формате.

Литература

1. Оценка эффективности защиты акустической (речевой) информации. – «электрон. текст. дан.». – Москва: [б.и.], 20.08.2016. – Режим доступа: https://itsec2012.ru/ocenka-effektivnosti-zashchity-akusticheskoy-rechevoy-informaciil.

2. Акустическая защита выделенного (защищаемого) помещения. – Электрон. журн. – Москва: DELPHI PLUS - ежедневные новости IT-технологий, 2017. – режим доступа к журн.: https://www.delphiplus.org/.

3. Хорев, А. А. Технические каналы утечки информации, обрабатываемой техническими средствами. / Хорев, А. А. // – Электрон. журн. – Москва: Бюро научно-технической информации, 2006. – режим доступа к журн.: http://www.bnti.ru/.

4. JBL flip5 АЧХ / JBL flip5 frequency response / EQ // – Электрон. журн. –Новосибирск: Webstudius Новосибирск, 2021. – режим доступа: https://webstudius.com/jbl-flip5-achh-jbl-flip5-frequency-response.

5. Михайлова, У. В. Эффективность применения СЗИ от утечки по акустическим каналам / У. В. Михайлова, Г. И. Лукьянов // Вестник УрФО. Безопасность в информационной сфере. 2014. № 4 (14). С. 14–18.

6. Михайлова, У. В. Защита информации в помещении от утечки по акустическому каналу /

У. В. Михайлова, Г. И. Лукьянов // Актуальные проблемы современной науки, техники и образования: тезисы докладов 76-й Междунар. науч.-техн. конф. 2018. С. 294.

7. Баранкова И. И. Компетентностно-ориентированный подход к формированию лабораторий учебно-тренировочных средств при подготовке специалистов в области информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 46–50.

8. Лукьянов, Г. И. Защита информации по виброакустическим каналам с использованием СЗИ «СОНАТА» / Г. И. Лукьянов, У. В. Михайлова, И. И. Баранкова, М. В. Коновалов // Актуальные проблемы современной науки, техники и образования. 2015. Т. 2. № 1. С. 186–188.

9. Хорев, А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А. А. Хорев // М: НПЦ «Аналитика», 2008. 436 с.

10. Григорьев И. А., Казановский А. И. / Методический подход к оценке эффективности защиты речевой информации // Вестник ВГТУ. 2010. №5. URL: https://cyberleninka.ru/article/n/metodicheskiy-podhod-k-otsenke-effektivnosti-zaschity-rechevoy-informatsii.

References

1. Ocenka jeffektivnosti zashhity akusticheskoj (rechevoj) informa-cii. – «jelektron. tekst. dan.». – Moskva: [b.i.], 20.08.2016. – Rezhim dostupa: https://itsec2012.ru/ocenka-effektivnosti-zashchity-akusticheskoy-rechevoy-informaciil.

2. Akusticheskaja zashhita vydelennogo (zashhishhaemogo) pomeshhenija. – Jelektron. zhurn. – Moskva: DELPHI PLUS - ezhednevnye novosti IT-tehnologij, 2017. – rezhim dostupa k zhurn.: https://www.delphiplus.org/.

3. Horev, A. A. Tehnicheskie kanaly utechki informacii, obrabaty-vaemoj tehnicheskimi sredstvami. / Horev, A. A. // – Jelektron. zhurn. – Moskva: Bjuro nauchno-tehnicheskoj informacii, 2006. – rezhim dostupa k zhurn.: http://www.bnti.ru/.

4. JBL flip5 AChH / JBL flip5 frequency response / EQ // – Jelektron. zhurn. –Novosibirsk: Webstudius Novosibirsk, 2021. – rezhim dostupa: https://webstudius.com/jbl-flip5-achh-jbl-flip5-frequency-response.

5. Mihajlova, U. V. Jeffektivnost' primenenija SZI ot utechki po akusticheskim kanalam / U. V. Mihajlova, G. I. Luk'janov // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2014. № 4 (14). P. 14–18.

6. Mihajlova, U. V. Zashhita informacii v pomeshhenii ot utechki po akusticheskomu kanalu / U. V. Mihajlova, G. I. Luk'janov // Aktual'nye pro-blemy sovremennoj nauki, tehniki i obrazovanija: tezisy dokladov 76-j Mezhdunar. nauch.-tehn. konf. 2018. P. 294.

7. Barankova I. I. Kompetentnostno-orientirovannyj podhod k formirovaniju laboratorij uchebno-trenirovochnyh sredstv pri podgotovke specialistov v oblasti informacionnoj bezopasnosti // Informacionnoe protivodejstvie ugrozam terrorizma. 2015. T. 1. № 25. P. 46–50.

8. Luk'janov, G. I. Zashhita informacii po vibroakusticheskim kana-lam s ispol'zovaniem SZI «SONATA» / G. I. Luk'janov, U. V. Mihajlova, I. I. Barankova, M. V. Konovalov // Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija. 2015. T. 2. № 1. P. 186–188.

9. Horev, A. A. Zashhita informacii ot utechki po tehnicheskim kana-lam. Chast' 1. Tehnicheskie kanaly utechki informacii / A. A. Horev // M: NPC «Analitika», 2008. 436 p.

10. Grigor'ev I. A., Kazanovskij A. I. / Metodicheskij podhod k ocenke jeffektivnosti zashhity rechevoj informacii // Vestnik VGTU. 2010. №5. URL: https://cyberleninka.ru/article/n/metodicheskiy-podhod-k-otsenke-effektivnosti-zaschity-rechevoy-informatsii.

ШПАК Виталий Алексеевич, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: xxx-yyy-2014@inbox.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: ylianapost@gmail.com

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующая кафедрой Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: inna_barankova@mail.ru

SHPAK Vitaliy Alekseevich, student of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: xxx-yyy-2014@inbox.ru

MIKHAILOVA Uliana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security f Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru

УДК 004.056.5:519.876.5 Вестник УрФО № 3(45) / 2022, с. 69–75

Литвинов Г.А.

DOI: 10.14529/secur220308

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ РЕПУТАЦИОННОЙ МОДЕЛИ ДЛЯ ПОИСКА МАРШРУТА В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ [1]

Для решения проблемы обеспечения безопасности передачи данных в самоорганизующихся сетях можно использовать подход, основанный на применении моделей доверия. Использование модели доверия для определения репутации узлов позволяет изолировать узлы с низкой репутацией из сетевого взаимодействия и тем самым гарантировать безопасность передачи данных. В статье исследуется разработанная ранее репутационная модель и её имплементация для обеспечения безопасности маршрутизации на основе протокола OLSR. С целью исследования эффективности предложенного комплекса решений проведено имитационное моделирование на базе сетевого симулятора NS-3. Сценарий экспериментального исследования представлен в виде транзитной сети с некоторым количеством узлов нарушителей. В результате исследования получена экспериментальная оценка эффективности нового протокола и проведен сравнительный анализ полученных результатов.

Ключевые слова: *самоорганизующиеся сети, безопасность маршрутизации, репутационные модели, сетевые атаки, имитационное моделирование.*

Litvinov G. A.

EXPERIMENTAL ANALYSIS OF THE REPUTATIONAL MODEL FOR ROUTING IN SELF-ORGANIZING NETWORKS

To solve the problem of ensuring the security of data transmission in ad hoc networks, an approach based on the use of trust models can be used. Using the trust model to determine the reputation of nodes allows you to isolate nodes with a low reputation from network interaction and thereby guarantee the security of data transmission. The article examines the previously

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90100.

developed reputation model and its implementation to ensure routing security based on the OLSR protocol. In order to research the effectiveness of the proposed set of solutions, simulation modeling was carried out on the basis of the NS-3 network simulator. The scenario of the experimental research is presented in the form of a transit network with a certain number of intruder nodes. As a result of the research, an experimental assessment of the effectiveness of the new protocol was obtained and a comparative analysis of the results obtained was carried out. *Acknowledgments: The reported study was funded by RFBR, project number 20-37-90100.*

Keywords: *ad-hoc networks, MANET, routing security, reputation model, network attacks, network simulation.*

Введение

Различные модели и способы вычисления репутации широко применяются для самых разных задач, включая системы электронной торговли и социальные сети [1-3]. Применение репутационной модели в рамках самоорганизующейся сети позволяет избегать ненадёжные узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации [4, 5]. Установление отношений доверия между узлами сети позволяет определять узлы нарушителей и исключать их из процесса сетевого взаимодействия. Узлы, препятствующие пересылке пакетов, не должны иметь доверия у других узлов сети. Определение доверия к узлам сети производится на основе вычисления значения репутации этих узлов другими узлами сети.

Для определения доверия в рамках процесса сетевого взаимодействия была разработана новая модель, основанная на вычислении репутации каналов связи и маршрутов доставки пакетов с использованием операций булевой алгебры [6]. В рамках разработанной модели был предложен способ определения локального значения репутации каждого канала связи путём отправки тестовых пакетов. Предложенный способ позволяет узлу определить репутацию каналов связи, входящих в маршрут между узлом, который отправил тестовое сообщение и узлом, к которому оно направлено. Производя проверку каналов связи с помощью тестовых пакетов, каждый узел формирует свою локальную базу значений репутации каналов связи в сети, а также производит широковещательную рассылку этих значений другим узлам сети.

Полученные значения репутации являются локальными, поскольку определяются в пределах конкретного узла сети. Значения локальной репутации не отражают объективную оценку репутации на основе наблюдений всех узлов сети. Нередко оценка одного узла может оказаться ошибочной и расходиться с оценками других узлов. Поэтому для получения более достоверной оценки необходимо использовать значения локальной репутации, полученные от всех узлов сети. Таким образом, значение глобальной репутации некоторого канала связи формируется в результате объединения значений локальной репутации от всех узлов сети. При этом конкретный способ определения глобальной репутации зависит от используемой репутационной модели.

