УДК 004.056.53
DOI: 10.12737/article_5a02fa007ea5c5.44257474

Т.В. Карлова, Н.М. Кузнецова

ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ КРУПНЫХ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ ОТ КОМПЛЕКСНЫХ КИБЕРАТАК

Предложены принципы защиты основных автоматизированных систем промышленных предприятий. Приведены режимы мониторинга внутреннего и внешнего информационного трафика как часть механизма противостояния комплексным кибератакам.

Ключевые слова: защита информации, противостояние кибератакам, мониторинг информационного трафика.

T.V. Karlova, N.M. Kuznetsova

BASIC PRINCIPLES FOR LARGE ENTERPRISE AUTOMATED SYSTEM PROTECTION AGAINST CYBER ATTACKS

A problem to assure automated system protection against cyber attacks is urgent. Modern enterprises face with the problem of information security threat in increasing frequency. These threats are directed not only to information resources, but to software-hardware ones which complicate the solution of the problem specified. Besides, these attacks become more and more sophisticated and have a complex character.

The paper reports the totality of methods for the complex cyber attacks resistance.

The physical isolation principle of the core of the enterprise basic automated system from environment consists in the application of analysis means of information traffic, in particular, in the use of systems of *DLP* class. The use of the technology mentioned envisages special requirements to the structure of information flows and a corresponding enterprise LVS topology.

An information traffic analysis is possible in three modes: automatic, automated and manual.

An automatic mode is intended for monitoring the external information traffic, an automated one – for internal one, manual – for the analysis of data coming in the core of the protected automated system of an enterprise.

A complex application of the presented in the paper protection principles of resources significant strategically for an enterprise will increase an information security level and decrease the probability of the majority of cyber attacks.

Key words: information protection, resistance to cyber attacks, information traffic monitoring.

При проектировании системы защиты от кибератак, направленных на стратегические ресурсы организации (предприятия), необходимо учитывать максимальное количество факторов, влияющих на уровень информационной безопасности.

К стратегическим ресурсам предприятия относятся:

– информационные;
– программные;
– аппаратные.

Основные автоматизированные системы предприятия, как правило, содержат все виды стратегических ресурсов. В связи с этим именно они должны стать объектами защиты.

Система информационной защиты включает в себя комплекс технических и административных мер.

Принцип физической изоляции

Наиболее важным фактором является обеспечение изоляции основных аппаратных ресурсов автоматизированной системы от внешней информационной среды. Достижение абсолютной изоляции невозможно, поэтому необходимо предусмотреть специальный механизм, отслеживающий информационный трафик. Примером подобного механизма служит технология класса *DLP* (*Data Leak Prevention*) – предотвращение утечки данных [1-3].

На рис. 1 представлена схема взаимодействия ресурсов основной автомати-

зированной системы предприятия с внешней информационной средой.

Контроль информационного трафика должен заключаться в детальном анализе данных, транслируемых в обоих направлениях [4; 5].

Анализ информации может проводиться в трёх основных режимах:

– автоматическом (решение принимает сама система контроля);

– автоматизированном (решение принимает оператор на основе проведенного системой контроля анализа);

– ручном (как мониторинг трафика, так и принятие решения осуществляет оператор).

Все перечисленные режимы имеют свои достоинства и недостатки. Рассмотрим подробно каждый из перечисленных режимов.

Рис. 1. Схема взаимодействия автоматизированной системы с внешней информационной средой

Режим автоматического мониторинга информационного трафика

Проведение постоянного автоматического контроля информационного трафика предполагает, что решение о блокировании потока данных принимает соответствующая автоматизированная система информационной безопасности (АСИБ) или определенный ее модуль.

Данный вид контроля уместен при работе со следующими *информационными ресурсами*:

– корреспонденция с заказчиками;

– корреспонденция с поставщиками (сырья, оборудования и т.д.);

– сведения о ситуации на рынке (в том числе на рынке труда).

К контролируемым *программным ресурсам* относятся:

– клиенты почтовых служб;

– браузеры;

– веб-сервисы и т.д.

К контролируемым *аппаратным ресурсам* относятся:

– принтеры;

– факсы;

– рабочие телефоны и т.д.

