

# Лабораторная работа №1. ЗАЩИТА ДАННЫХ СЕГМЕНТА АСУ ТП

Дисциплина: Кибербезопасность предприятия

---

Астраханцева Анастасия Ганина Таисия Ибатулина Дарья Шошина Евгения Кадирова Мехрубон  
Хассан Факи Абакар

30 сентября 2025

Группа НФИбд-01-22

Российский университет дружбы народов, Москва, Россия

## Вводная часть

---

## Цели и задачи

---

Целью лабораторной работы является изучение методов обнаружения, анализа и устранения последствий компьютерных атак в сегменте автоматизированных систем управления технологическим процессом (АСУ ТП) на базе программного комплекса “Ampire”. Работа направлена на формирование навыков защиты данных от внешних нарушителей, использующих уязвимости в программном обеспечении, и освоение инструментов мониторинга сетевой безопасности, таких как ViPNet IDS NS, ViPNet TIAS и Security Onion.

## Задание

---

1. Изучить типовые уязвимости, используемые при атаке на сегмент АСУ ТП.
2. Проанализировать последовательность действий нарушителя на каждом этапе атаки.
3. Освоить методы детектирования атак с использованием средств мониторинга и анализа безопасности.
4. Выполнить мероприятия по устранению последствий атаки.
5. Отработать навыки анализа сетевых соединений и процессов с помощью стандартных утилит.

## Заполнение карточек инцидентов

---

Для обнаружения и анализа атак использовались средства ViPNet IDS NS. Были зафиксированы следующие ключевые инциденты, соответствующие этапам атаки

The screenshot shows the 'Основная информация' (Main Information) tab selected in the header. The main content area contains several sections: 'Дата и время события' (Event Date and Time) showing '16.09.2025 09:39'; 'Описание' (Description) detailing a 'Несанкционированный доступ к файлам и приложениям, AM EXPLOIT Generic Path Traversal in HTTP URI var 21'; 'Индикаторы компрометации' (Compromise Indicators) listing 'web-application-attack'; 'Рекомендации' (Recommendations) suggesting to 'Обновить axis2, добавить правило в iptable для блокировки доступа к конфигурационному файлу'; and 'Прикреплённые файлы' (Attached Files) showing 'IDS\_packet\_time-2025-09-16T06\_39\_23.332563Z\_ruleid-3106358.pcap'. On the right side, there is a sidebar with a rating section ('Оценка' with 5 stars), author information ('Автор' - Ибатуллина Дарья, ID 1132226434@pfur.ru), responsible person ('Ответственный' - Ганина Твягин, ID 1132226429@pfur.ru), and source information ('Источник' - 196.239.174.11). A 'В работе' (In Progress) button is also visible.

Рис. 1: Получение доступа через уязвимый Apache Axis 2

« AM EXPLOIT Generic Command Injection in HTTP URI: 'netcat' in request

Основная информация Чат Новый

Дата и время события ①  
16.09.2025 09:39

Описание ①  
Зафиксирован HTTP-запрос к веб-серверу. Попытка выполнить командную инъекцию/удалённый запуск утилиты

Индикаторы компрометации ①  
web-application-attack

Рекомендации ①  
Изолировать хост, заблокировать источник, проверить процессы/соединения и завершить подозрительные, сменить пароли и ключи, обновить веб-приложение и компоненты

Прикреплённые файлы ①  
IDS\_packet\_time-2025-09-16T06\_39\_39.6888936Z\_ruleid-3111399.pcap

Оценка  
☆ ☆ ☆ ☆ ☆

Автор  
Ибатуллина Даирей  
@132226434@pfur.ru

Ответственный  
Не заполнено

Источник  
195.238.174.11

Поражённые активы  
10.10.1.24

Рис. 2: AM EXPLOIT Generic Command Injection in HTTP URI

< AM POLICY Apache Axis2 v1.6 Default Admin Credential (CVE-2010-0219)

Основная информация Чат Новый

Дата и время события ⓘ  
16.09.2025 09:39

Описание ⓘ  
Уязвимая версия axis2 установлена на AppServer под управлением Apache Tomcat. В типовом шаблоне информационной системы используется для развертывания веб-сервисов, работает через порт 80

Индикаторы компрометации ⓘ  
attempted-admin

Рекомендации ⓘ  
- Настройка правила в iptables, которое отказывает в доступе к конфигурационному файлу при наличии в заголовке строки axis2.xml; - Обновить axis2 до последней версии.

Прикреплённые файлы ⓘ  
IDS\_packet\_time-2025-09-16T06\_39\_45.884269Z\_ruleid-3006394.pcap

Оценка  
☆ ☆ ☆ ☆ ☆

Автор  
ИД Ибатуллина Даюя  
@132226434@phur.ru

Ответственный  
Не заполнено

Источник  
199.239.174.11

Пораженные активы  
10.10.1.24

The screenshot shows a detailed view of a security incident report. At the top, there's a back arrow and the title 'AM POLICY Apache Axis2 v1.6 Default Admin Credential (CVE-2010-0219)'. Below the title, there are two tabs: 'Основная информация' (Main information) and 'Чат' (Chat), with 'Основная информация' being the active tab. A green button labeled 'Новый' (New) is located in the top right corner. The main content area is divided into several sections: 'Дата и время события' (Event date and time) showing '16.09.2025 09:39'; 'Описание' (Description) detailing the vulnerability of Axis2 version 1.6 on an AppServer running Apache Tomcat; 'Индикаторы компрометации' (Compromised indicators) listing 'attempted-admin'; 'Рекомендации' (Recommendations) with instructions for iptables configuration and axis2 update; and 'Прикреплённые файлы' (Attached files) showing a pcap file named 'IDS\_packet\_time-2025-09-16T06\_39\_45.884269Z\_ruleid-3006394.pcap'. On the right side, there are additional details: 'Оценка' (Rating) with five stars, 'Автор' (Author) with user 'Ибатуллина Даюя' and ID '132226434@phur.ru', 'Ответственный' (Responsible) listed as 'Не заполнено' (Not filled), 'Источник' (Source) with IP '199.239.174.11', and 'Пораженные активы' (Affected assets) with IP '10.10.1.24'.