В рамках разработанной репутационной модели значение глобальной репутации для каждого канала связи определяется как булевозначный вектор. Формирование значения глобальной репутации r(u, v) канала связи (u, v) между узлами u и v производится, используя значения локальной репутации $r_{vi}(u, v)$ этого канала связи, определяемые всеми соответствующими узлами сети v_i:

$$r(u, v) = (r_{v1}(u, v), r_{v2}(u, v), ..., r_{vn}(u, v))$$

Применение указанной репутационной модели позволяет найти наиболее безопасные маршруты от источника до каждого узла назначения. Для этого топология сети рассматривается как булевозначная сеть [7]. При этом стоимость дуги булевозначной сети определяется значением глобальной репутацией соответствующего канала связи. Для оценки безопасности маршрутов в сети была определена соответствующая вогнутая метрика безопасности маршрутов или глобальная репутация пути. Таким образом, метрика безопасности некоторого маршрута в самоорганизующейся сети определяется как мощность соответствующего пути в булевозначной сети. То есть, наиболее безопасным является путь, все дуги которого одновременно рекомендованы максимальным количеством узлов.

Для поиска наиболее безопасных маршрутов до узлов сети был разработан соответ-

ствующий эффективный алгоритм, основанный на булевозначном представлении сети передачи данных. Учитывая вогнутую метрику безопасности маршрутов, определенную в рамках репутационной модели, указанный алгоритм позволяет находить маршруты с наилучшей репутацией, что позволяет избегать узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации.

Для имплементации, разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов был выбран протокол маршрутизации OLSR, который является базовым проактивным протоколом маршрутизации для самоорганизующихся сетей [8]. Стандартная версия протокола не содержит механизмов защиты от внутренних нарушителей и скомпрометированных узлов сети. В результате имплементации была подготовлена имитационная модель протокола маршрутизации BOLSR [9].

Предложенная имплементация предлагает расширение существующих таблиц хранения данных о состояниях каналов связи, для хранения значений репутации. Оценка каналов связи сохраняется в виде вектора, содержащего адреса устройств, рекомендующих рассматриваемый канал связи. Также были предложены два дополнительных типа сообщений. Каждый узел периодически выполняет рассылку другим узлам сети скрытых проверочных сообщений запроса ECHO, маскируемых под полезный трафик. При получении запроса ECHO, узел должен направить ECHO ответ отправителю запроса. При получении ответа, узел определяет локальную репутацию всех каналов связи, образующих маршрут до получателя, как 1. В противном случае, если ответ не был получен в течение заданного временного интервала, локальная репутация всех каналов связи, образующих маршрут до получателя, устанавливается как 0. Широковещательная рассылка значений локальной репутации выполняется посредством сообщений RM.

Предложенная модель была реализована на базе распространенного сетевого симулятора с открытым исходным кодом NS-3 [10]. В ходе программной реализации разработанного протокола маршрутизации BOLSR была поставлена задача экспериментального исследования эффективности предложенного комплекса решений посредством имитационного моделирования.

Описание эксперимента

Для указанного экспериментального исследования был предложен сценарий взаимодействия удаленных узлов с использованием транзитной самоорганизующейся сети с некоторым количеством узлов нарушителей в этой сети. В данном сценарии узел нарушителя выполняет атаку «блэкхол», действия которой вызывают отброс всех передаваемых пакетов полезных данных, в то время как передача сообщений вспомогательных сетевых протоколов, включая протоколы маршрутизации, продолжается без изменений. Оценка эффективности была выполнена на основе сравнительного анализа результатов взаимодействия узлов при использовании протоколов OLSR и BOLSR.

На рис. 1 в качестве примера представлена одна из случайных сетевых топологий, использованных в рамках эксперимента, и обозначены маршруты доставки пакетов от отправителя до получателя, выбранные при помощи протоколов OLSR и BOLSR. Пунктирной линией ограничена область расположения транзитных узлов. Следует обратить внимание, что в предложенном примере при использовании протокола OLSR был выбран маршрут доставки пакетов через узел нарушителя. При этом, при использовании BOLSR был найден альтернативный маршрут доставки пакетов. Несмотря на то, что данный маршрут может не являться кратчайшим, маршрут исключает узлы нарушителей при доставке пакетов до получателя.

Основные параметры проведенной серии экспериментов в сетевом симуляторе NS-3 представлены в табл. 1. Каждая топология транзитной сети включает 50 устройств, положение которых определяется случайным образом согласно модели симулятора «Random Rectangle Position Allocator». Проверка связности между отправителем и получателем производилась с помощью отправки сетевого трафика с постоянной скоростью передачи (Constant Bit Rate, CBR).

Результатом каждого испытания является файл трассировки, включающий информацию о всех отправленных и полученных пакетах. Анализ файла трассировки позволяет определить коэффициент доставки пакетов (Packet Delivery Ratio, PDR).

Кроме того, в ходе каждого испытания фиксировалась расширенная таблица маршрутизации узла, выполняющего отправку пакетов. Расширенная версия таблицы маршру-

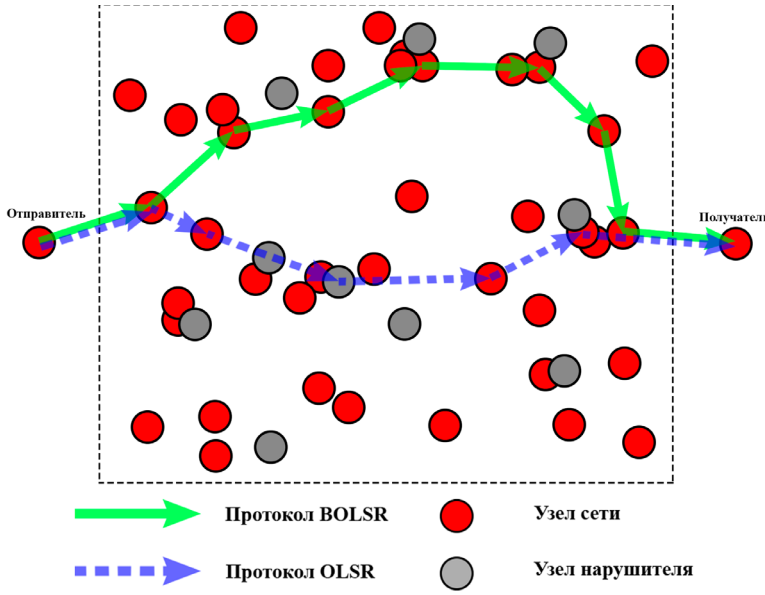

Рис. 1. Пример различного выбора маршрутов при использовании OLSR и BOLSR

Таблица 1

Предлагаемые параметры сценария эксперимента

Параметры эксперимента	Значение
Количество повторений	100
Время симуляции	180 с
Площадь расположения узлов	600м х 900м
Количество устройств в сети	52
Мобильность устройств	Статическая
Радиус взаимодействия	200 м
Протоколы маршрутизации	[OLSR, BOLSR]
Передаваемые данные	UDP
Частота отправки пакетов	1 с
Количество нарушителей	[0 - 6]
Наблюдаемые характеристики	Коэффициент доставки пакетов (Packet Delivery Ratio, PDR), Количество маршрутов через узлы нарушителей, Средняя длина маршрута

тизации, помимо адреса следующего перехода, включает также весь предполагаемый маршрут доставки пакетов до узла назначения. Полученная информация позволяет сравнить среднюю длину маршрутов до всех узлов сети, а также определить процентное отношение маршрутов, включающих узлы нарушителей. Указанные наблюдаемые характеристики позволили оценить эффективность предложенной репутационной модели поиска маршрутов и её программной реализации для имитационной модели протокола маршрутизации BOLSR.

Анализ результатов эксперимента

В результате проведения экспериментальных исследований, согласно описанному выше сценарию, была получена оценка эффективности предложенной репутационной модели для поиска маршрутов и ее программной реализации в рамках протокола BOLSR.

На рис. 2 представлены полученные графики зависимости коэффициентов доставки пакетов (Packet Delivery Ratio, PDR) от количества узлов нарушителей в транзитной сети для базового протокола маршрутизации OLSR и протокола BOLSR. Появление в транзитной сети хотя бы одного узла нарушителя приводит к тому, что некоторые из пакетов полезных данных не могут быть доставлены до получателя. Очевидно, что при увеличении количества нарушителей в транзитной сети, значение показателя PDR снижается в

любом случае. Важно, что при использовании протокола BOLSR это снижение происходит значительно медленнее по сравнению с базовым протоколом OLSR. Таким образом, по результатам экспериментальной оценки протокол BOLSR позволил повысить коэффициент доставки пакетов (на значение от 10% до 70%, в зависимости от количества нарушителей) по сравнению с базовым протоколом OLSR.

На рис. 3 представлен график зависимо-

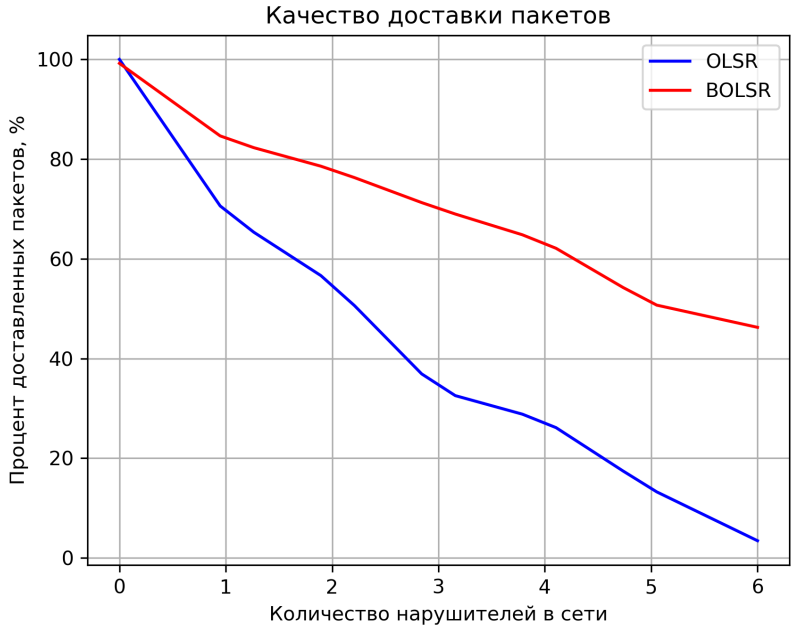

Рис. 2. Сравнение коэффициентов доставки пакетов при использовании OLSR и BOLSR

сти относительного количества маршрутов, проходящих через узлы нарушителей, от числа нарушителей. Можно отметить, что при увеличении числа узлов нарушителей в транзитной сети, относительное количество маршрутов через узлы нарушителей при использовании протокола BOLSR растёт медленнее по сравнению с базовым протоколом OLSR.