Режим автоматизированного мониторинга информационного трафика

Данный режим предусматривает, что окончательное решение о блокировании потока данных принимает оператор (человек). Однако все сведения о соответству-

ющем потоке оператору предоставляет АСИБ.

Данный режим мониторинга применим при анализе внутреннего корпоративного трафика и уместен при работе со следующими *информационными ресурсами*:

– детальная информация о проектах и разработках;

– детальная информация о процессах разработок;

– детальные характеристики готовых разработок;

– исходный код программ;

– проектная документация и т.д.

К контролируемым *программным ресурсам* относятся:

– внутренняя почтовая служба;

– корпоративные программные продукты (для внутреннего пользования);

– базы данных (БД) сотрудников предприятия, проектов и разработок и т.д.;

– среды разработок (в том числе среды программирования);

– веб-сервисы внутренней корпоративной сети.

К контролируемым *аппаратным ресурсам* относятся:

– принтеры;

– факсы;

– внутренние телефоны;

– хранилища данных;

– серверные фермы.

Режим ручного мониторинга информационного трафика

Данный режим предусматривает, что и принятие решения, и анализ данных осуществляет оператор (человек).

Данный режим применим к работе со стратегически важными *информационными ресурсами*:

– информация особой важности;

– совершенно секретная информация.

К контролируемым *программным и аппаратным ресурсам* относится ядро основной автоматизированной системы предприятия (включая все составляющие модули, средства телекоммуникации модулей, устройства ввода-вывода и т.д.).

Топология локально-вычислительной сети предприятия

На рис. 2 представлена схема информационных потоков промышленного предприятия.

Таким образом, к автоматическому мониторингу относятся информационные потоки предприятия, исходящие из следующих департаментов:

– департамента маркетинга;

– отдела кадров;

– департамента снабжения;

– департамента экономики;

– департамента связи с общественностью.

Важно отметить, что данные отделы относятся как к автоматическому, так и к автоматизированному мониторингу информационного трафика. В случае обращения сотрудников перечисленных департаментов к внешней среде (Интернет) происходит анализ потока данных в автоматическом режиме. В случае обращения сотрудников к внутренним хранилищам данных (многочисленные БД, серверы хранения информации) запросы контролируются уже в автоматизированном режиме.

В автоматизированном режиме также происходит контроль потока данных между сотрудниками перечисленных отделов и сотрудниками отделов, связанных непосредственно с процессом разработки, к которым относятся:

– программисты;

– конструкторы;

– разработчики;

– специалисты по контролю документации (нормоконтроль);

– сотрудники департамента контроля качества;

– системные администраторы.