Рис. 3: AM POLICY Apache Axis2 v1.6 Default Admin Credential

◀ ET TROJAN Possible Metasploit Payload Common Construct Bind\_API (from server)

Основная информация Чат Новый

Дата и время события ⓘ  
16.09.2025 09:52

Описание ⓘ  
Возможная активность трояна / Metasploit bind-payload — подозрительный байт-контент в ответе сервера (Client Endpoint)

Индикаторы компрометации ⓘ  
trojan-activity

Рекомендации ⓘ  
Изолировать заражённый хост от сети, заблокировать источник через iptables, ограничить исходящий трафик заражённого узла, завершить подозрительные соединения, провести антивирусное сканирование, удалить или восстановить систему из чистой резервной копии, сменить все пароли и ключи, установить обновления ОС и приложений

Прикреплённые файлы ⓘ  
IDS\_packet\_time-2025-09-16T06\_52\_31.569047Z\_ruleid-2025644.pcap

Оценка  
☆ ☆ ☆ ☆ ☆

Автор  
ИД: Ибатуллина Даира  
@1152226434@pfir.ru

Ответственный  
Не заполнено

Источник  
195.239.174.11

Поражённый актив  
10.10.1.253

The screenshot displays a detailed threat intelligence report. At the top, there's a navigation bar with back, forward, and search icons, followed by the title 'ET TROJAN Possible Metasploit Payload Common Construct Bind\_API (from server)'. Below the title, there are tabs for 'Основная информация' (Main Information) and 'Чат' (Chat), with 'Основная информация' being the active tab. A green button labeled 'Новый' (New) is located in the top right corner. The main content area is divided into several sections: 'Дата и время события' (Event Date and Time) showing '16.09.2025 09:52'; 'Описание' (Description) containing the note about possible Metasploit bind-payload; 'Индикаторы компрометации' (Indicators of Compromise) listing 'trojan-activity'; 'Рекомендации' (Recommendations) providing guidance on isolation and system recovery; and 'Прикреплённые файлы' (Attached Files) showing a pcap file named 'IDS\_packet\_time-2025-09-16T06\_52\_31.569047Z\_ruleid-2025644.pcap'. To the right of the main content, there's a sidebar with sections for 'Оценка' (Rating) with five stars, 'Автор' (Author) with the ID 'ИД: Ибатуллина Даира' and email '@1152226434@pfir.ru', 'Ответственный' (Responsible) marked as 'Не заполнено' (Not filled), 'Источник' (Source) with the IP '195.239.174.11', and 'Поражённый актив' (Affected host) with the IP '10.10.1.253'. The entire interface has a dark theme.

Рис. 4: ET TROJAN Possible Metasploit Payload Common Construct Bind\_API

◀ Уязвимая версия IGSS AM Exploit 7T Interactive Graphical SCADA Buffer Overflow 0d

Основная информация Чат В работе

Дата и время события ⓘ  
16.09.2025 09:52

Описание ⓘ  
Переполнение стека в программе с графическим интерфейсом IGSSdataServer.exe при использовании операции ListAll ведет к удаленному выполнению кода и прямому подключению нарушителя к серверу

Индикаторы компрометации ⓘ  
web-application-attack

Рекомендации ⓘ  
Ограничить внешний доступ к уязвимому приложению, используя встроенный межсетевой экран

Прикрепленные файлы ⓘ  
IDS\_packet\_time-2025-09-16T06\_52\_19.781082Z\_ruleid-3006078.pcap