В то время как для протокола маршрутизации OLSR в качестве основной маршрутной

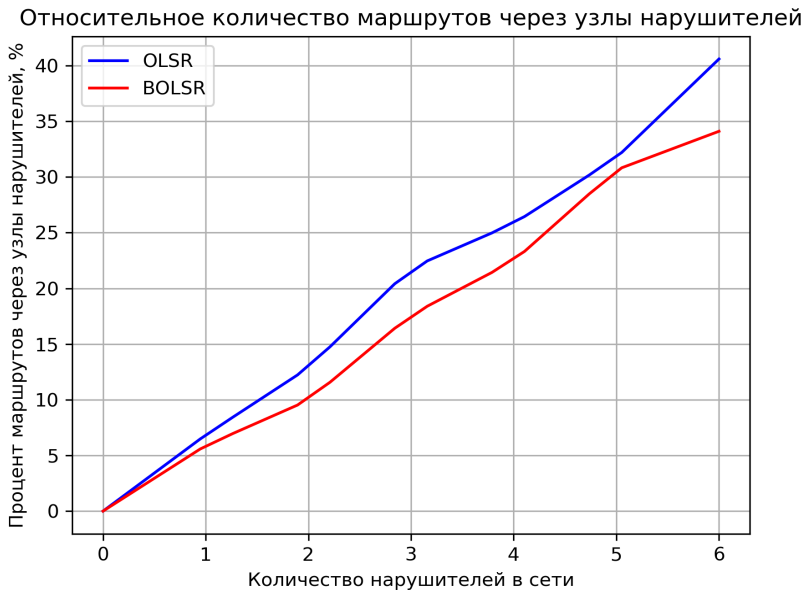

Рис. 3. Сравнение относительного количества маршрутов через узлы нарушителей при использовании OLSR и BOLSR

метрики используется количество переходов, в рамках протокола BOLSR была определена новая вогнутая метрика безопасности маршрутов, основанная на их репутации. Поскольку

маршруты с наилучшей репутацией не всегда являются кратчайшими относительно количества переходов, использование таких маршрутов может приводить к увеличению средней длины маршрутов в таблицах маршрутизации, что может негативно сказываться на других характеристиках сетевого взаимодействия, включая задержки и пропускную способность.

На рис. 4 представлен график, позволяющий оценить увеличение средней длины маршрутов до всех узлов в сети с увеличением количества нарушителей при использовании протокола BOLSR. Поскольку при использовании протокола OLSR выбор маршрутов доставки не зависит от поведения узлов сети, средняя длина маршрутов не изменяется при появлении узлов нарушителей в транзитной сети. Следует заметить, что применение протокола BOLSR вместо OLSR приводит лишь к незначительному увеличению средней длины маршрутов.

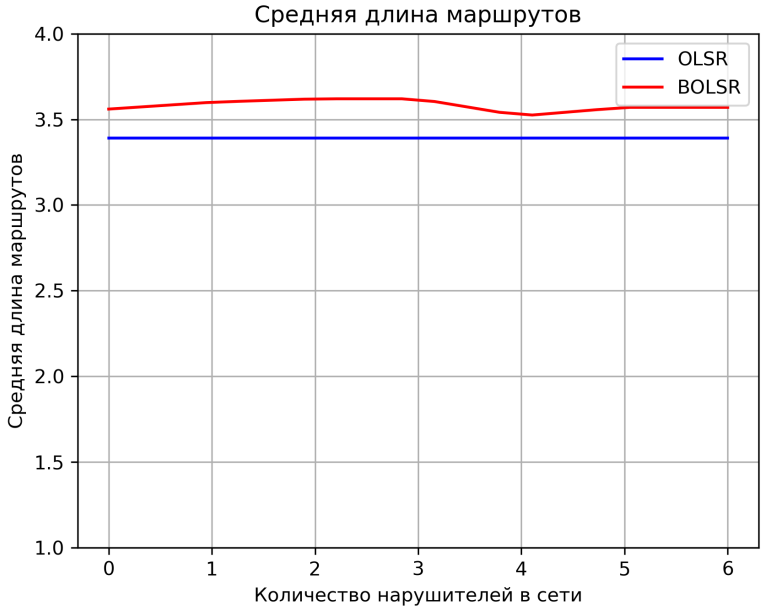

Рис. 4. Сравнение средней длины маршрутов при использовании OLSR и BOLSR

Заключение

Таким образом, в результате исследования была получена экспериментальная оценка эффективности протокола маршрутизации BOLSR для самоорганизующихся сетей, основанного на имплементации разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов для существующего протокола маршрутизации OLSR. Указанная оценка позволила провести сравнительный анализ протоколов BOLSR и OLSR на основе объективных количественных характеристик, включая коэффициент доставки пакетов, относительное количество маршрутов через узлы нарушителей и среднюю длину маршрутов.

В частности, было зафиксировано, что при увеличении числа узлов нарушителей в сети, относительное количество маршрутов через узлы нарушителей для протокола BOLSR растёт медленнее по сравнению с исходным протоколом OLSR. Кроме того, по результатам экспериментальной оценки протокол BOLSR позволил повысить коэффициент доставки пакетов по сравнению с исходным протоколом OLSR. При этом, средняя длина маршрутов при использовании BOLSR по сравнению с оригинальным протоколом OLSR увеличилась незначительно. Указанные результаты свидетельствуют о том, что применение протокола BOLSR в самоорганизующихся сетях вместо протокола OLSR позволяет минимизировать влияние сетевых атак на доступность информации и, как следствие, повысить безопасность передачи данных в этих сетях при незначительном увеличении накладных расходов.

Литература

1. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models // ACM Computing Surveys. 2018. Vol. 51, №5. P. 1–40.

2. Nosovsyi M.M., Degtiarev K.Yu. Reputation Systems in E-commerce: Comparative Analysis and Perspectives to Model Uncertainty Inherent in Them. Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS). 2019;31(3):99-122.

3. Al-Yazidi S.A., Berri J. and Hassan M.M. Novel hybrid model for organizations' reputation in online social networks. Journal of King Saud University-Computer and Information Sciences, 2022.

4. Овасапян Т.Д., Иванов Д.В. Обеспечение безопасности WSN-сетей на основе модели доверия // Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 64–72.

5. Литвинов Г.А., Щерба Е.В. Применение моделей доверия и репутации для обеспечения безопасности маршрутизации в динамически организуемых сетях // Вестник УрФО. Безопасность в информационной сфере. – 2021. – №. 3 (41). – С. 12–23.

6. Shcherba E. V., Litvinov G. A., Shcherba M. V. A novel reputation model for trusted path selection in the OLSR routing protocol //2019 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2019. – С. 1–5.

7. Салий В.Н. Оптимизация в булевозначных сетях // Дискретная математика. – 2005. – Т. 17, № 1. – С. 141–146.

8. RFC7181: The Optimized Link State Routing Protocol Version 2 / T. Clausen, C. Dearlove, P. Jacquet, U. Herberg. – 2014. – URL: https://tools.ietf.org/html/rfc7181

9. Litvinov G., Shcherba E. Implementation of the Reputation Model for Secure Routing Based on the OLSR Protocol //2021 International Conference Engineering and Telecommunication (En&T). – IEEE, 2021. – С. 1–4.

10. Свидетельство о государственной регистрации программы для ЭВМ 2021661846 Российская Федерация. Репутационный модуль поиска наиболее безопасных маршрутов для протокола маршрутизации OLSR: № 2021661027: заявл. 14.07.2021: опубл. (зарег.) 16.07.2021 / Г. А. Литвинов, Е. В. Щерба; заявитель ОмГТУ.

References

1. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models // ACM Computing Surveys. 2018. Vol. 51, №5. P. 1–40.

2. Nosovsyi M.M., Degtiarev K.Yu. Reputation Systems in E-commerce: Comparative Analysis and Perspectives to Model Uncertainty Inherent in Them. Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS). 2019;31(3):99-122.

3. Al-Yazidi S.A., Berri J. and Hassan M.M. Novel hybrid model for organizations' reputation in online social networks. Journal of King Saud University-Computer and Information Sciences, 2022.

4. 4. Ovasapyan T.D., Ivanov D.V. Obespecheniye bezopasnosti WSN-setey na osnove modeli doveriya // Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy. 2017. № 4. P. 64–72.

5. 5. Litvinov G.A., Shcherba Ye.V. Primeneniye modeley doveriya i reputatsii dlya obespecheniya bezopasnosti marshrutizatsii v dinamicheski organizuyemykh setyakh // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. – №. 3 (41). – P. 12–23.

6. Shcherba E. V., Litvinov G. A., Shcherba M. V. A novel reputation model for trusted path selection in the OLSR routing protocol //2019 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2019. – P. 1–5.

7. Saliy V.N. Optimizatsiya v bulevoznachnykh setyakh // Diskretnaya matematika. – 2005. – T. 17, № 1. – P. 141–146.

8. RFC7181: The Optimized Link State Routing Protocol Version 2 / T. Clausen, C. Dearlove, P. Jacquet, U. Herberg. – 2014. – URL: https://tools.ietf.org/html/rfc7181

9. Litvinov G., Shcherba E. Implementation of the Reputation Model for Secure Routing Based on the OLSR Protocol //2021 International Conference Engineering and Telecommunication (En&T). – IEEE, 2021. – P. 1–4.

10. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM 2021661846 Rossiyskaya Federatsiya. Reputatsionnyy modul' poiska naiboleye bezopasnykh marshrutov dlya protokola marshrutizatsii OLSR: № 2021661027: zayavl. 14.07.2021: opubl. (zareg.) 16.07.2021 / G. A. Litvinov, Ye. V. Shcherba; zayavitel' OmGTU.

