УДК 004.056

ИССЛЕДОВАНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

В.В. МАЛИКОВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 20 ноября 2017

Аннотация. Рассмотрены основные элементы структуры сетевых систем видеонаблюдения. Проведено статистическое исследование по критерию близости: преимущественное использование на объектах различных категорий в Республике Беларусь. Выполнено тестирование сетевых систем видеонаблюдения на предмет возможности проведения удаленных атак по информационно-телекоммуникационным сетям.

Ключевые слова: сетевые системы видеонаблюдения, несанкционированный доступ, уязвимость.

Abstract. The main elements of the structure of the network videosurveillance systems has been described. The statistical study on the criterion of proximity has been performed: the predominant use on the objects of different categories in the Republic of Belarus. The testing of network videosurveillance systems for ability to conduct remote attacks on information and telecommunications networks has been provided.

Keywords: network video surveillance systems, unauthorized access, vulnerability.

Doklady BGUIR. 2018, Vol. 111, No. 1, pp. 25-29
Evaluation of the IT-security level of network videosurveillance
V.V. Malikov

Введение

Сетевые системы инженерно-технической безопасности (ССИТБ) обеспечивают непосредственный физический контроль объектов различных категорий, включая критически важные объекты. В настоящее время существует значительное число инцидентов, связанных с несанкционированным удаленным доступом (НСД) к ССИТБ: охранной сигнализации (ОС), сетевым системам видеонаблюдения (ССВН), системам контроля и управления доступом (СКУД) и др. Как правило, НСД сопровождается дистанционным отключением ССИТБ с последующим нарушением целостности, доступности и конфиденциальности обрабатываемой/хранимой информации. Дополнительно существует высокая вероятность последующего физического проникновения на объекты и совершения террористических актов [1].

Наиболее распространенной подгруппой ССИТБ являются ССВН, которые позволяют проводить идентификацию сотрудников при доступе к различным зонам охраняемого объекта, а также осуществлять оперативный интеллектуальный поиск в архивных данных по заданным критериям поиска.

Согласно статистическим данным [2], в мире основным источником угроз для промышленных систем является интернет (рис. 1). Поэтому важным условием надежного функционирования таких систем является проведение тестирования на предмет возможности проведения удаленных атак по информационно-телекоммуникационным сетям.

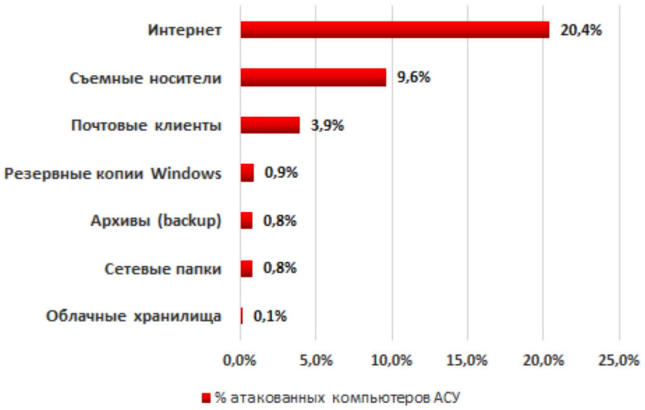

Рис. 1. Основные источники угроз, заблокированных на компьютерах АСУ (первое полугодие 2017 г.) [2]

Содержательная постановка задачи

В связи с тем, что в настоящее время в мире и Беларуси основную часть отрасли ССИТБ занимают ССВН [3], дальнейшее исследование будем проводить только в части информационной безопасности таких систем от удаленных атак по информационно-телекоммуникационным сетям.

В качестве основных элементов структуры для тестирования ССВН будем считать:

– цифровой видеорегистратор – DVR (Digital Video Recorder): изделие, предназначенное для приема, обработки, хранения, воспроизведения видеосигнала, поступающего от видеокамер объекта охраны, а также имеющее дополнительную возможность удаленного сетевого подключения;

– сетевой видеорегистратор – NVR (Network Video Recorder): изделие, предназначенное для приема, обработки, хранения, воспроизведения и локальной/сетевой передачи видеосигнала, поступающего от IP-камер объекта охраны;

– сетевую систему хранения данных – NAS (Network Attached Storage): систему, предназначенную для предоставления сервисов хранения данных в цифровом формате другим устройствам в сети, подключенным по каналам сопряжения и коммуникации на основе IP-протокола;

– цифровую IP-камеру (Internet Protocol): видеокамеру, предназначенную для передачи видеосигнала по каналам сопряжения и коммуникации в цифровом формате на основе IP-протокола.