Онлайн  
☆ ☆ ☆ ☆ ☆

Автор  
Ибатуллина Дарья  
@1132226434@pfur.ru

Ответственный  
Ганина Тамара  
@1132226429@pfur.ru

Источник  
10.10.4.11

Подражательские активы  
10.10.3.10

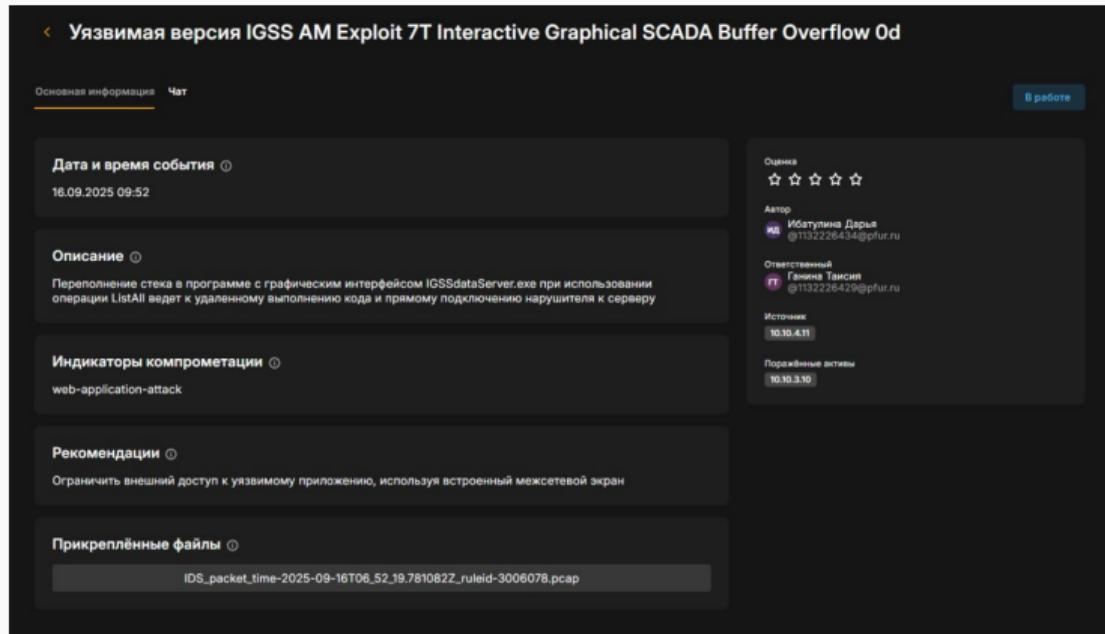


Рис. 5: Уязвимая версия IGSS AM Exploit 7T Interactive Graphical SCADA Buffer Overflow

## Устранение первой уязвимости и последствия (Axis2, App backdoor)

---

## Процесс аутентификации на целевом хосте

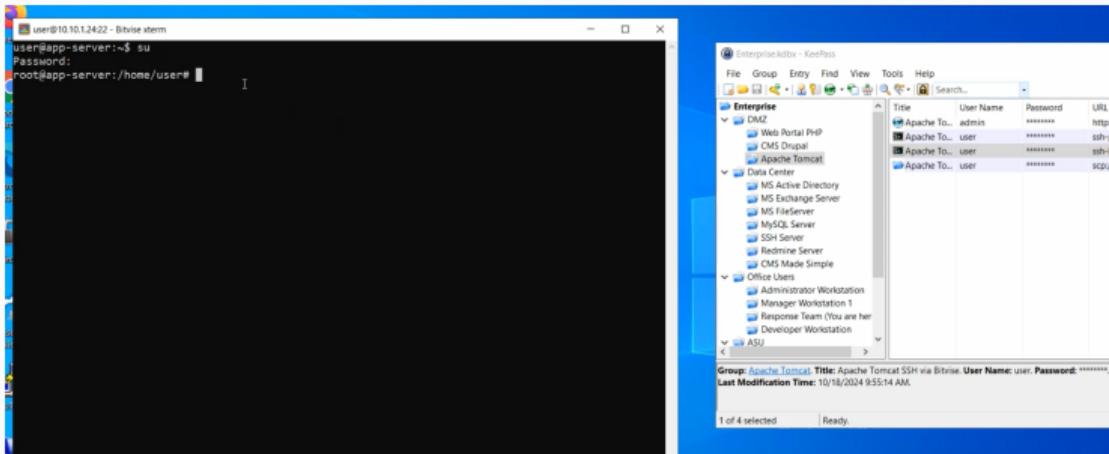


Рис. 6: Процесс аутентификации

Для блокировки доступа к конфигурационному файлу axis2.xml и предотвращения эксплуатации уязвимости CVE-2010-0219 в межсетевой экран iptables было добавлено специальное правило

```
user@app-server: ~
Chain ufw-user-logging-forward (0 references)
pkts bytes target     prot opt in     out    source      destination

Chain ufw-user-limit (0 references)
pkts bytes target     prot opt in     out    source      destination
  0     0 LOG          all -- *      *      0.0.0.0/0      0.0.0.0/0
      limit: avg 3/min burst 5 LOG flags 0 level 4 prefix "[UFW LIMIT BLOCK]"
  *     0     0 REJECT      all -- *      *      0.0.0.0/0      0.0.0.0/0
      reject-with icmp-port-unreachable

Chain ufw-user-limit-accept (0 references)
pkts bytes target     prot opt in     out    source      destination
  0     0 ACCEPT        all -- *      *      0.0.0.0/0      0.0.0.0/0

root@app-server:/home/user# sudo iptables -I INPUT 1 -j REJECT -p tcp --dport 80 -m string --string "axis2.xml" --algo kmp
root@app-server:/home/user# sudo iptables -L INPUT -n --line-numbers
```

Рис. 7: Добавление правила в iptables для блокировки доступа к axis2.xml

## Устранена уязвимость Axis2

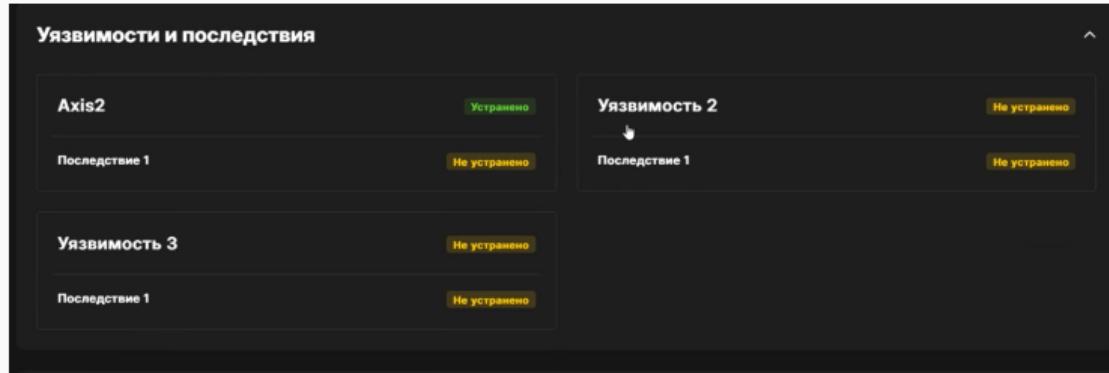


Рис. 8: Устранена уязвимость Axis2

Для полной проверки с помощью утилиты ss было выявлено установленное соединение с IP-адресом злоумышленника 195.239.174.11 на порт 7777, связанное с процессом evil.conf (PID 8367). Данное соединение является обратным shell-соединением (backdoor), установленным нарушителем, и подлежало немедленному завершению.

```
user@app-server:~
```