ЛИТВИНОВ Георгий Александрович, аспирант кафедры комплексной защиты информации, Омский государственный технический университет, 644050, г. Омск, пр. Мира, 11. E-mail: georgyfunds@gmail.com

LITVINOV George, Graduate student, Department of Complex Information Protection, Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: georgyfunds@gmail.com

УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 76–82

Баранкова И.И., Семавина Е.А., Михайлова У.В. DOI: 10.14529/secur220309

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ, НАПРАВЛЕННЫЙ НА ОЦЕНКУ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ РОССИЙСКОГО И МЕЖДУНАРОДНОГО ЗАКОНОДАТЕЛЬСТВА

Статья посвящена аудиту информационной безопасности (ИБ) промышленных предприятий, направленному на оценку соответствия принятых мер защиты информации требованиям российского и международного законодательства. В материале поднят вопрос о необходимости проведения данного процесса и описаны его основные виды. Рассмотрены приказы ФСТЭК России, утверждающие требования к мерам защиты информации, и Национальный стандарт, содержащий указания по проведению аудита ИБ. Выделены основные вопросы и сложности проведения аудита автоматизированных систем управления технологическими процессами (АСУ ТП) и приведены рекомендации для упрощения процесса.

Ключевые слова: *информационная безопасность, аудит, критическая информационная инфраструктура (КИИ), автоматизированная система управления технологическим процессом (АСУ ТП), нормативно правовые акты (НПА).*

INFORMATION SECURITY AUDIT OF INDUSTRIAL ENTERPRISES, AIMED AT ASSESSING COMPLIANCE WITH RUSSIAN AND INTERNATIONAL LEGISLATION

The article is devoted to the audit of information security of industrial enterprises, aimed at assessing the compliance of the information protection measures taken with the requirements of Russian and international legislation. The material raises the question of the need for this process and describes its main types. The orders of the Federal Service for Technical and Export Control that approve the requirements for information security measures and the National Standard that contains instructions for information security auditing are considered. The main issues and complexities of auditing automated process control systems are highlighted and recommendations are given to simplify the process.

Keywords: *information security, audit, critical information infrastructure, automated process control system, regulatory documents.*

Информационная безопасность (ИБ) промышленных предприятий, а именно предприятий, относящихся к критическим информационным инфраструктурам (далее КИИ), является частью национальной безопасности Российской Федерации в информационной сфере. Кибератаки на информационные системы объектов КИИ могут стать причиной: аварии, экономического ущерба для предприятия и страны, угрозы жизни и здоровью сотрудников и граждан, проживающих в непосредственной близости от производства.

При обеспечении ИБ КИИ одинаково важно обеспечивать, как процессы разработки и реализации защитных мер, так и процессы проверок и контроля состояния ИБ [1]. Подобный контроль дает возможность провести проверку для установления валидности и актуальности используемых средств и систем защиты информации (СЗИ) [2].

На практике у большинства промышленных предприятий нет цельной, четко отлаженной СЗИ. Так, например, антивирусные программные средства установлены на многих АСУ ТП, чего не скажешь о системах обнаружения/предотвращения вторжений или правилах и регламентах реагирования на компьютерные инциденты. Вследствие чего возникает необходимость оценить положение дел и разобраться, какие меры по защите информации реализованы, а какие в обязательном порядке требуют немедленного внедрения.

Аудит информационной безопасности (далее аудит ИБ) способствует получению наиболее точных данных о текущем состоянии предприятия в сфере обеспечения безопасности информации [3]. Своевременное обнаружение всех возможных актуальных уязвимостей и угроз безопасности, которые могут возникнуть из-за недостатка принятых мер защищенности, позволит обеспечить построение адекватной и эффективной СЗИ, которая будет соответствовать специфике предприятия.

Аудит ИБ занимает особое положение среди процессов контроля и проверки, т.к. на данный момент для него не существует стро-

гого нормативного определения. Согласно ГОСТ Р ИСО 19011–2021 «аудит (audit): Систематический, независимый и документированный процесс установления объективного свидетельства и его объективного оценивания для получения степени соответствия критериям аудита» [4]. В области ИБ принято выделять четыре вида аудита такие как:

1. Экспертный направлен на выявление недостатков СЗИ с помощью опытных экспертов по обеспечению безопасности информации (ОБИ);

2. Оценка соответствия требованиям российского и международного законодательства. Цель настоящего аудита – выявление недостатков СЗИ посредством анализа полноты исполнения требований по ОБИ регламентов, нормативно правовых актов и законодательства;

3. Инструментальный анализ. Данный вид предполагает выявление уязвимостей программного и программно-аппаратного обеспечения исследуемой системы;

4. Комплексный аудит включает в себя все вышеперечисленные виды проведения проверки [5].

В данной статье будет рассматриваться второй, самый практичный вид аудита ИБ, в процессе которого устанавливается уровень выполнения требований регуляторов в области ИБ России (ФСТЭК России, ФСБ) и международных стандартов.

Международный стандарт ISO 19011-2021 содержит общее представление о процессе аудита ИБ – термины, принципы, этапы и способ оценки компетентности аудитора. Руководствуясь данным документом, аудитор может грамотно и полно разработать программу аудита ИБ и все необходимые организационно-распорядительные документы (далее ОРД), список и содержание которых, от первого этапа «инициирования аудита» и до седьмого «завершение аудита», так же описаны в стандарте. Данные рекомендации применимы для аудита ИБ любых информационных систем, в том числе объектов КИИ.

Конкретно для объектов КИИ ФСТЭК России разработал Приказы №31 [6] и №239[7]. Данные документы необходимы для проведения выбранного вида аудита, т.к. содержат базовые наборы требований по «обеспечению защиты информации в автоматизированных системах управления производством и технологическим процессом» (АСУП и АСУ ТП). Далее важно заметить, что выполнение требований Приказа ФСТЭК России № 239 необходимо лишь для объектов КИИ, признанных значимыми на основании проведенной процедуры по правилам категорирования утвержденным Постановлением Правительства РФ № 127[8]. Незначимые же объекты КИИ должны выполнять требования Приказа ФСТЭК России №31, а также обязанности ч.2 ст. 9 Федерального закона №187[9] (требования данного ФЗ распространяются и на значимые объекты).

Рассматриваемые приказы во многом схожи. Они формируют требования и определяют составы мер по обеспечению безопасности на всех этапах жизненного цикла АСУ ТП (при разработке, внедрении, в ходе эксплуатации и при выводе из нее).

Наименование мер защиты информации идентичны, их различие состоит в том, что для незначимых объектов перечень мер определен для каждого из уровней значимости обрабатываемой в них информации, в то время как для значимых –по трем категориям значимости.

В ходе проведения аудита ИБ, когда все обязанности уже распределены между аудиторами и разработана требующаяся предварительная ОРД, для каждого объекта КИИ создается сводная таблица с данными о выполнении (не выполнении) требований соответствующего Приказа. В случае если мера защиты выполняется, не лишним будет указать, СрЗИ или нормативный документ, который ответственен за ее перекрытие. Для СрЗИ важно отметить номер и срок действия сертификата из реестра ФСТЭК, т.к. он может быть просрочен и используемое в работе СЗИ средство необходимо будет заменить.

Кратко можно выделить основные вопросы проведения аудита, которые безусловно потребуют ответов [10]:

1. Какие силы обеспечения ИБ организованы на предприятии?

2. Какие ОРД по ОБИ (и в каком объеме/составе) разработаны и внедрены на предприятии?

3. Какие внедрены программные/ программно-аппаратные СрЗИ и каков срок действия их сертификатов?

4. Какие осуществляются, как реализованы и чем регламентированы мероприятия для обеспечения безопасности информации?

Таким образом, основная часть аудита ИБ, направленного на оценку соответствия требований законодательства, сводится к анализу таблицы, в которой собрана инфор-

мация о том, какие меры приказа выполняются, а какие нет.

В проведении подобного рода аудита для промышленных предприятий существует множество тонкостей и сложностей [11], рассмотрим некоторые из них на примере цеха ЛПЦ-10 ПАО «ММК». Материалы для статьи были собраны при прохождении производственной преддипломной практики на предприятии ПАО «ММК» г. Магнитогорск.

Первое с чем столкнутся аудиторы на рассматриваемом объекте - это сбор информации о АСУ ТП. Компоненты системы, такие как: АРМ операторов/инженеров, сервера, ПЛК компоненты полевого уровня; локализированы и располагаются, строго соответствуя документам, а различного рода сетевое оборудование (коммутаторы, хабы и т.п.) рассредоточены по разным частям цеха без какой-либо документации, регламентирующей его физическое местонахождение. Отсутствие схем и правил размещения оборудования не дает возможности аудиторам видеть сетевую архитектуру целиком, что в свою очередь затрудняет выстраивание границ между технологической сетью с ее специфической конфигурацией и стандартной корпоративной [12]. Устранение данной сложности целиком зависит от владельца предприятия и руководителя цеха, поскольку именно им необходимо инициировать процесс разработки данной технической документации. Разработанные схемы расположения сетевого оборудования поспособствуют облегчению работы не только аудиторов, но и сетевых администраторов дочерних компаний, ответственных за обеспечение работы сетевой составляющей АСУ ТП, которые выполняют свои должностные обязанности из офиса и редко посещают цех.

Отсутствие действующего специалиста по ОБИ в цехе осложняет работу аудиторов, т.к. в данном случает инициируется работа с технологами (инженерами, операторами), которые знают, как устроены технологические процессы, однако совершенно не разбираются в области информационных технологий, в частности и в информационной безопасности. В следствие человеческого фактора и не полного понимания поставленной задачи, сотрудники на местах сами неосознанно начинают тормозить процесс аудита. Данная сложность устраняется путем расширения штата персонала. В цехе необходим администратор безопасности, контролирующий и поддерживающий СЗИ.

После внедрения ФЗ РФ №187 в 2018 году руководство предприятия озаботилось разработкой организационно распорядительной и технической документации, однако в рассматриваемом цехе технические паспорта на многие объекты информатизации устарели, а ОРД разработаны не в полном объеме, требуемом ФСТЭК России. В связи с чем аудитор будет вынужден анализировать полноту выполнения требований по реализации мер безопасности информации обходя каждый объект информатизации лично. Данная сложность, как и предыдущая легко устраняется наймом администратора безопасности в конкретный цех.