–

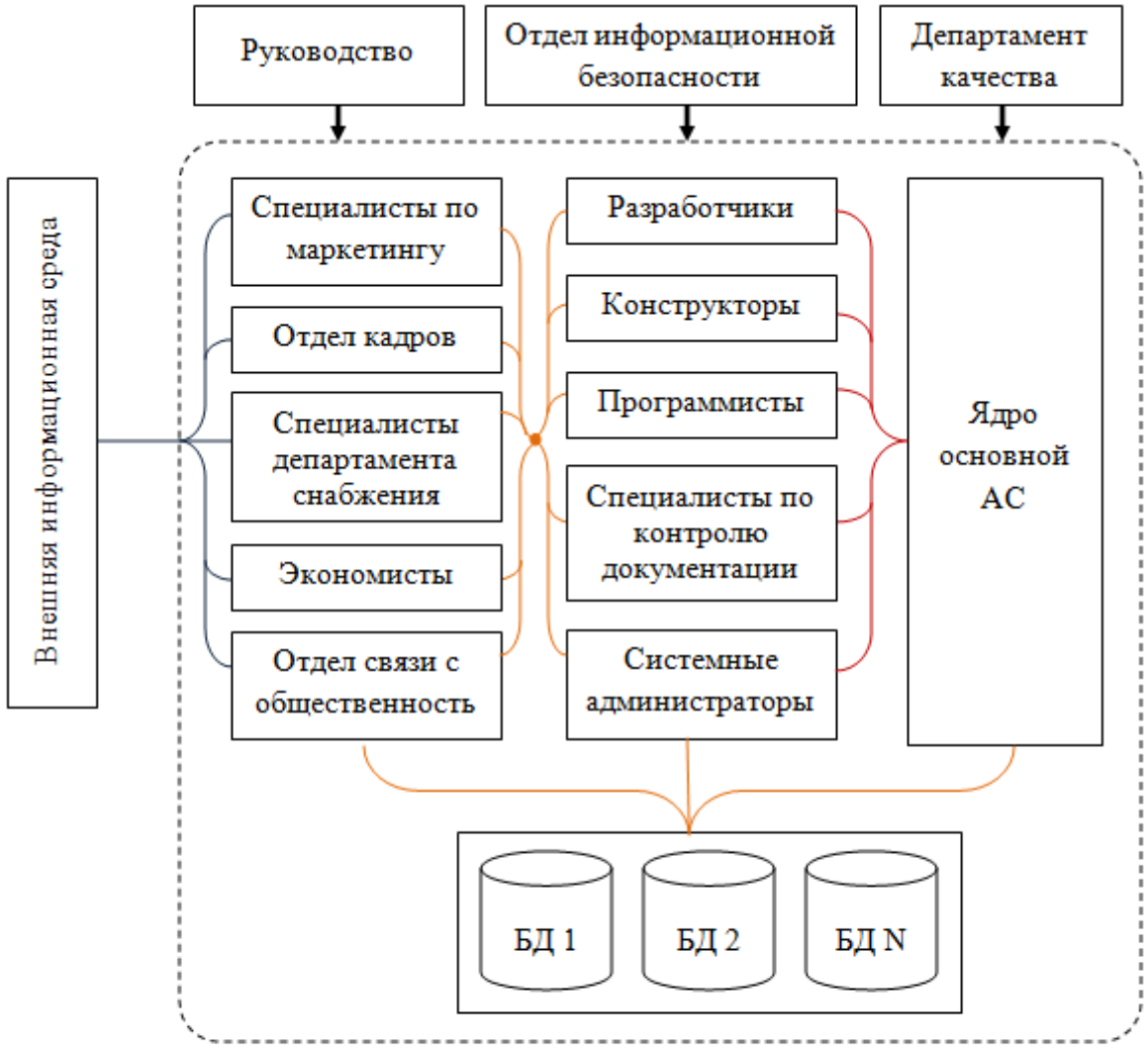

Рис. 2. Схема информационных потоков промышленного предприятия

В том случае, когда сотрудники отделов непосредственной разработки обращаются к ядру основной автоматизированной системы, мониторинг трафика данных осуществляется в ручном режиме.

Важно отметить, что на предприятии должен быть сформирован отдел информационной безопасности, часть должностных обязанностей сотрудников которого заключается в тщательном контроле информационного трафика между сотрудниками подразделений разработки и ядром основной АС предприятия.

Сотрудники отдела контроля качества должны проводить аудит внутренних систем [6]. Также в данной процедуре аудита должны участвовать сотрудники отдела информационной безопасности.

При проведении всех процедур, связанных с обеспечением информационной безопасности автоматизированных систем предприятия, необходимо соблюдать принцип комплексности, при котором для достижения цели применяется совокупность методов защиты [7-9]. При этом срабатывает синергетический эффект, кото-

рый приводит к достижению максимального уровня безопасности.

В качестве методов защиты выступают аппаратно-технические, программные, организационные и т.д. [10].

При построении внутренней информационной системы предприятия необходимо стремиться к физической изоляции ядра основной автоматизированной системы от внешней среды (Интернет) [11].

Эффективное обеспечение технической защиты информации возможно только при наличии компетентных и высокопрофессиональных специалистов в этой области [12].

Таким образом, в качестве основных мер защиты автоматизированных систем промышленного предприятия выступают принцип максимальной физической изоляции ядра системы от внешней информационной среды, а также мониторинг информационного трафика. Мониторинг данных может проводиться в трёх режимах – в зависимости от степени секретности передаваемой информации. В статье представлено применение автоматического, автоматизированного и ручного режимов мониторинга на примере основных информационных потоков предприятия в рамках соответствующей топологии локально-вычислительной сети.