State	Local Address	Foreign Address	Process
ESTAB	0	0	users:(["sshd",pid=11576,fd=3],["sshd",pid=11574,fd=3])
ESTAB	0	10.10.1.24:55718	195.239.174.11:7777
CLOSING	1	127.0.0.1:34556	users:(["evil.conf",pid=8367,fd=3])
http-alt			
FIN-WAIT-1	0	127.0.0.1:34714	http-alt
FIN-WAIT-1	0	127.0.0.1:34714	http-alt
ESTAB	0	[:ffff:10.10.1.24]:http-alt	users:(["java",pid=598,fd=116])
ESTAB	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=120])
FIN-WAIT-2	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=120])
FIN-WAIT-2	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=1214])
ESTAB	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=214])
FIN-WAIT-2	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=214])
ESTAB	0	[:ffff:10.1.24]:58406	users:(["java",pid=598,fd=530])
FIN-WAIT-2	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=530])
ESTAB	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=530])
FIN-WAIT-2	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=530])
ESTAB	0	[:ffff:127.0.0.1]:http-alt	users:(["java",pid=598,fd=530])

Рис. 9: Процесс evil.conf

```
user@app-server:~
```

34658			
FIN-WAIT-2	0	0	[::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:
34626			
ESTAB	0	0	[::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:
34714		users:(("java",pid=598,fd=54))	
FIN-WAIT-2	0	0	[::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:
34676			
FIN-WAIT-1	0	20376	[::ffff:10.10.1.24]:http-alt [::ffff:10.10.1.253]:
20226			
ESTAB	0	0	[::ffff:10.10.1.24]:http-alt [::ffff:10.10.1.253]:
40148		users:(("java",pid=598,fd=130))	
ESTAB	0	0	[::ffff:10.10.1.24]:http-alt [::ffff:10.10.1.253]:
61668		users:(("java",pid=598,fd=125))	
CLOSE-WAIT	1	0	[::ffff:10.10.1.24]:http-alt [::ffff:195.239.174.11]:
33071		users:(("java",pid=598,fd=529))	
FIN-WAIT-2	0	0	[::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:
34598			
FIN-WAIT-2	0	0	[::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:
34612			
ESTAB	0	20375	[::ffff:10.10.1.24]:http-alt [::ffff:10.10.1.253]:
64496		users:(("java",pid=598,fd=127))	
root@app-server:/home/user#	/var/log/syslog		
bash:	/var/log/syslog:	Permission denied	
root@app-server:/home/user#	nano /var/spool/cron/crontabs/tomcat		

Рис. 10: Переход к редактированию файла

The screenshot shows a terminal window titled "user@app-server: ~" running the "GNU nano 3.2" editor. The file being edited is located at "/var/spool/cron/crontabs/tomcat". The content of the file is as follows:

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.  
# (/tmp/crontask installed on Tue Sep 16 09:40:38 2025)  
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)  
*/1 * * * * /opt/tomcat/webapps/evil.conf
```

The bottom of the terminal window displays the nano editor's command-line interface with various keyboard shortcuts:

- [ Read 4 lines ]
- ^G Get Help
- ^O Write Out
- ^W Where Is
- ^K Cut Text
- ^J Justify
- ^C Cur Pos
- ^X Exit
- ^R Read File
- ^\\ Replace
- ^U Uncut Text
- ^T To Spell
- ^ Go To Line

Рис. 11: Редактирование файла /var/spool/cron/crontabs/tomcat

The screenshot shows a terminal window titled "user@app-server: ~". The window title bar also displays "GNU nano 3.2" and the file path "/var/spool/cron/crontabs/tomcat". The main content area of the terminal shows the following text:

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.  
# (/tmp/crontask installed on Tue Sep 16 09:40:38 2025)  
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
```

The bottom of the terminal window shows a menu bar with various keyboard shortcuts:

- ^G Get Help
- ^C Write Out
- ^W Where Is
- ^K Cut Text
- ^J Justify
- ^C Cur Pos
- ^X Exit
- ^R Read File
- ^\\ Replace
- ^U Uncut Text
- ^T To Spell
- ^L Go To Line

Рис. 12: Удалили строку

```
user@app-server: ~
FIN-WAIT-2 0      0      [:ffff:127.0.0.1]:http-alt      [:ffff:127.0.0.1]:
34676
FIN-WAIT-1 0      20376  [:ffff:10.10.1.24]:http-alt      [:ffff:10.10.1.253]:
20226
ESTAB    0      0      [:ffff:10.10.1.24]:http-alt      [:ffff:10.10.1.253]:
40148      users:(["java",pid=598,fd=130])
ESTAB    0      0      [:ffff:10.10.1.24]:http-alt      [:ffff:10.10.1.253]:
61668      users:(["java",pid=598,fd=125])
CLOSE-WAIT 1      0      [:ffff:10.10.1.24]:http-alt      [:ffff:195.239.174.11]:
33071      users:(["java",pid=598,fd=529])
FIN-WAIT-2 0      0      [:ffff:127.0.0.1]:http-alt      [:ffff:127.0.0.1]:
34598
FIN-WAIT-2 0      0      [:ffff:127.0.0.1]:http-alt      [:ffff:127.0.0.1]:
34612
ESTAB    0      20375  [:ffff:10.10.1.24]:http-alt      [:ffff:10.10.1.253]:
64496      users:(["java",pid=598,fd=127])
root@app-server:/home/user# /var/log/syslog
bash: /var/log/syslog: Permission denied
root@app-server:/home/user# nano /var/spool/cron/crontabs/tomcat
root@app-server:/home/user# nano /var/spool/cron/crontabs/tomcat
root@app-server:/home/user# cd /opt/tomcat/webapps
root@app-server:/opt/tomcat/webapps# rm evil.conf
root@app-server:/opt/tomcat/webapps# kill 8367
root@app-server:/opt/tomcat/webapps#
```

