www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.4.6

УДК 004.056.5
ББК 68.823

ИССЛЕДОВАНИЕ СИСТЕМ ВИДЕОЗАХВАТА КАК СРЕДСТВА РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Егор Андреевич Жуйков

Студент кафедры информационной безопасности,
Волгоградский государственный университет
27egor@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Елена Александровна Максимова

Кандидат технический наук, доцент,
заведующий кафедрой информационной безопасности,
Волгоградский государственный университет
maksimova@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Статья посвящена рассмотрению систем видеозахвата, которые могут помочь предотвратить утечку информации с персональных компьютеров на предприятии. Предложенная в работе схема экспертной оценки средств видеозахвата позволяет определить систему, исходя из выбранных критериев и заданных для них весовых коэффициентов, и предоставить пользователю оптимальный выбор в процессе принятия решения конкретной задачи.

Ключевые слова: видеозахват, инсайдер, защищенность, инсайдерская информация, информационная безопасность.

Одной из тенденций настоящего времени является рост инцидентов, связанных с информационной безопасностью. Подтверждение тому – данные компании InfoWatch, согласно которым количество утечек конфиденциальной информации в первом полугодии 2017 г. на 10 % больше, чем за аналогичный период 2016 г., и равно 925 случаям [8]. При этом из 925 случаев утечки 53 % осуществлены сотрудниками компании, 1,7 % – руководителями, то есть потенциальными инсайдерами.

В современном мире инсайдер – это очень распространенное понятие. Оно применимо в разных сферах хозяйственной деятельности. Согласно наиболее распространенному определению инсайдер – это физическое или юридическое лицо, которое благодаря своему положению имеет доступ к ценной (в основном, конечно, с экономической точки зрения) информации [6]. Ценную информацию также называют инсайдерской информацией.

Инсайдерская информация (англ. *Insider information*) – существенная, публично не раскрытая служебная информация компании, которая, в случае ее раскрытия, способна повлиять на рыночную стоимость ценных бумаг компании [5]. К этой категории можно отнести: информацию о готовящейся смене руководства и новой страте-

гии, о подготовке к выпуску нового продукта и к внедрению новой технологии, об успешных переговорах о слиянии компаний или идущей скупке контрольного пакета акций; материалы финансовой отчетности, прогнозы, свидетельствующие о трудностях компании; информация о тендерном предложении (на торгах) до его раскрытия публике, список аффилированных лиц и т. д. [1; 6].

На рисунке представлены категории лиц, относящиеся к инсайдерам [4; 7].

Чтобы сократить количество утечек конфиденциальной информации, можно воспользоваться специальными средствами видеозахвата монитора, так как данные системы помогут определить, откуда и когда была взята информация, кто имел допуск к ней. Данные программы пишут видеозапись постоянно и сохраняют ее в указанном месте. Кроме того, полученные материалы могут храниться неопределенное количество времени.

Согласно [3] захват видео (от англ. Video capture – захват видео) – процесс преобразования видеосигнала из внешнего источника в - цифровой видеопоток при помощи персонального компьютера и запись его в видеофайл с целью последующей его обработки, хранения или воспроизведения.

Таким образом, под термином «видеозахват» будем понимать перенос видеоматериала с видеокамеры (цифровой или аналоговой) на компьютер или другой носитель информации. Программа видеозахвата представляет собой приложение, служащее для упрощения этого процесса.

В настоящее время существует множество средств видеозахвата, которые делят на 2 класса: программные и аппаратные [2].

Среди программных средств наиболее популярными являются: CamStudio, UVScreenCamera, BB FlashBack, Movavi Screen Capture Studio, ActivePresenter, HyperCam и т. д.

Среди аппаратных средств наиболее популярными являются: AVerMedia Technologies Live Gamer Portable, AVerMedia Technologies Game Capture HD II, AVerMedia Technologies DarkCrystal HD Capture Station.

Для исследования средств видеозахвата выделены следующие критерии:

К1 – выбор формата сохранения видео;

К2 – редактирование видео;

К3 – подсветка нажатий мыши / клавиатуры;

К4 – скорость записи;

К5 – разрешение записи;

К6 – совместимость с ОС;

К7 – число видеоканалов;

К8 – скорость просмотра;

К9 – запись звука;