В рамках настоящей статьи проведем тестирование ССВН (DVR, NVR, NAS и IP-камер), наиболее часто применяемых в Беларуси, на предмет возможности проведения удаленных атак по информационно-телекоммуникационным сетям.

Приведенные в рамках данной статьи материалы носят исключительно научно-исследовательский характер. Исследование проводилось автором строго в научных целях, его результаты не являются и не могут признаваться руководством к совершению каких-либо противоправных действий. При проведении исследования автор действовал в рамках законодательства Республики Беларусь. Автор не несет ответственности за инциденты в сфере информационной безопасности, имеющие отношение к тематике исследования.

Результаты и обсуждение

В связи с тем, что производством ССВН занимается значительное число компаний/вендоров ССИТБ, для проведения исследования необходимо сформировать перечень производителей, изделия которых наиболее используются в Беларуси. Для выбора номенклатуры компаний/вендоров ССИТБ, подлежащих исследованию по критерию близости: преимущественное использование на объектах различных категорий в Республике Беларусь, совместно с ресурсом «aercom.by» [4] было проведено статистическое исследование отрасли путем on-line анкетирования 86 специалистов служб безопасности (рис. 2).

Таким образом, по результатам опроса основными вендорами по ССВН в Беларуси являются «Hikvision» (34,6 %), «Dahua Technology» (10,3 %), «Axis» (9 %). Проведем исследование продукции указанных вендоров на предмет наличия уязвимостей, а также способов их эксплуатации через сетевые каналы сопряжения и коммуникации.

При проведении тестирования ССВН (DVR, NVR, NAS и IP-камер) будем использовать специализированные ресурсы: открытую базу уязвимостей сервиса «Vulners» [5] и сетевой сканер «Censys» [6]. Итоговые результаты тестирования ССВН приведены в табл. 1.

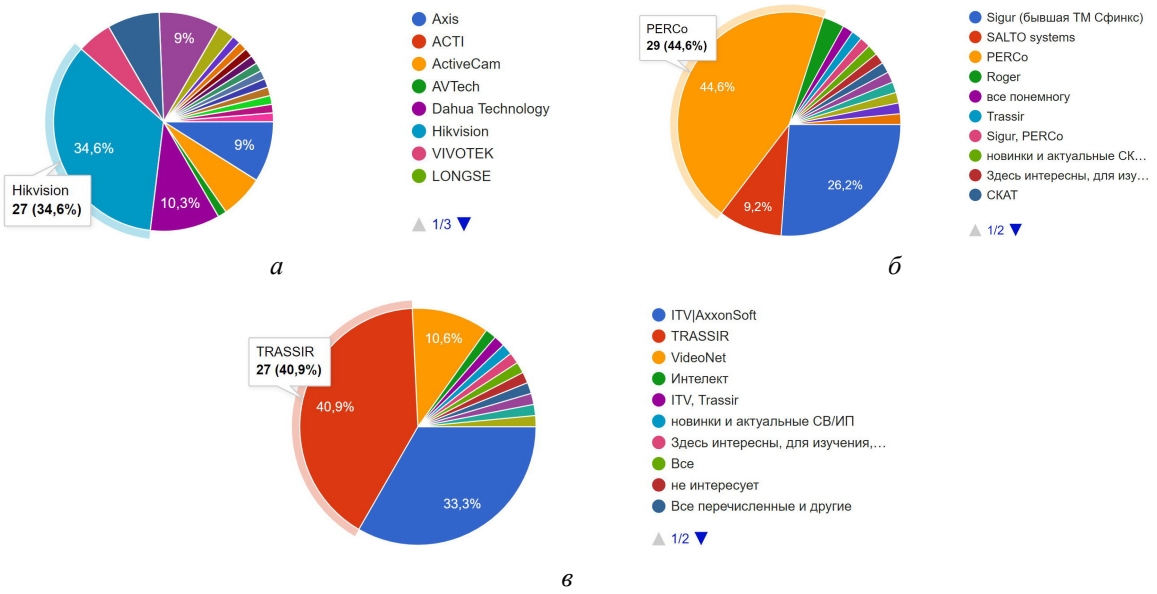

Рис. 2. Основные результаты статистического исследования:
а – ССВН; *б* – СКУД; *в* – системы видеоаналитики