Рис. 13: Удаление вредоносного файла и завершение процесса

The screenshot shows a dark-themed interface for a threat intelligence portal. At the top left is a circular logo with orange concentric rings and the text 'CSIRT'. To its right is a timer showing '00:00:00'. Below the timer are scenario details: 'Сценарий: Защита данных сегмента АСУ ТП', 'Шаблон: Офис', and 'Запущена в: 09:38'. To the right of the scenario details is a section titled 'Уязвимая версия IGSS AM Exploit 77 Interactive Graphical SCADA Buffer Overflow 0d' with the sub-instruction 'Получение доступа через уязвимый Apache Axis2'. The main content area is divided into two sections: 'Уязвимости и последствия' and 'Ресурсы'. The 'Уязвимости и последствия' section contains three items: 'Axis2' (status 'Устраниено'), 'App backdoor' (status 'Устраниено'), and 'Уязвимость 3' (status 'Не устраниено'). The 'Уязвимость 3' item has a sub-item 'Последствие 1' (status 'Не устраниено'). A cursor is hovering over the 'Устраниено' button for the 'App backdoor' item. The 'Ресурсы' section shows a table with columns 'Название:', 'IP Адрес:', 'Логин:', and 'Пароль'. The single entry is 'AM Threat Intelligence Portal' with a link icon. To the right of the 'Уязвимости и последствия' section is a small video window showing a person wearing headphones.

Рис. 14: Устранена первая уязвимость и её последствие

Была реализована блокировка сетевого трафика (в Manager Workstation) для уязвимой программы CoolReaderPDF, что является ключевой мерой по предотвращению дальнейшего распространения вредоносного кода и установления обратных соединений с машиной злоумышленника

