УДК 34

МАКСИМОВА Елена Александровна,
кандидат технических наук, доцент,
г. Волгоград, Россия
Russia@prescopus.com

ЦЫБУЛИН Анатолий Михайлович,
Кандидат технических наук, г. Волгоград, Россия,

СВИЩЕВА Марина Николаевна,
Ассистент кафедры «Информационная безопасность»,
г. Волгоград, Россия

ВИТЕНБУРГ Екатерина Александровна,
студент, г. Волгоград, Россия

КОНТРОЛЬ ДЕЯТЕЛЬНОСТИ ПЕРСОНАЛА И ЗАЩИЩЕННОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОРГАНИЗАЦИИ

Анализ деятельности сотрудников и защищенности информационных ресурсов организации показал, что контроль за деятельностью сотрудников необходим не только с точки зрения реализации продуктивного рабочего процесса, но и для обеспечения информационной безопасности организации. Контроль эффективности работы персонала предлагается выполнять с помощью специальной методики.

Ключевые слова: **оценка эффективности, работа пользователей, инсайдеры, методы инвентаризации, конфиденциальные данные, мониторинг, аудит, защищенность, информационная система.**

MAXIMOVA Elena Alexandrovna,
Candidate for Doctorate in Technics, Associate Professor, Volgograd city, Russia
Russia@prescopus.com

TSYBULIN Anatoly Mikhaylovich,
Candidate for Doctorate in Technics,
Volgograd city, Russia

SVISCHEVA Marina,Nikolaevna,
Assistant at the Chair of Information Security,
Volgograd city, Russia

VITENBURG Ekaterina Alexandrovna,
Student, Volgograd city, Russia

STAFF PERFORMANCE CONTROL AND SECURITY OF CORPORATE INFORMATION RESOURCES

The paper considered the study of corporate manpower' operation and information security for corporate data resources that evidenced necessity of controlling operation of employees for both productive work performance and the secured corporate database as well. The study suggested the monitoring of work performance' efficiency in the staff done with a specific technique, with a symbolic model drafted for soft wiring.

Keywords: **performance assessment, users' work, insiders, inventory making' techniques, confidential data, monitoring techniques, audit, protection from internal threats, information setup.**

Благодарность: Исследование выполнено при финансовой поддержке РФФИ (Российского Фонда Фундаментамльных Исследований) и Волгоградской области в рамках научного проекта №14-7-97014р_поволжье_а.
Acknowledgement: The study was performed with the funding by the Russian Foundation for Basic Research (RFBR) and the Volgograd region budget funding in the framework of the research project №14-7-97014r_povolzhe_a.

Одной из важнейших задач, решаемой руководителем любой организации, является задача обеспечения рационального использования рабочего времени сотрудниками. Часть работников в течение рабочего дня, кроме выполнения прямых функциональных задач, также занимается своими личными делами, используя электронные ресурсы организации. В ряде случаев это допустимо. Однако данная ситуация может рассматриваться как воровство на рабочем месте: напрямую – за счет использования каналов утечки информации (электронная почта, USB-носители, устройства Wi-Fi) и опасного (вирусы, трояны и др.) для предприятия интернет-трафика, косвенно – за счет упущенной выгоды из-за простоя производственных мощностей, не выполненных в срок работ и т.д.

Утечка конфиденциальной информации может происходить как в результате преднамеренных действий инсайдера-злоумышленника, так и в результате халатности и неправильных действий сотрудников, которые могут даже не иметь доступа к этой информации.

По данным ежегодного исследования института Info Watch [2], более 70% инсайдерских атак приводят к финансовым потерям, а для 30% опрошенных компаний финансовые потери от инсайдерских атак превышают 60% от общих потерь. Опасность инсайдерских атак связана также с тем, что основное внимание в системе обеспечения информационной безопасности уделяется внешним угрозам и многие организации оказываются практически беззащитными перед внутренними угрозами.

Инсайдер может использовать любой из следующих групп каналов утечки информации при внутренних атаках: сетевые, локальные, незаконное завладение носителем – кража (утеря) носителей, компьютеров и мобильных устройств [1]. В частности, электронная почта остается одним из наиболее опасных каналов утечки информации, широко используемым инсайдерами для несанкционированной передачи конфиденциальной информации или ведения вредоносной

деятельности [2]. Необходимо учитывать, что, так как через Интернет происходит практически такое же количество непреднамеренных утечек информации, вызванных халатностью сотрудников, то защита Интернет-ресурсов является одной из самых актуальных проблем обеспечения безопасности информации предприятия.