Особенности построения архитектуры АСУ ТП кардинально отличают ее от привычной всем корпоративной информационной системы (КИС): начиная от специфических протоколов передачи данных (Modbus, DP, FDL, FMS), используемого оборудования (датчики, программируемые логические контроллеры, OPC сервера и др.) и программного обеспечения (SCADA, MES системы), заканчивая средой, в которой они функционируют (цеха, производственные помещения). В КИС основной защищаемый ресурс – информация, а цель – обеспечение конфиденциальности [13]. В технологических системах первостепенной задачей является сохранение непрерывности производства, которую обеспечивают доступность и целостности данных [14]. АСУ ТП имеют жестко фиксированную конфигурацию, не допускающую существенных изменений (обновления ПО, использование наложенных СрЗИ, корректировка настроек «по умолчанию») [15]. Достаточно сложно создать СЗИ, использующую СрЗИ не влияющие на технологический процесс и учитывающие специфику его работы. В условиях роста геополитической напряженности вокруг России эта и без того нетривиальная задача стала еще сложнее. К сожалению, на рынке отечественных СрЗИ недостаточно программных и программно-аппаратных средств, которые бы в полной мере покрывали все требования регулятора в области защиты информации.

Множественные кибератаки, происходящие в начале 2022 года, показали, что существует острая необходимость в обеспечении безопасности информации на объектах КИИ. Вовремя проведенный аудит ИБ позволит промышленным предприятиям сформировать стратегию защиты информации и вы-

строить наиболее полную и оптимизированную СЗИ, которая в свою очередь не допустит возникновение угроз безопасности информации, или по крайней мере значительно сократит ущерб от их реализации.

Литература

1. Санарбаев Р.Ж., Михайлова У.В. Типовые проблемы аудита информационной безопасности на примере транспортной компании ООО «АНСЕР» // Образование России и актуальные вопросы современной науки. сборник статей II Всероссийской научно-практической конференции. 2019. С. 147–151.

2. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии // Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие». Материалы конференций ГНИИ «НАЦРАЗВИТИЕ». Выпускающий редактор Ю.Ф. Эльзессер, Ответственный за выпуск С.В. Викторенкова. 2019. С. 341–345.

3. Баранкова И. И., Михайлова У. В., Быкова Т. В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии // Вестник УрФО. 2019. № 1(31). С. 53–56.

4. Национальный стандарт Российской Федерации. ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента» [Текст], Принят Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2021 г. – 2021. – 41 с.

5. Лекция 19: Аудит информационной безопасности. [Электронный ресурс] - Режим доступа: https://intuit.ru/studies/courses/600/456/lecture/10226 (Дата обращения: 20.03.2022).

6. Приказ ФСТЭК России №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (в ред. Приказов ФСТЭК России от 23.03.2017 № 49, от 09.08.2018 № 138, от 15.03.2021 № 46) [Текст], Утвержден ФСТЭК России от 14 марта 2014 г. – 2014. – 33 с.

7. Приказ ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35) [Текст], Утвержден ФСТЭК России от 25 декабря 2017 г. – 2017. – 37 с.

8. Постановление Правительства №127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изменениями от 24 декабря 2021 г.) [Текст], утверждено постановлением Правительства Российской Федерации от 8 февраля 2018 г. – 2018. – 20 с.

9. Федеральный закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Текст], Принят Государственной думой 12 июля 2017г., Одобрен Советом Федерации 19 июля 2017 г. – 2017. – 20 с.

10. Особенности проведения аудита информационной безопасности объектов критической информационной инфраструктуры [Электронный ресурс] – Режим доступа: https://www.itsec.ru/articles/osobennosti-provedeniya-audita-informacionnoj-bezopasnosti-obektov-kriticheskoj-informacionnoj-infrastruktury (Дата обращения: 20.03.2022).

11. Barankova I.I., Mikhailova U.V., Kalugina O.B. Analysis of the problems of industrial enterprises information security audit // Lecture Notes in Electrical Engineering. 2020. Т. 641 LNEE. С. 976–985.

12. Специфика защиты АСУ ТП [Электронный ресурс] – Режим доступа: http://lib.itsec.ru/articles2/asu-tp/spetsifika-zaschity-asu-tp (Дата обращения: 20.03.2022).

13. Кибербезопасность АСУ ТП – что это и зачем [Электронный ресурс] – Режим доступа: https://www.dialognauka.ru/press-center/article/13226/ (Дата обращения: 20.03.2022).

14. Где кроются реальные проблемы защиты АСУ ТП [Электронный ресурс] – Режим доступа: https://lib.itsec.ru/articles2/import/gde-kroyutsya-realnye-problemy-zaschity-asu-tp (Дата обращения: 20.03.2022).

15. Безопасность АСУ ТП [Электронный ресурс] – Режим доступа: http://www.asku.ru/services/sec_services/sec_industry/ (Дата обращения: 20.03.2022).

References

1. Sanarbaev R.ZH., Mihajlova U.V. Tipovye problemy audita in-formacionnoj bezopasnosti na primere transportnoj kompanii OOO "AN-SER" // Obrazovanie Rossii i aktual'nye voprosy sovremennoj nauki. sbornik statej II Vserossijskoj nauchno-prakticheskoj konferencii. 2019. P. 147–151.

2. Mihajlova U.V., Bykova T.V. Audit informacionnoj bezopasno-sti na predpriyatii // Sbornik izbrannyh statej po materialam nauchnyh konferencij GNII «Nacrazvitie». Materialy konferencij GNII «NACRAZVITIE». Vypuskayushchij redaktor YU.F. El'zesser, Otvetstven-nyj za vypusk S.V. Viktorenkova. 2019. P. 341–345

3. Barankova I. I., Mihajlova U. V., Bykova T. V. Slozhnosti, voznikayushchie pri provedenii audita informacionnoj bezopas-nosti na predpriyatii [Difficulties arising during the audit of information security at the enterprise]. Vestnik UrFO, 2019, no. 1(31), P. 53–56.

4. Nacional'nyj standart rossijskoj federacii. GOST R ISO 19011-2021 «Ocenka sootvetstviya. Rukovodyashchie ukazaniya po provedeniyu audita sistem menedzhmenta» [Text], Adopted by the Order of the Federal Agency for Technical Regulation and Metrology of April 21 2021 r. – 2021. – 41 P.

5. Lekciya 19: Audit informacionnoj bezopasnosti. Available a: https://intuit.ru/studies/courses/600/456/lecture/10226 (Accessed: 20.03.2022).

6. Prikaz FSTEK Rossii №31 «Ob utverzhdenii trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh siste-mah upravleniya proizvodstvennymi i tekhnologicheskimi proces-sami na kriticheski vazhnyh ob"ektah, potencial'no opasnyh ob"ektah, a takzhe ob"ektah, predstavlyayushchih povyshennuyu opas-nost' dlya zhizni i zdorov'ya lyudej i dlya okruzhayushchej prirodnoj sredy» [Tekst], Utverzhden FSTEK Rossii ot 14 marta 2014 g. – 2014. – 33 P.

7. Prikaz FSTEK Rossii №239 «Ob utverzhdenii trebovanij po obespecheniyu bezopasnosti znachimyh ob"ektov kriticheskoj in-formacionnoj infrastruktury rRossijskoj Federacii» [Tekst], Utverzhden FSTEK Rossii ot 25 dekabrya 2017 g. – 2017. – 37 P.

8. Postanovlenie Pravitel'stva №127 «Ob utverzhdenii pravil kategorirovaniya ob"ektov kriticheskoj informacionnoj infra-struktury Rossijskoj Federacii, a takzhe perechnya pokazatelej kriteriev znachimosti ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij» [Tekst], Utverzhdeno Pravitel'stvom Rossijskoj Federacii 8 fevralya 2018 g. – 2018. – 20 P.

9. Federal'nyj zakon №187 «O bezopasnosti kriticheskoj informacionnoj infra-struktury rossijskoj federacii» [Tekst], Prinyat Gosudarstvennoj dumoj 12 iyulya 2017g., Odobren Sovetom Federacii 19 iyulya 2017 g. – 2017. – 20 P.

10. Osobennosti provedeniya audita informacionnoj bezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury. Available a: https://www.itsec.ru/articles/osobennosti-provedeniya-audita-informacionnoj-bezopasnosti-obektov-kriticheskoj-informacionnoj-infrastruktury (Accessed: 20.03.2022).

11. Barankova I.I., Mikhailova U.V., Kalugina O.B. Analysis of the problems of industrial enterprises information security audit // Lecture Notes in Electrical Engineering. 2020. T. 641 LNEE. P. 976–985.

12. Specifika zashchity ASU TP. Available a: http://lib.itsec.ru/articles2/asu-tp/spetsifika-zaschity-asu-tp (Accessed: 20.03.2022).

13. Kiberbezopasnost' asu tp – chto eto i zachem? Available a: https://www.dialognauka.ru/press-center/article/13226/ (Accessed: 20.03.2022).

14. Gde kroyutsya real'nye problemy zashchity ASU TP Available a: https://lib.itsec.ru/articles2/import/gde-kroyutsya-realnye-problemy-zaschity-asu-tp (Accessed: 20.03.2022).

15. Bezopasnost' ASU TP Available a: http://www.asku.ru/services/sec_services/sec_industry/ (Accessed: 20.03.2022).

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой Информатики и информационной безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

СЕМАВИНА Екатерина Александровна, студент кафедры Информатики и информационной безопасности Магнитогорского государственного технического университета им Г.И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38, E-mail: katuxa.karlina@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и информационной безопасности Магнитогорского государственного технического университета им Г.И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38, E-mail: ylianapost@gmail.com

BARANKOVA Inna Ilyinichna, Department, Nosov Magnitogorsk State Technical University (NMSTU), D. Sc., Head of Computer Science and Information Safety Engineering (CSISE), Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru

SEMAVINA Ekaterina Alexandrovna, student, Department, Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: katuxa.karlina@mail.ru

MIKHAILOVA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security of Magnitogorsk State Technical University named after G. I. Nosova. Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com

УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 83–91

Шевяков И.А., Соколов А.Н.

DOI: 10.14529/secur220310

МЕТОД ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ КРИТИЧЕСКИХ УЗЛОВ ИНФОРМАЦИОННОЙ СЕТИ ТРАНСПОРТНОГО СРЕДСТВА[1]

В статье предложен метод определения уровня защищённости к кибератакам узлов информационной сети транспортного средства, функционирование которых важно для безопасности дорожного движения. Метод основан на применении математического аппарата И/ИЛИ графов для моделирования операционных зависимостей в узлах информационной сети. Приведен перечень угроз, актуальных для информационной сети транспортного средства, и средств защиты информации, применяемых в сетях такого типа. Оценка уровня защищённости проводится для типовой сети транспортного средства, содержащей несколько электронных блоков управления. Сделан вывод об эффективности разработанного метода.