Таблица 1. **Результаты тестирования ССВН**

№ теста	Описание проводимого теста	Описание запроса теста (сетевой сканер «Censys» [6])	Результаты теста, шт.
1	Количество сетевых ССВН с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	(DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus	2066
2	Количество сетевых ССВН «Hikvision» с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	metadata.manufacturer:Hikvision and (DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus	34
3	Количество сетевых ССВН «Dahua Technology» с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	metadata.manufacturer:Dahua Technology and (DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus	33
4	Количество сетевых ССВН «Axis» с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	metadata.manufacturer:Axis and (DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus	1
5	Количество уязвимых к атаке «heartbleed» (CVE-2014-0160) [5, 7] сетевых ССВН с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	(DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus and heartbleed (DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus and 443.https.heartbleed.heartbleed_vulnerable:True	9
6	Количество сетевых ССВН с открытым портом «23/telnet» с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	((DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus) AND protocols.raw:"23/telnet"	23
7	Количество сетевых ССВН с открытым портом «445/smb» с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	((DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus) AND protocols.raw: "445/smb"	10
8	Количество сетевых ССВН с открытым портом «21/ftp» с локацией в Беларуси, потенциально доступных (HTTP, код состояния 200) по порту 80 (TCP, UDP)	((DVR or NVR or NAS or IP-cameras or Network Camera) and 80.http.get.status_code:200 and location.country: Belarus) AND protocols.raw: "21/ftp"	824

В ходе проведенных исследований (табл. 1, тесты № 1–4) были выявлены типовые ССВН с возможностью удаленного сетевого доступа к панели администратора веб-сервера (рис. 3). Дополнительное тестирование таких веб-серверов ССВН на предмет наличия заводских (по умолчанию) настроек «логин-пароль» администратора позволило выявить 1 уязвимую ССВН.

а *б*

Рис. 3. Удаленный сетевой доступ к панели администратора веб-сервера ССВН

По результатам тестирования (табл. 1, тесты № 6–8) следует отметить, что множество ССВН в Беларуси имеют доступ к портам /протоколам: «21/ftp», «23/telnet», «445/smb», которые имеют большое число уязвимостей, в том числе в составе вредоносных эксплойт-паков [5].

Для оценки потенциальной возможности эксплуатации уязвимости «Heartbleed» (CVE-2014-0160) [7] в криптографическом программном обеспечении «OpenSSL», позволяющей осуществлять несанкционированное чтение памяти на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера, проведем тестирование одной из типовых выявленных уязвимых ССВН (табл. 1, тест № 5). Результаты тестирования типовой ССВН сетевым сканером «Censys» [6] приведены в табл. 2.

Таблица 2. **Результаты эксплуатации уязвимости «Heartbleed» на типовой ССВН**

Наименование показателя	Значение
Протокол	TLS (v. 1.2)
Уязвимый порт/сервис	443 / HTTPS
Алгоритм шифрования /хэш-функция	RSA / SHA256
Имя сертификата	IMM2-6cae8b5aa67c
Серийный номер сертификата	15163727005938176607
Значение хэш-функции сертификата (SHA256)	a746a52c65929eeee321991c1cac7b2cc9c1ad7d0ed4b5c64e91d472ebf03b04
Значение хэш-функции открытого ключа (SPKI SHA256 / 2048 bit)	3e9012535931455a3a59afb747f2e3dede703b17f5af61360f5e16276df6345e
Возможность эксплуатации уязвимости CVE-2014-0160 (Heartbleed)	Да (уязвим к CVE-2014-0160)
Возможность подключения к порту «23/Telnet» через эксплуатации уязвимости CVE-2014-0160 (Heartbleed)	Да (уязвим к CVE-2014-0160)

Заключение

На основании проведенных исследований ССВН можно сделать следующие выводы.

1. По результатам статистического исследования (опроса) по критерию близости: преимущественное использование на объектах различных категорий в Республике Беларусь, основными вендорами по ССВН в Беларуси являются: «Hikvision» (34,6 %), «Dahua Technology» (10,3 %), «Axis» (9 %).