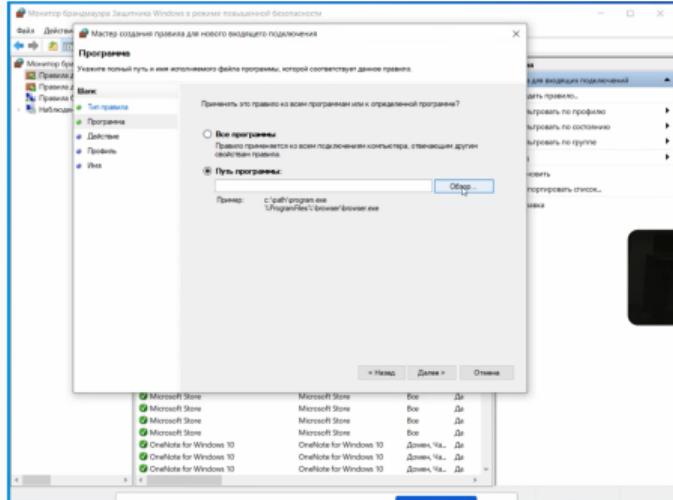


Рис. 15: Этап создания нового правила брандмауэра

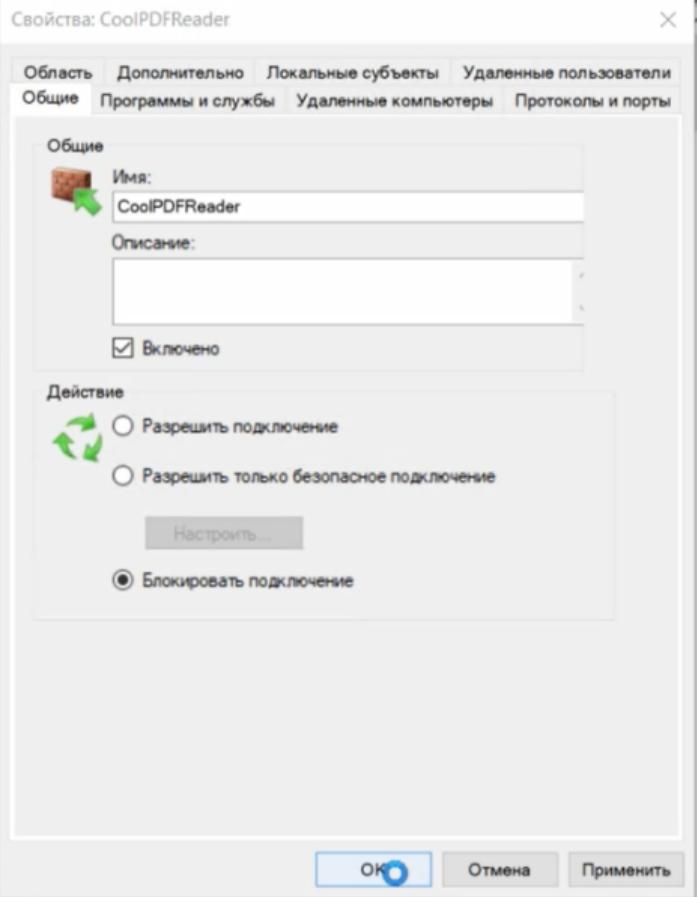


Рис. 16: Окно настройки создаваемого правила

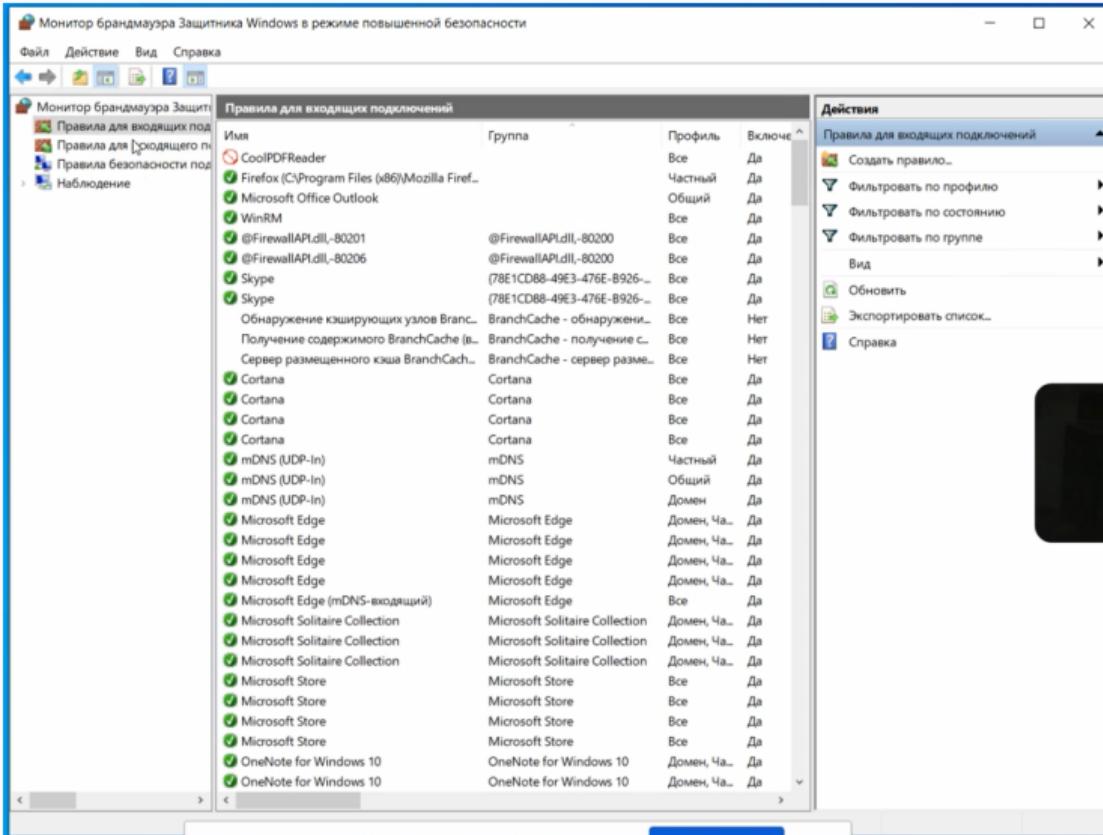


Рис. 17: Проверка в «Мониторе брандмауэра Защитника Windows»

После открытия командной строки  
была выполнена команда `netstat -bno`, которая выводит список всех  
TCP-соединений вместе с именами  
процессов и их PID. Для устранения  
угрозы была выполнена команда:  
`taskkill /f /pid 5348`. Эта  
команда принудительно (/f)  
завершает процесс с  
идентификатором 5348.

```

TCP 10.10.4.11:58401 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58400 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58403 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58404 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58405 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58406 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58407 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58408 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58409 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58410 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58411 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58412 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58413 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58414 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58415 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58416 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58417 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58418 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58419 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58420 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58421 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58422 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58423 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58424 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58425 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58426 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58427 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58428 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58429 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58430 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58431 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58432 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58433 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58434 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:58435 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58436 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:58437 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:60438 195.239.174.11:4445 ESTABLISHED 5348
[coolPDFReader.exe]
TCP 127.0.0.1:33333 127.0.0.1:49632 ESTABLISHED 4
Не удается получить сведения о владельце
TCP 127.0.0.1:49632 127.0.0.1:33333 ESTABLISHED 8164
[EpgLocalConsole.exe]

PS C:\Users\adминистратор> taskkill /f /pid 5348
Процесс, управляемый пользователем 5348, успешно завершен.
PS C:\Users\adминистратор>

```

Рис. 18: taskkill /f /pid 5348

The screenshot shows a dark-themed web application interface for managing security incidents. At the top left, there's a header bar with the text "CSIRT" and "Шаблон: Офис". Below this, a message says "Запущена в: 09:38". On the right side, a blue banner indicates a resolved issue: "Лабораторная 1-В (вторник)" with the note "(16 сент. 20:37) Последствие "Manager meterpreter" устранено".

The main content area is divided into sections:

- Уязвимости и последствия**: This section lists vulnerabilities and their status:
  - Axis2: Устранено (Resolved)
  - App backdoor: Устранено (Resolved)
  - CoolReaderPDF: Устранено (Resolved)
  - Manager meterpreter: Устранено (Resolved)
- Уязвимость 3**: A section for vulnerability 3, which is currently unaddressed ("Не устранено"). It includes:
  - Последствие 1: Не устранено (Not resolved)
- Ресурсы**: A table listing system resources with their details:

Название	IP Адрес	Логин	Пароль
AM Threat Intelligence Portal			
Удалённое рабочее место	10.140.2.169	ampire it10	*****
SecOnion	10.140.2.137	admin	*****

Рис. 19: Полностью устранена вторая уязвимость и её последствия

Для проведения работ по защите SCADA-сервера необходимо было получить удалённый доступ к нему. Для этого был использован менеджер паролей KeePass.