Ключевые слова: *информационная безопасность, защита информации, информационная сеть транспортного средства, подключенное транспортное средство, электронный блок управления (ЭБУ), И/ИЛИ граф, гиперграф, средство защиты информации (СЗИ), кибератака, кибербезопасность.*

Sheviakov I.A., Sokolov A.N.

METHOD FOR DETERMINING THE LEVEL OF SECURITY OF CRITICAL NODES OF THE INFORMATION NETWORK OF A VEHICLE

The article proposes a method for determining the levels of protection against cyberattacks of vehicle information network nodes, the functioning of which is important for road safety. The method based on the use of the mathematical apparatus of AND/OR graphs for modeling operational dependencies in the nodes of the information network. A list of threats relevant to the

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ МТУСИ) в рамках научного проекта № 40469-25/2021-К.

information network of the vehicle, and information protection tools used in networks of this type is given. The security level assessed for a typical vehicle network containing several electronic control units. A conclusion made about the effectiveness of the developed method.

Keywords: *Information security, information security, vehicle information network, connected vehicle, electronic control unit (ECU), AND/OR graphs, hypergraphs, information security tools, cyberattack, cybersecurity.*

Введение

Большинство современных моделей транспортных средств (ТС) в значительной степени компьютеризированы и имеют возможность подключения через внешние беспроводные сети к другим ТС, придорожным приборам, мобильным устройствам и сервисным центрам производителей оригинального оборудования (OEM производителей) [1]. Ввиду наличия большого количества угроз информационной безопасности (ИБ) в этих сетях, компьютерная и сетевая безопасность требует защиты всех компонентов инфраструктуры на нескольких уровнях [2]. Внутренние и внешние информационные сети всех ТС, а также дорожная информационная инфраструктура («умные светофоры», «умные знаки», системы управления дорожным движением и т.д.) являются частью критической информационной инфраструктуры (КИИ) системы дорожного движения города, следовательно, должны приниматься соответствующие меры по защите информации. Обеспечение большей части этих мер должно закладываться в информационные системы ещё на этапе проектирования.

На информационных ресурсах имеется много публикаций о кибератаках на автомобильные системы, некоторые из которых попали под пристальное внимание средств массовой информации [3], что привело к ущербу репутации производителей автомобилей.

Помимо ущерба репутации, стоимость обеспечения кибербезопасности стала значительной проблемой для производителей автомобилей. Обнаружение уязвимостей узлов информационных сетей транспортных средств (ИСТС) привело к постоянному увеличению количества отзывов автомобилей для устранения неисправностей. Так, в 2010 году Чарли Миллер и Крис Валасек [4] продемонстрировали концепцию удаленных атак, взяв под контроль джип и отправив его в бездорожье, что вызвало отзыв 1,4 миллиона автомобилей. Исследователи безопасности взломали электронную систему BMW Connected Drive и смогли удаленно разблокировать автомобили, что оказало еще большее влияние на промышленность – было отозвано 2,2 миллиона автомобилей [5]. Подобные угрозы информационной безопасности оказывают значительное влияние на безопасность дорожного движения и конфиденциальность персональных данных пассажиров и других граждан.

Из описанных выше примеров следует, что при проектировании ТС особое внимание должно уделяться безопасности информации как на уровне всей информационной сети в целом, так и на уровне отдельных узлов и подсистем. Для этого необходимо на этапе проектирования обладать информацией о необходимых мерах защиты, которые требуется применить в информационной сети каждого конкретного разрабатываемого транспортного средства, чтобы обеспечить требуемый уровень безопасности информации, передающейся по внутренней сети ТС.

Вопросы, связанные с исследованием и классификацией угроз безопасности информации в сети ТС, рассмотрены в работах Juan Deng [2] и Florian Sommer, Jürgen Dürrwang [6]. Авторами представлена классификация для описания атак на информационные системы ТС, а также предложены методы защиты от таких вредоносных воздействий, как в рамках отдельного узла, так и в рамках системы в составе информационной сети ТС.

Применению математических методов и алгоритмов анализа защищённости информации в сетях технических объектов и идентификации критических узлов в сложных сетях посвящено множество работ, среди которых необходимо отметить труды Martín Barrère, Chris Hankin [7]. Авторы представили методику оценки уровня информационной безопасности, направленную на определение критических киберфизических компонентов и измерение общей безопасности сетей АСУ ТП. В основе подхода к созданию методики лежит использование моделей на основе графов И/ИЛИ, позволяющее исследовать зависимости между компонентами промышленных сетей.

Используя подходы, предложенные в [2, 6, 7, 8], разработан метод определения уровня защищённости критических узлов ИСТС. При разработке метода определен перечень актуальных угроз безопасности информации в сети ТС и типовой состав узлов и подсистем сети ТС.

Типовая архитектура информационной сети транспортного средства

Большинство архитектур ИСТС включают нескольких систем, связанных между собой центральным шлюзом (рис. 1). Системы отвечают за различные функциональные характеристики компонентов ТС. При компрометации этих компонентов могут появиться риски нарушения ИБ. Влияние этих рисков на безопасное, для дорожного движения, функционирование ТС может варьироваться. По этой причине, критичные для безопасности дорожного движения, компоненты ТС требуют соответствующей защиты.

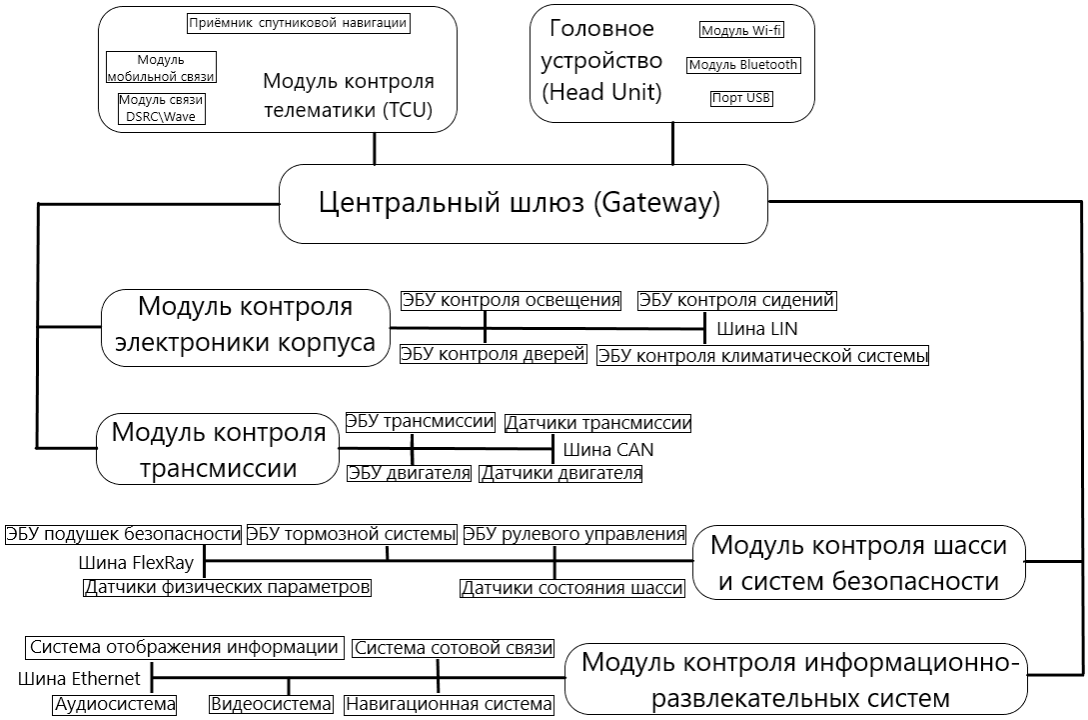

Рис. 1. Структура информационной сети транспортного средства

Компоненты разделяются по следующим категориям:

– управление трансмиссией;

– управление шасси;

– контроль корпуса;

– управление информационно-развлекательной системой;

– контроль коммуникаций;

– системы диагностики и обслуживания.

Угрозы, актуальные для информационной сети транспортного средства

Для представления основных задач информационной безопасности, актуальных для информационной сети транспортного средства, рассмотрены угрозы, которые могут возникнуть при эксплуатации и обслуживании транспортных средств. Большая часть угроз безопасности информации в ИСТС описана в базе данных Automotive Attack Database (AAD) [6], разработанной в университете Карлсруэ. База данных предлагает схему классификации для описания автомобильных атак безопасности в виде единой таксономии. Чтобы иметь возможность использовать описания атак на нескольких этапах разработки в качестве источника информации, атаки представлены с различным уровнем детализации.

Все угрозы, актуальные для ИСТС, можно объединить в несколько групп.

Угрозы потери информации:

– угроза потери информации в облаке;

– угроза потери целостности конфиденциальной информации;

– угрозы потери информации от конфликтов DRM.

Угрозы возникновения сбоев и неисправностей:

– угроза сбоя или перебоев в электроснабжении;

– угроза наличия критических программных ошибок;

– угроза сбоя или нарушения работы каналов связи.

Угрозы перехвата и подделки сообщений сети:

– угроза перехвата информации через побочные электромагнитные излучения;

– угроза подделки сообщений сети;

– угроза «человек посередине» (MitM).

Угрозы вредоносного воздействия на информационную сеть:

– угроза отказа в обслуживании;

– угроза манипуляции с аппаратным и программным обеспечением, манипулирования информацией;

– угроза несанкционированного доступа к информационной системе/сети;

– угроза компрометации конфиденциальной информации;

– угроза действия вредоносного программного обеспечения;

– угроза удаленного исполнения кода.

Для противодействия угрозам информационной безопасности в сети транспортного средства используются меры обеспечения ИБ, которые применяются и к компьютерным информационным сетям, но модифицируются с учётом специфики используемых протоколов и алгоритмов работы устройств, а также требований надёжности и быстродействия. Все меры защиты условно можно поделить на две категории – программные и аппаратные.