2. Тестирование ССВН на предмет наличия уязвимостей, а также способов их эксплуатации через сетевые каналы сопряжения и коммуникации показало:

– общее количество устройств ССВН (DVR, NVR, NAS и IP-камер), доступных через сеть – 2066 шт. (табл. 1, тест № 1), из них 866 шт. (41,9 %) – имеют потенциальные уязвимости

(табл. 1, тесты № 6–8);

– общее количество доступных через сеть устройств ССВН (DVR, NVR, NAS и IP-камер) производителей: «Hikvision» – 34 шт. (1,7 %), «Dahua Technology» – 33 шт. (1,6 %), «Axis» – 1 шт. (0,05 %);

– как минимум, 1 веб-сервер ССВН имеет заводские (по умолчанию) настройки логина и пароля администратора;

– показан пример успешной эксплуатации уязвимости «Heartbleed» (CVE-2014-0160) [7] на типовой уязвимой ССВН, выявленной по результатам тестирования (табл. 1, тест № 5).

Список литературы

1. Hackers hit D.C. police closed-circuit camera network, city officials disclose // washingtonpost.com [Электронный ресурс]. – URL: https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.c4e302e386d9/ (дата обращения: 08.10.2017).
2. Ландшафт угроз для систем промышленной автоматизации: первое полугодие 2017 // ics-cert.kaspersky.ru [Электронный ресурс]. – URL: https://ics-cert.kaspersky.ru/reports/2017/09/28/threat-landscape-for-industrial-automation-systems-in-h 1-2017/ (дата обращения: 08.10.2017).
3. Видеонаблюдение: Аналитика, цифры, прогнозы, технологии // techportal.ru [Электронный ресурс]. – 2003-2017. – URL: http://www.techportal.ru/ glossary/videonabludenie.html/ (дата обращения: 08.10.2017).
4. Безопасность в Беларуси // aercom.by [Электронный ресурс]. – URL: https://aercom.by/ (дата обращения: 08.10.2017).
5. Vulners // vulners.com [Электронный ресурс]. – URL: https://vulners.com/ (дата обращения: 09.10.2017).
6. Censys // censys.io [Электронный ресурс]. – URL: https://censys.io/ (дата обращения: 10.10.2017).
7. The Heartbleed Bug // heartbleed.com [Электронный ресурс]. – URL: http://heartbleed.com/ (дата обращения: 12.10.2017).

References

1. Hackers hit D.C. police closed-circuit camera network, city officials disclose // washingtonpost.com [Electronic resource]. – URL: https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story .html?utm_term=.c4e302e386d9/ (access date: 08.10.2017).
2. Landshaft ugroz dlya sistem promyishlennoy avtomatizatsii: pervoe polugodie 2017 // ics-cert.kaspersky.ru [Electronic resource]. – URL: https://ics-cert.kaspersky.ru/reports/2017/09/28/threat-landscape-for-industrial-automation-systems-in-h 1-2017/ (access date: 08.10.2017). (in Russ.)
3. Videonablyudenie: Analitika, tsifryi, prognozyi, tehnologii // techportal.ru [Electronic resource]. – URL: http://www.techportal.ru/ glossary/videonabludenie.html/ (access date: 08.10.2017). (in Russ.)
4. Bezopasnost v Belarusi // aercom.by [Electronic resource]. – URL: https://aercom.by/ (access date: 08.10.2017). (in Russ.)
5. Vulners // vulners.com [Electronic resource]. – URL: https://vulners.com/ (access date: 09.10.2017).
6. Censys // censys.io [Electronic resource]. – URL: https://censys.io/ (access date: 10.10.2017).
7. The Heartbleed Bug // heartbleed.com [Electronic resource]. – URL: http://heartbleed.com/ (access date: 12.10.2017).

Сведения об авторах

Маликов В.В., к.т.н., доцент, докторант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Malikov V.V., Ph.D., associate professor, doctoral candidate of information security department of Belarusian state university of informatics and radioelectronics.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6,
Белорусский государственный
университет информатики и радиоэлектроники
тел. +375-29-623-46-84;
e-mail: malvvv104@mail.ru
Маликов Владимир Викторович

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka st., 6,
Belarusian state university
of informatics and radioelectronics
tel. +375-29-623-46-84;
e-mail: malvvv104@mail.ru
Malikov Vladimir Viktorovich