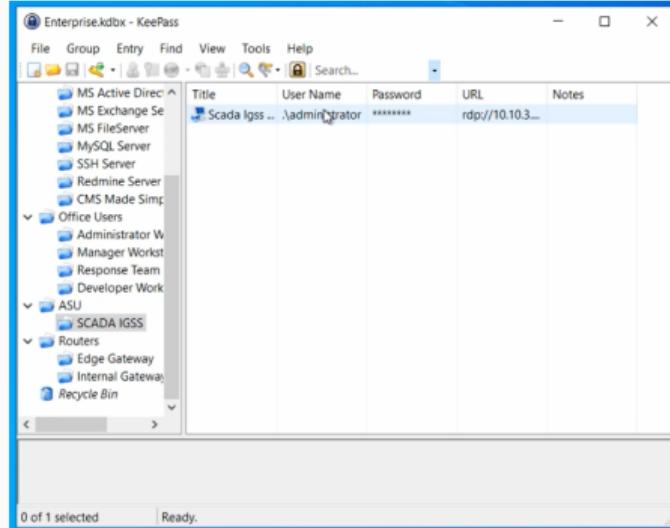


Рис. 20: Удаленный доступ к SCADA-сервер

Далее был запущен “Windows security center”: в меню “Пуск” - “Accessories” - “System Tools” - “Security center”.

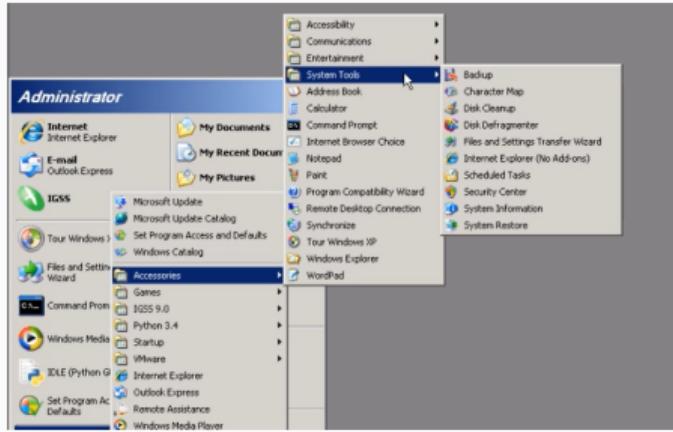


Рис. 21: “Пуск” - “Accessories” - “System Tools” - “Security center”

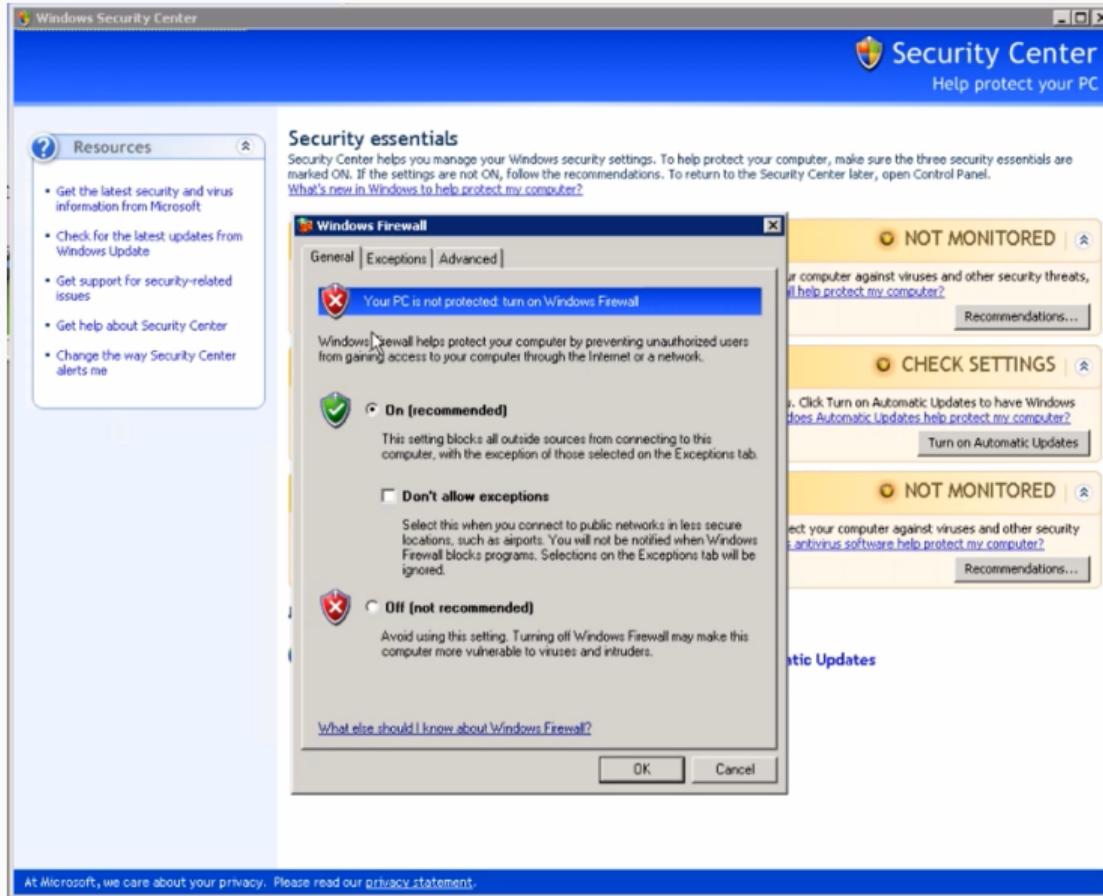


Рис. 22: Брандмауэр

На вкладке “Исключения” брандмауэра виден список правил, для которых мы убрали из исключений IGSS Dataserver. Эти правила были использованы злоумышленником для эксплуатации уязвимости.