Программные меры защиты информации в сети ТС:

– обфускацию кода;

– использование криптографических методов;

– ловушки руткитов.

Аппаратные меры защиты информации в сети ТС:

– использование системы обнаружения вторжений;

– применение межсетевого экрана на центральном шлюзе и других критически важных узлах.

Методика оценки уровня уязвимости узлов ИСТС

Автомобильную информационную сеть W можно представить как ориентированный И/ИЛИ граф G = (V, E), который представляет взаимодействия между узлами в W (рис. 2). Граф включает три типа базовых вершин, называемых атомарными узлами (V_{AT}), которые моделируют различные компоненты сети: S представляет набор узлов датчиков, C представляет набор узлов исполнительных механизмов, а A представляет набор программных агентов (работающих, например, в ЭБУ и TCU). V_{AT} определяется как: $V_{AT} = S \cup C \cup A$. Кроме того, граф также включает два типа искусственных узлов, которые моделируют логические зависимости между компонентами сети: Δ представляет собой набор логических узлов И, а Θ представляет собой набор узлов логического ИЛИ. Набор всех узлов графа определяется как $V(G) = VAT \cup \Delta \cup \Theta$. E(G) является набором ребер между узлами, и их семантика зависит от типа узлов, которые они соединяют.

Меры защиты, применяемые в информационных сетях транспортного средства, могут применяться сразу к нескольким узлам сети, поэтому могут быть представлены как дополнительный уровень над графом логических зависимостей информационной сети транспортного средства. Множество задействованных мер безопасности Mi определяется как $S = \{s_1, s_2, ...\}$.

Гиперребра объединяют каждый сетевой узел с мерами безопасности, которые используются для их защиты. Таким образом, можно следовать той же логической структуре, что и в исходном графе, и объединять эти суперузлы с помощью связок И/ИЛИ, как показано на рис. 3.

Рассмотрим проблему с логической точки зрения, следовательно, с точки зрения выполнимости.

Решение задачи максимальной выполнимости для описанного логического представления информационной сети транспортного средства, где веса задаются функциями $\phi(n)$ для каждого узла $n \in Vr$ и q(s) для каждой меры безопасности $s \in S$, состоит из нескольких этапов:

1. Операционные зависимости представляются в подсистеме в виде логических зависимостей типа И/ИЛИ графа G.

2. Зависимости графа G преобразуются в эквивалентное логическое представление g(x).

3. Зависимость g(t) преобразуется в новую форму k(t), где каждый не виртуальный узел сети $n \in Vr$ в g(x) заменяется на $(n \vee s_i \vee ... \vee s_j)$, где $s_i \vee ... \vee s_j$ — это дизъюнкция мер безопасности, которые защищают узел n.

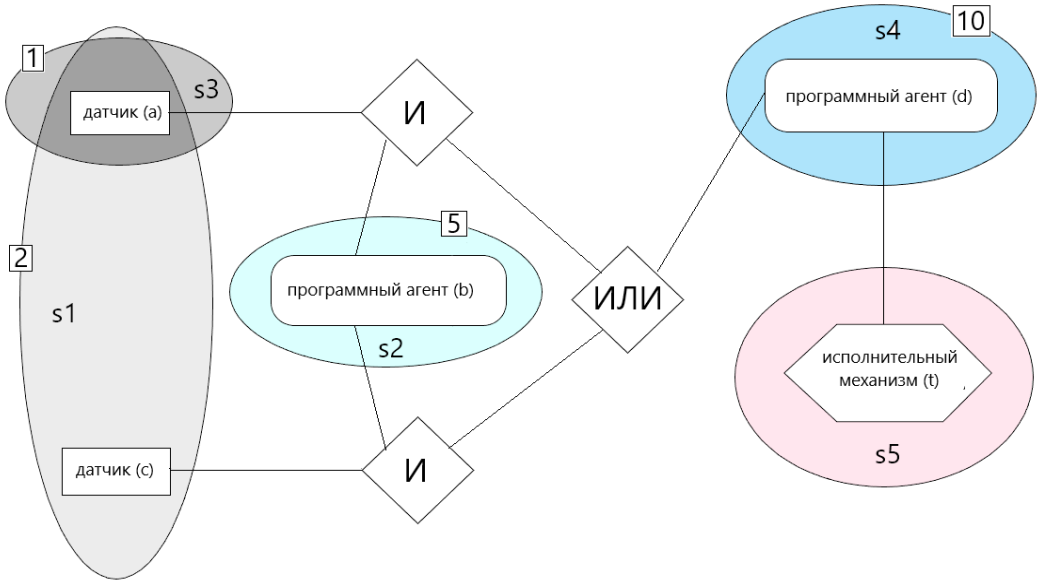

Рис. 2. Участок информационной сети в виде И/ИЛИ графа с перекрывающимися мерами безопасности

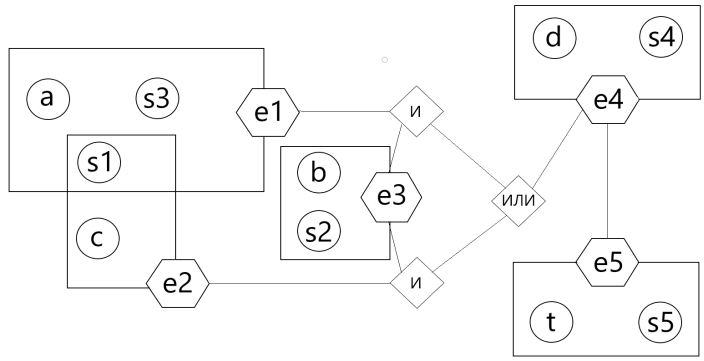

Рис. 3. Представление узлов сети (a, b, c, d, c1) и мер безопасности (s1, s2, s3, s4, s5) в виде рёбер гиперграфа И/ИЛИ (e1, e2, e4, e5)

4. Цель атакующего ¬k(t) преобразуется в конъюнктивную нормальную форму (КНФ) с помощью преобразования Цейтина, т. е. G(x) = КНФ (¬g(x)), где $g(x) = (v_{1i} \vee ... \vee v_{1j}) \wedge ... \wedge (v_{hi} \vee ... \vee v_{hj})$.

5. Определяется мягкое предложение для каждого невиртуального узла $n \in V_r$ и каждой меры безопасности $s \in S$ и присваиваем им веса (n, w(n)) и (s, q(s)) соответственно.

Оценка защищённости узлов

Для реализации метода разработано программное обеспечение (ПО), в основу которого положен обобщённый алгоритм решения задачи максимальной выполнимости. Функционально ПО состоит из трёх вычислительных модулей, модуля отображения результата, модуля чтения исходных данных и модуля формирования результата. Модуль расчёта показателей основан на решателе META4ICS [9], используемом для анализа защищённости сетей АСУ ТП.

Результаты, представленные в табл. 1, представляют собой список узлов и экземпляров мер защиты (М1 – М6) для информационной сети ТС, представленной на рис. 1, каждая система которой представлена в виде И/ИЛИ графа (рис. 4), которые необходимо применить к этим узлам, чтобы затраты злоумышленника на преодоления данного узла были максимальны. Затраты злоумышленника, необходимые для преодоления системы защиты в расчитанной конфигурации, приведены в третьем столбце табл. 1.

Полученные данные о количестве и виде защитных мер можно использовать в системах автоматизированного проектирования, а также вносить в спецификации выпускаемых изделий.

Оценка быстродействия и эффективности метода

Для оценки быстродействия предложенного подхода проведён набор эксперимен-

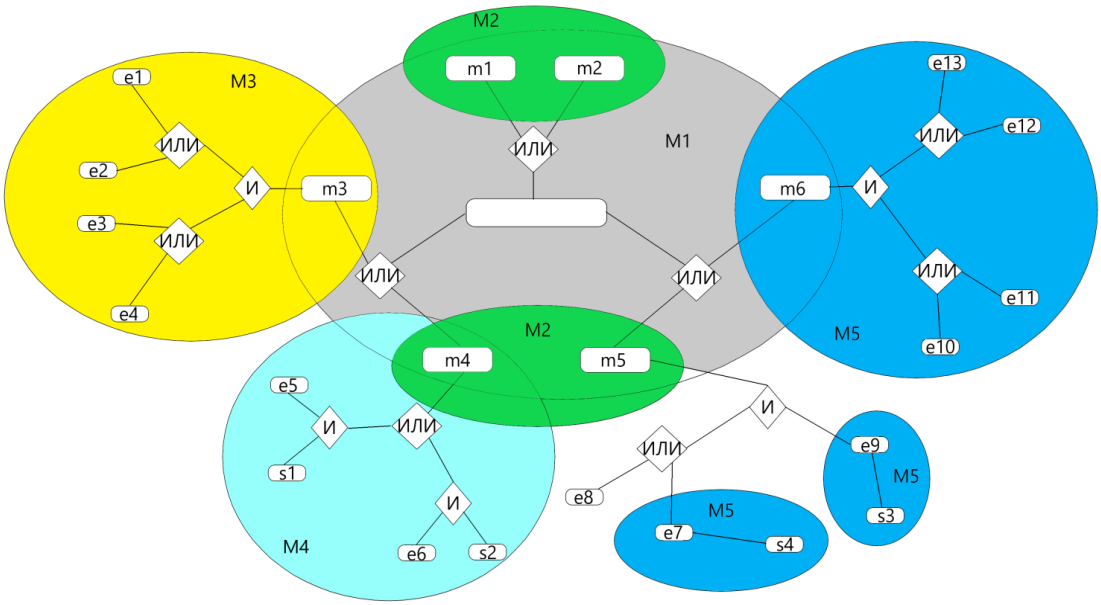

Рис. 4. Модель распределения средств защиты в типовой информационной сети ТС (e1…e13 – ЭБУ, s1… s4 – датчики, m1 … m6 – модули)

Таблица 1

Список мер защиты для каждого из компонент подсистемы

Мера защиты	Тип меры защиты	Затраты на преодоление	Защищаемые узлы
M1	M1	1	m1, m2, m3, m4, m5, m6
M2-1	M2	1	m1, m2
M2-2	M2	2	m4, m5
M3	M3	4	e1, e2, e3, e4, m3
M4	M4	4	e5, e6, s1, s2, m4
M5-1	M5	3	e7, s4
M5-2	M5	3	e9, s3
M5-3	M5	2	e10, e11 e12, e13, m6

тов, основанных на синтетических псевдослучайных графах И/ИЛИ разного размера и состава.