Решение данной проблемы сводится к решению двух основных задач: 1) предотвращение (блокирование) передачи конфиденциальной информации через Интернет; 2) расследование инцидентов, связанных с утечкой информации и неправомерным использованием ресурсов Интернет.

К программным способам ограничения доступа к внешним портам и контроля за их использованием относятся такие известные средства, как Pointsec Protector [3], Device Lock [4], Zlock [5] другие. При соответствующей настройке программных продуктов обеспечивается контроль использования внешних портов. При этом копирование информации из корпоративной сети, как правило, запрещается. К системам физического ограничения доступа к внешним портам и жестким дискам рабочих станций относится способ построения защищенной локальной сети с выносными консолями на оптоэлектронных развязках.

По данным компании Info Wath [2], основными виновниками утечки конфиденциальной информации являются сотрудники организации (75,8% – в небольших и средних фирмах, 44,8% – в крупных фирмах). На рисунке 1 представлено распределенеие персонала предприятия как виновников утечки информации.

Рисунок 1. Распределение персонала предприятия как виновников утечки информации
Figure 1. The distribution of personnel as heroes of the information leakage

На основании вышеизложенного можно утверждать, что для обеспечения эффективной работы сотрудников предприятий и предотвращения утечки конфиденциальной информации необходимо проводить постоянный контроль деятельности сотрудников при работе с информацией.

Таким образом, актуальными в организации являются следующие задачи: 1) контроль эффективности деятельности пользователей в информационной системе организации в процессе постоянного (периодического) мониторинга и аудита их деятельности; 2) обеспечение информационной безопасности в организации.

В настоящее время используются следующие методы оценки эффективности работы персонала [6]: метод анкетирования, описательный метод оценки, метод классификации, метод сравнения по парам, метод сравнения, метод заданного распределения, метод оценки по решающей ситуации, метод рейтинговых поведенческих установок и др.

Данные методы используют различные инструменты для оценки эффективности работы персонала. Определено, что для проведения автоматизированной оценки эффективности работы персонала наиболее оптимальным является комбинация методов заданного распределения и оценки на основе моделей компетентности.

Оценка эффективности работы персонала имеет своей целью сопоставить реальное содержание, качество, объем и интенсивность труда персонала с эталонными. Эталонные характеристики работы персонала, как правило, представлены в планах, программах и технологических картах работы предприятия. Оценка эффективности базируется на следующих свойствах: количество, качество, время.

Эффективность использования рабочего времени сотрудником (**Эф**) определяется на основе следующих показателей [7]:

1) относительная оценка использования рабочего времени:

(1)

$$T = \frac{T_t}{T_n} * 100\%$$

где T_t – время, затраченное пользователем на выполнение своих должностных обязанностей, T_n– нормативное время работы пользователя;

2) относительное количество выполненных работ за время : T_t

(2)

$$Q = \frac{Q_t}{Q_n} * 100\%,$$

где Q_t – текущее количество выполненных работ, Q_n – требуемое количество выполненных работ;

3) относительное качество выполненных работ за время : T_t

(3)

$$C = \sum_{i=1}^{Q} \frac{C_{t_i}}{C_n} * 100\%$$

где C_n – требуемое качество выполненных работ, C_t – текущее качество выполненных работ;

4) отсутствие запрещенных действий за время T_n:

(4)

$$P_n = \begin{cases} 0, \text{не обнаружены запрещенные действия} \\ 1, \text{обнаружены запрещенные действия} \end{cases}$$

Анализ формул 1–4 позволяет говорить о проблеме в определении T_t.

Из данных формул видно, что величина эффективности может изменяться от 0 до 100%. Больше 100% эффективность может быть только в случае, если пользователь тратит свое личное время для выполнения поставленных задач, при условии средней производительности его труда.

При $T_t = T_n$ эффективность работы пользователя соответствует 100%. Данные случаи нуждаются в проверке со стороны руководства, так как достижение подобных результатов может быть связано с нарушением режима работы пользователя и не всегда является однозначно хорошим показателем эффективной работы.

При $T_t < T_n$ эффективность работы пользователя менее 100%. Это говорит о том, что во времени работы есть перерывы на другую деятельность. Данный показатель соответствует работе инсайдеров, которые не эффективно используют свое рабочее время.