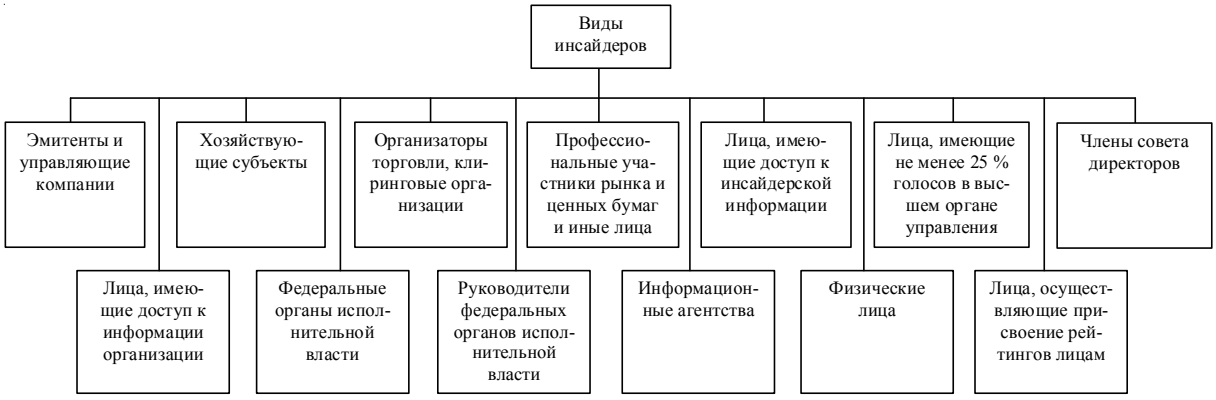
К10 – функциональность;

К11 – выбор режима захвата.

По выделенным критериям проанализированы обозначенные выше классы средств видеозахвата (см. табл. 1).

В таблице 1 «1» соответствует выполнению выделенного критерия, «0» – невыполнению.

Таким образом, класс программных средств видеозахвата с точки зрения выделенных критериев можно рассматривать как наиболее рациональные. Результаты предполагают равнозначность критериев. При необходимости в оценку для каждого критерия вводятся весовые коэффициенты.



Классификация инсайдеров

Приведенная экспертная оценка детализирована при рассмотрении класса программных средств видеозахвата. Исследованы по выбранным критериям такие средства, как CamStudio, UVScreenCamera, BB FlashBack, Movavi Screen Capture Studio, ActivePresenter, HyperCam. Результаты исследований представлены в таблице 2. По данным в ней сведениям наиболее рациональной для применения можно считать программу Movavi Screen Capture Studio.

Формализованная модель, описывающая систему видеозахвата как средство расследования инцидентов информационной безопасности на предприятии, представима в виде:

$$F = F(\{M\},\{K\},\{M\}),$$

где M – множество видов кодеков видео; K – множество вариантов скорости записи видео; W – множество выбора частоты кадров.

Таблица 1

Сравнение классов средств видеозахвата

Средства	Критерии											
	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11	Итог
Программные средства видеозахвата	1	1	1	1	1	0	0	1	1/0	1	1	0,77
Аппаратные средства видеозахвата	1	0	1/0	1	1	1	1	1	1	0	0	0,68

Таблица 2

Сравнение программ видеозахвата

Программы	CamStudio	UVScreenCamera	BB FlashBack	Movavi Screen Capture Studio	ActivePresenter	HyperCam
Разработчик	RenderSoft	Юрий Выровщиков	BlueberrySoftware	Movavi	AtomiSystems, Inc.	HyperionicsTechnology, LLC
Лицензия	Freeware	Shareware (600 руб.)	Shareware ($89)	Shareware (1490 руб.)	Shareware ($299+)/Freeware	Freeware
Локализация на русский язык	0	1	0	1	0	0
Форматы сохранения видео	AVI, SWF	UVF, EXE, AVI, SWF, FLV, GIF	Flash, QuickTime (H264), WMV, MPEG4, AVI, GIF, MS Powerpoint, EXE	AVI, DV AVI, XVID, MPEG 1,2, MP4, FLV (H.263, H.264), WMV, 3GPP, 3GPP2, MOV, QT, VOB, IFO, MOD, DAT, M2TS, MKV, OGV, WEBM	WMV, AVI, MPEG4, WebM, FLV имн. др.	AVI
Редактор видео	0	1	1	1	1	0
Режимы захвата	Окно, регион, фиксированный регион, полный экран	Полноэкранный, регион, окно	Полноэкранный, регион, окно	Полноэкранный, регион, окно	Полноэкранный, регион, окно	Полноэкранный, регион, окно
Публикация онлайн	0	1	1	1	1	0
Автопанорамирование	1	0	0	0	1	0
Аннотации во время записи	1	1	1	0	1	1
Подсветка нажатий мыши / клавиатуры	1/0	1/1	1/1	1/0	1/1	1/0

$$M = \{M1, \ldots, M9\},$$

в которой:

M1 – MPEG4;
M2 – WMV1;
M3 – WMV2;
M4 – MSMPEG4v2;
M5 – MSMPEG4v3;
M6 – H263P;
M7 – FLV1;
M8 – MPEG2;
M9 – RAW;

$$K = \{K1, \ldots, K6\},$$

в которой:

K1 – _50 kbit;
K2 – _100 kbit;
K3 – _500 kbit;
K4 – _1000 kbit;
K5 – _2000 kbit;
K6 – _3000 kbit;

$$W = \{W1, \ldots , W25\},$$

в которой W1, ... , W25 – частота кадров (FPS: max 25fps).