Эти эксперименты проводились на системе с процессором AMD Ryzen 5 5600 3,7 ГГц, 32 ГБ памяти DDR4 2400 МГц. Процедура построения графа И/ИЛИ размера n выглядит следующим образом.

На рис. 5 показано поведение методологии на взвешенных графах И/ИЛИ, когда размер входного графа увеличивается. В этом эксперименте создаются псевдослучайные графы И/ИЛИ размера n и композиционной конфигурации (60, 20, 20). Размер n изменяется как $n \in [0, 500, 1000, 1500, \ldots, 20000]$, и процесс оценки повторяется 10 раз для каждого значения n.

Для графов с 10 000 узлов среднее время разрешения составляет около 3 секунд, а для графов с 20 000 узлов среднее время составляет около 15 секунд. В целом время преобразования Цейтина стабильно на всех итерациях, процесс разрешения MAX-SAT требует больше времени для решения проблемы на одних графах, чем на других. Это происходит из-за того, что некоторые графы дают формулы с более длинными последовательностями операторов И или ИЛИ, соединяющих различные комбинации узлов графа, что требует переменного времени вычислений. Получен-

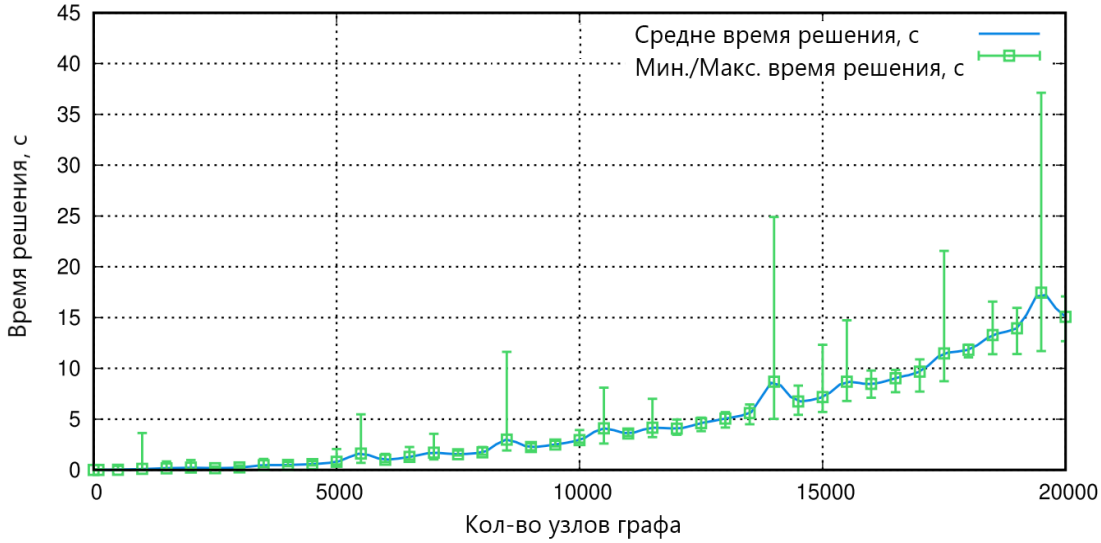

Рис. 5. Результаты измерения производительности при масштабируемости размера графа до 20000 узлов

ные результаты показывают, что представленный подход может эффективно масштабироваться до больших графов И/ИЛИ, включающих тысячи узлов, защищенных несколькими мерами безопасности.

Для оценки эффективности разработанного метода, сравним эффективность определения уязвимостей критических узлов системы защиты информации информационной сети ТС (СЗ ИСТС) при использовании предложенного программного средства и при выполнении этой работы традиционными методами. Для сравнения применён метод многокритериального анализа альтернатив Беллмана-Заде. Полученное отношение множеств $P_2 / P_1 = 1{,}47$ позволяет сделать вывод, что применение разработанного ПО делает процесс оценки уязвимостей СЗ ИСТС в полтора раза более эффективным.

Заключение

В работе приведён обобщённый метод определения защищённости узлов, состоящий из пяти этапов, позволяющий применять его для сети любого размера. Однако необходимо учитывать, что для большого количества узлов возможно существенное снижение производительности вычислений.

Разработано программное средство расчёта конфигурации мер защиты информации в ИСТС. Проведён анализ производительности программного комплекса на различных конфигурациях модельных сетей с разным количеством, атомарных и виртуальных узлов.

Полученные в ходе работы результаты могут быть использованы при проектировании СЗИ ИСТС и при моделировании инцидентов ИБ на специализированных стендах [10].

Литература

1. What Is an OEM? [Электронный ресурс]. – Режим доступа: https://www.cars.com/articles/what-is-an-oem-1420696948647/, свободный (дата обращения: 01.09.2022 г.).

2. Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, Richard R. Brooks, Chapter 6 – Security and Data Privacy of Modern Automobiles // Data Analytics for Intelligent Transportation Systems, Elsevier, 2017, P. 131–163.

3.WIRED: Car Hacking. [Электронный ресурс]. – Режим доступа: https://www.wired.com/tag/car-hacking/, свободный (дата обращения: 01.09.2022 г.).

4. Charlie Miller, Chris Valasek. Adventures in Automotive Networks and Control Units. [Электронный ресурс]. – Режим доступа: https://illmatics.com/car_hacking.pdf, свободный (дата обращения: 01.09.2022 г.).

5. Beemer, Open Thyself! – Security vulnerabilities in BMW's Connected Drive [Электронный ресурс]. – Режим доступа: https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html, свободный (дата обращения: 01.09.2022 г.).

6. Sommer F, Dürrwang J, Kriesten R. Survey and Classification of Automotive Security Attacks. Information. 2019; 10 (4):148. https://doi.org/10.3390/info10040148.

7. Martín Barrère, Chris Hankin, Nicolas Nicolaou, Demetrios G. Eliades, Thomas Parisini, Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies // Journal of Information Security and Applications, Volume 52, 2020, 102471, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102471.

8. A. Barinov, N. Davydkin, D. Sharova and S. Skurlaev, "Prioritization methodology of computing assets for connected vehicles in security assessment purpose," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), 2019, pp. 1–6.

9. M. Barrère. META4ICS – metric analyser for industrial control systems. [Электронный ресурс]. – Режим доступа: https://github.com/mbarrere/meta4ics, свободный (дата обращения: 01.09.2022 г.).

10. Шевяков И. А., Соколов А. Н. Концепция стенда для исследования кибербезопасности устройств на шине FlexRay «подключенного» транспортного средства, основанная на использовании интерфейсных плат // Вестник УрФО: Безопасность в информационной сфере. – Челябинск: Изд-во Южно-Уральский юридический вестник. – 2019. – №3(33) – С.73–81.

References

1. What Is an OEM? [Online]. – Rezhim dostupa: https://www.cars.com/articles/what-is-an-oem-1420696948647/, svobodnyj (data obrashhenija: 01.09.2022).

2. Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, Richard R. Brooks, Chapter 6 - Security and Data Privacy of Modern Automobiles // Data Analytics for Intelligent Transportation Systems, Elsevier, 2017, P. 131–163.

3. WIRED: Car Hacking. [Online]. – Режим доступа: https://illmatics.com/car_hacking.pdf, свободный (дата обращения: 01.08.2022 г.)

4. Charlie Miller, Chris Valasek. Adventures in Automotive Networks and Control Units. [Online]. – Rezhim dostupa: https://illmatics.com/car_hacking.pdf, svobodnyj (data obrashhenija: 01.09.2022).

5. Beemer, Open Thyself! – Security vulnerabilities in BMW's Connected Drive [Online]. – Rezhim dostupa: https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-Connected Drive-2540957.html, svobodnyj (data obrashhenija: 01.09.2022).

6. Sommer F, Dürrwang J, Kriesten R. Survey and Classification of Automotive Security Attacks. Information. 2019; 10 (4) :148. https://doi.org/10.3390/info10040148.

7. Martín Barrère, Chris Hankin, Nicolas Nicolaou, Demetrios G. Eliades, Thomas Parisini, Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies // Journal of Information Security and Applications, Volume 52, 2020, 102471, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102471.

8. A. Barinov, N. Davydkin, D. Sharova and S. Skurlaev, "Prioritization methodology of computing assets for connected vehicles in security assessment purpose," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), 2019, pp. 1–6.

9. M. Barrère. META4ICS – metric analyser for industrial control systems. [Online]. – Rezhim dostupa: https://github.com/mbarrere/meta4ics, svobodnyj (data obrashhenija: 01.09.2022).

10. Sheviakov I. A., Sokolov A. N. Koncepcija stenda dlja issledovanija kiberbezopasnosti ustrojstv na shine FlexRay «podkljuchennogo» transportnogo sredstva, osnovannaja na ispol'zovanii interfejsnyh plat // Vestnik UrFO: Bezopasnost' v informacionnojsfere. – Chelyabinsk: Izd-vo Juzhno-Ural'skij juridicheskij vestnik. – 2019. – №3(33) – P. 73–81.

ШЕВЯКОВ Игорь Андреевич, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: regnlager@yandex.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

SHEVIAKOV Igor Andreevich, PhD student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: regnlager@yandex.ru

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76, ЮУрГУ,
Издательский центр

ВЕСТНИК УрФО
Безопасность в информационной сфере № 3(45) / 2022
Подписано в печать 30.09.2022. Дата выхода в свет 11.10.2022.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 8,4. Тираж 50 экз.
Заказ 00/000.
Цена свободная.

Отпечатано в типографии Издательского центра ФГАОУ ВО "ЮУрГУ (НИУ)".
454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 3(45) / 2022
Signed to print 30.09.2022. Date of publication of the 11.10.2022.
Format 70×108 1/16. Screen printing. Conventional printed sheet 8,4. Circulation – 50 issues.
Order 00/000.
Open price.

Printed in the printing house of the Publishing Center of FGAOU VO "SUSU (NIU)".
SUSU, Publishing Center, 76, Lenina Str., Chelyabinsk, 454080