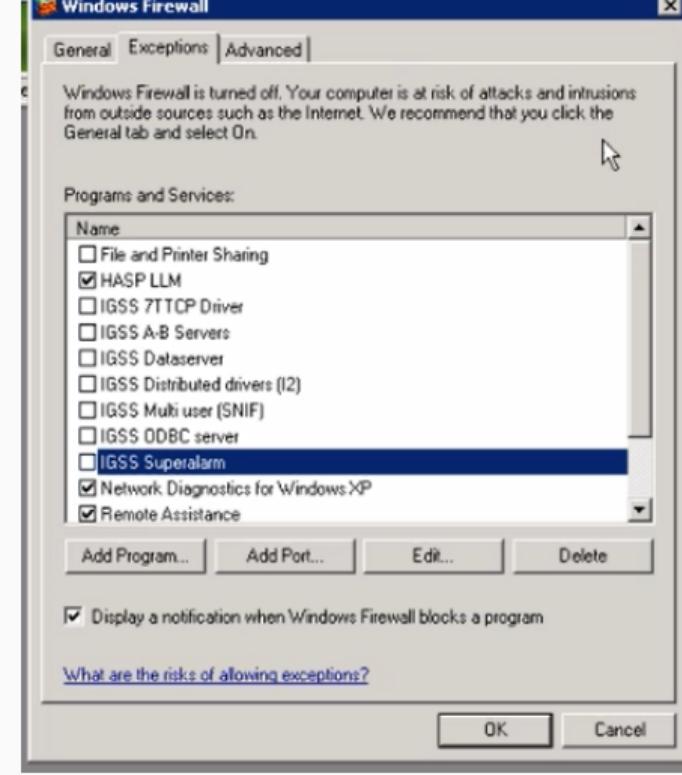


Рис. 23: Убрали из исключений IGSS Dataserver

Команда netstat -bno (рис. (fig:030?))

выявила установленное

TCP-соединение между

SCADA-сервером (10.10.3.10:1163) и

IP-адресом злоумышленника

(195.239.174.11:28002). Процесс,

ответственный за соединение, —

IGSSdataServer.exe (PID 2484).

```
C:\> netstat -bno
Active Connections
Proto  Local Address          Foreign Address        State      PID
TCP    10.10.3.10:1163        195.239.174.11:28002  ESTABLISHED 2484
[TGSSdataServer.exe]
TCP    10.10.3.10:3389       --unknown component(s)---  ESTABLISHED 868
[svchost.exe]
TCP    127.0.0.1:1249         127.0.0.1:12481     TIME_WAIT   0
TCP    127.0.0.1:1250         127.0.0.1:12481     TIME_WAIT   0
TCP    127.0.0.1:1259         127.0.0.1:12481     TIME_WAIT   0
TCP    127.0.0.1:1260         127.0.0.1:12481     TIME_WAIT   0
C:\> taskkill /f /pid 2484
SUCCESS: The process with PID 2484 has been terminated.
C:\>
```

Рис. 24: TCP-соединение

## Полностью устранена третья уязвимость и её последствия

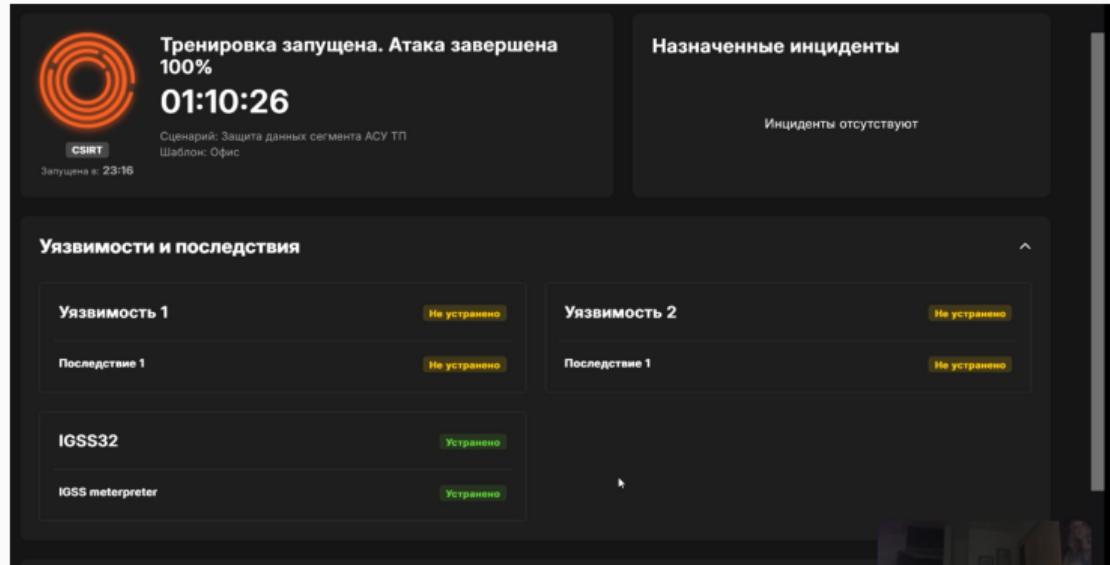


Рис. 25: Полностью устранена третья уязвимость и её последствия

## Результаты

---

## Результаты

---

В ходе выполнения лабораторной работы был успешно отработан сценарий комплексной кибератаки на сегмент АСУ ТП и проведены мероприятия по её обнаружению и нейтрализации.