Таким образом, мера функции – результат декартового произведения:

$$|F| = K * M * W.$$

Рассмотренная схема экспертной оценки средств видеозахвата позволяет определить систему, исходя из выбранных критериев и заданных для них весовых коэффициентов, и предоставить пользователю оптимальный выбор в процессе принятия решения конкретной задачи.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 01.01.2000. – М. : Стандартинформ, 2003. – 9 с.

2. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. – Введ. 01.01.2016. – М. : Стандартинформ, 2014. – 23 с.

3. Захват видео. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/Захват_видео 24 (дата обращения: 19.03.2018). – Загл. с экрана.

4. Инсайдер. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/Инсайдер (дата обращения: 19.03.2018). – Загл. с экрана.

5. Инсайдерская информация. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/Инсайдерская_информация (дата обращения: 19.03.2018). – Загл. с экрана.

6. Методы борьбы с инсайдерами. – Электрон. текстовые дан. – Режим доступа: https://studwood.ru/1358385/pravo/metody_borby_insayderami (дата обращения: 19.03.2018). – Загл. с экрана.

7. Федеральный закон «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» от 27.07.2010 № 224-ФЗ // Собрание законодательства РФ. – 02.08.2010. – № 31. – Ст. 4193.

8. InfoWatch // Интуит. – Электрон. текстовые дан. – Режим доступа: https://www.infowatch.ru/analytics/reports (дата обращения: 19.03.2018). – Загл. с экрана.

REFERENCES

1. *GOST R 51275-99. Zashchita informatsii. Obyekt informatizatsii. Faktory, vozdeystvuyushchie na informatsiyu. Vved. 2000–01–01* [GOST R 51275-99. Information Protection. The Object of Informatization. Factors Affecting the Information. Introduced on January 1, 2000]. Moscow, Standartinform Publ., 2003. 9 p.

2. *GOST R 51558-2014. Sredstva i sistemy okhrannye televizionnye. Klassifikatsiya. Obshchie tekhnicheskie trebovaniya. Metody ispytaniy. Vved.01.01.2016* [GOST R 51558-2014. Video Means and Systems of Security. Classification. General Technical Requirements. Test Methods. Introduced on January 1, 2016]. Moscow, Standartinform Publ., 2014. 23 p.

3. *Zakhvat video* [Video Capture]. URL: https://ru.wikipedia.org/wiki/Захват_видео 24 (accessed 19 March 2018).

4. *Insider*. URL: https://ru.wikipedia.org/wiki/Инсайдер (accessed 19 March 2018).

5. *Insayderskaya informatsiya* [Insider Information]. URL: https://ru.wikipedia.org/wiki/Инсайдерская_информация (accessed 19 March 2018)

6. *Metody borby s insayderami* [The Methods of Struggle with Insiders]. URL: https://studwood.ru/1358385/pravo/metody_borby_insayderami (accessed 19 March 2018).

7. Federalnyy zakon «O protivodeystvii nepravomernomu ispolzovaniyu insayderskoy informatsii i manipulirovaniyu rynkom i o vnesenii izmeneniy v otdelnye zakonodatelnye akty Rossiyskoy Federatsii» ot 27.07.2010 № 224-FZ [Federal Law 'On Counteraction to Illegal Use of Insider Information and Market Manipulation and on Modification of Separate Legal Acts of the Russian Federation' of 27 July 2010 No. 224-FZ]. *Sobranie zakonodatelstva RF* [Collected Legislation of the Russian Federation], 2010, 2 Aug., no. 31, art. 4193.

8. InfoWatch. *Intuit*. URL: https://www.infowatch.ru/analytics/reports (accessed 19 March 2018).

VIDEO CAPTURE SYSTEMS AS A MEANS OF INVESTIGATING INFORMATION SECURITY INCIDENTS AT THE ENTERPRISE

Egor A. Zhuykov

Student, Department of Information Security,
Volgograd State University
27egor@gmail.com
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Elena A. Maksimova

Candidate of Sciences (Engineering), Associate Professor,
Head of Department of Information Security,
Volgograd State University
maksimova@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Today's trend is the growth of information security incidents. Confirmation of this is the data of the company InfoWatch, according to which the number of leaks of confidential information in the first half of 2017 has increased by 10% as compared to the same period of 2016, and equals to 925 cases. However, 53% out of these 925 cases of diversion were sold by company employees, and 1.7% – by potential insiders. In the modern world, an insider is a very common concept. It is applicable in different spheres of economic activity. In a general sense, an insider is a natural or legal person who, due to his or her position, has access to valuable (mainly, of course, from an economic point of view) information. Valuable information is also called insider information.

The article is devoted to the consideration of video capture systems that can help prevent leakage of information from personal computers in the enterprise.

The proposed scheme of expert evaluation of video capture allows you to determine the system based on the selected criteria and specified weight coefficients, and lets the user make the best choice in the decision-making process of a specific problem.

Key words: video capture, insider, security, insider information, information security.