В этом случае тT_t определяется как:

$$T_t = T_h + T_б, \quad (5)$$

где T_h – это полезное время, в течение которого пользователь решал функциональные задачи; $T_б$ – это бесполезное время, в течение которого пользователь работал как инсайдер, решал другие задачи.

Процесс осуществления несанкционированных действий с информацией и использование каналов утечки информации пользователями-инсайдерами требует значительных затрат времени. Пользователь-инсайдер, как правило, использует часть своего рабочего времени на эти процессы. Эффективность работы пользователя будет максимальной при следующих значениях зависимых переменных: maxT_h (min$T_б$), max Q, max C, min P.

На основании описанной выше математической модели создан программный комплекс «Контроль эффективности работы персонала». Данный программный комплекс позволяет выявить несанкционированные действия пользователя, контролировать каналы утечки на предмет несанкционированного использования и комплексно оценить эффективность использования рабочего времени.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Защита ресурсов Интернет и расследование инцидентов, связанных с инсайдерскими атаками [электронный ресурс] – Режим доступа:http://www.epos.ua/view.php (дата обращения – 11.10.14).
2. Глобальное исследование утечек информации за 2011 год [электронный ресурс] / Info Watch – Режим доступа: http://www.infowatch.ru/ (дата обращения – 11.10.14).
3. DLP–система Pointsec Protector. Режим доступа: http://www.misoft.com.vn/ (дата обращения – 11.10.2014).
4. DLP–система DeviceLock. Режим доступа:www.devicelock.com.
5. DLP–система Zlock. Режим доступа:www.zlock.ru.
6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [электронный ресурс] / Консультант Плюс – Режим доступа: http://base.consultant.ru/ (дата обращения – 11.10.14).
7. *Власова Л.А.* Защита информации: учебное пособие / Власова Л.А. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.

REFERENCES

1. Protection of Internet resources and investigating incidents of insider attacks Mode of access: http: //www.epos.ua/view.php (date accessed 11/10/14).
2. A global study of leakage of information for the year 2011 / Info Watch, Mode of access: http://www.infowatch.ru/ (дата treatment 10/11/14).
3. DLP- system Pointsec Protector. Mode of access: http://www.misoft.com.vn/. (date of treatment: 11/10/2014)
4. DLP- system DeviceLock. Mode of access: www.devicelock.com
5. DLP- system Zlock. Mode of access: www.zlock.ru
6. Federal Law of 27.07.2006 N 149-FZ On Information, Information Technologies and Protection of Information / Consultant - Mode of access:http://base.consultant.ru/cons/cgi/online. (the date of circulation 10/11/14).
7. Vlasova, LA Protection of information [text]: Textbook. Vlasov LA. *Khabarovsk: RIC KSAEL*, 2007.p 84.

Информация об авторе

Максимова Елена Александровна, кандидат технических наук, доцент кафедры «Информационная безопасность»,ФГАОУ ВПО «Волгоградский государственный университет», 400062 г. Волгоград, Россия

Цыбулин Анатолий Михайлович, Кандидат технических наук, Старший Научный Сотрудник, зав. кафедрой «Информационная безопасность»,ФГАОУ ВПО «Волгоградский государственный университет», пр. Университетский, 100, Волгоград, 400062 г. Волгоград, Россия

Свищева Марина Николаевна, Ассистент кафедры «Информационная безопасность», ФГАОУ ВПО «Волгоградский государственный университет», пр. Университетский, 100, 400062 г. Волгоград, Россия

Витенбург Екатерина Александровна, студент, ФГАОУ ВПО «Волгоградский государственный университет», пр. Университетский, 100, Волгоград, 400062 Волгоград, Россия

Получена: 02.11.2014

Information about the author

Maximova Elena Alexandrovna, Candidate for Doctorate in Technics, Associate Professor at the Chair of Information Security, Volgograd State University, 100, University Avenue, 400062 Volgograd city, Russia

Tsybulin Anatoly Mikhaylovich, Candidate for Doctorate in Technics, Senior Staff Scientist, Head of the Chair of Information Security, Volgograd State University, 100, University Avenue, 400062 Volgograd city, Russia

Svischeva Marina,Nikolaevna, Assistant at the Chair of Information Security, Volgograd State University, 100, University Avenue, 400062 Volgograd city, Russia

Vitenburg Ekaterina Alexandrovna, Student, Volgograd State University, 100, University Avenue, 400062

Volgograd city, Russia

Received: 02.11.2014