Представленные в статье методы защиты должны применяться в совокупности и коррелировать между собой с целью повышения уровня информационной безопасности предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Карлова, Т.В. Контроль технических каналов утечки информации с помощью технологии Data Loss Prevention в автоматизированной системе разграничения доступа к конфиденциальной информации / Т.В. Карлова, Н.М. Кузнецова // Конкурентоспособность предприятий и организаций: сб. ст. IX всерос. науч.-практ. конф. / МНИЦ ПГСХА. – Пенза: РИО ПГСХА, 2012. – С. 84-87.
2. Кузнецова, Н.М. Классификация каналов утечки конфиденциальной информации на современном промышленном предприятии / Н.М. Кузнецова, Т.В. Карлова // Повышение управленческого, экономического, социального и инновационно-технического потенциала предприятий, отраслей и народно-хозяйственных комплексов: сб. ст. IV междунар. науч.-практ. конф. / МНИЦ ПГСХА. – Пенза: РИО ПГСХА, 2012. – С. 82-85.
3. Криптоанализ сообщений в автоматизированных системах предотвращения утечек информации по каналам связи с применением теории графов / С.А. Шептунов, Т.В. Карлова, Н.М. Кузнецова // Учёные записки Комсомольского-на-Амуре государственного технического университета. – 2015. - Т. 1. - № 4 (24). - С. 33-37.
4. Карлова, Т.В. Разработка концепции обеспечения многоуровневого доступа к конфиденциальной информации / Т.В. Карлова, Н.М. Кузнецова // Вестник МГТУ «Станкин». - 2011. - № 2 (14). - С. 87-90.
5. Карлова, Т.В. Оптимизация доступа к информационным ресурсам / Т.В. Карлова, Н.М. Кузнецова, А.Ю. Бекмешов // Вестник Брянского государственного технического университета. - 2015. - № 3 (47). - С. 135-138.
6. ГОСТ Р ИСО МЭК 15408. Общие критерии оценки безопасности ИТ (Common Criteria for Technology Security Evaluation).
7. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие / П.Б. Хорев. - 4-е изд., стер. - М.: Академия, 2008. - 256 с.
8. Горбатов, В.С. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: учеб. пособие / В.С. Горбатов [и др.]; под общ. ред. Ю.Н. Лаврухина. – М.: НИЯУ МИФИ, 2014. – 560 с.
9. Будников, С.А. Информационная безопасность автоматизированных систем: учеб. пособие / С.А. Будников, Н.В. Паршин. - 2-е изд., доп. - Воронеж: Изд-во им. Е.А. Болховитинова, 2011.
10. Методика управления разграничением доступа к конфиденциальной информации программных проектов промышленного предприятия / Н.М. Кузнецова, Т.В. Карлова // Проблемы развития предприятий: теория и практика: сб. ст. III междунар. науч.-практ. конф. / Пензенский государственный университет, Международная академия организации производства. - 2016. – С. 32-36.
11. Карлова, Т.В. Автоматизированная система разграничения доступа к конфиденциальной информации с модулем контроля на основе усовершенствованного криптоаналитического метода «грубой силы» / Т.В. Карлова, Н.М. Кузнецова // Известия Кабардино-Балкарского государственного университета. - 2012. - Т. II. - № 4. - С. 90-92.
12. Общесистемные вопросы защиты информации: кол. моногр. / под ред. Е.М. Сухарева. - М.: Радиотехника, 2003. - Кн. 1. - 296 с. - (Серия «Защита информации»).

1. Karlova, T.V. Control of technical channels of information outflow using Data Loss Prevention technologies in automated distribution system of access to confidential information / T.V. Karlova, N.M. Kuznetsova // *Enterprise and Company Competitiveness: Proceedings of the IX-th All-Russian Scientific-Pract. Conf.* / MSIC PSAA. – Penza: RIO PSAA, 2012. – pp. 84-87.
2. Kuznetsova, N.M. Classification of confidential information outflow channels at modern enterprise / N.M Kuznetsova, T.V. Karlova // *Increase of Administrative, Economic, Social and Innovation-Technical Potential of Enterprises, Braches and Public-Household Complexes: Proceedings of the IV-th Inter. Scientific-Pract. Conf. / MSIC PSAA*. – Penza: RIO PSAA, 2012. – pp. 82-85.
3. Crypto-analysis of information in automated systems of information outflow prevention through communication channels using theory of graphs / S.A. Sheptunov, T.V. Karlova, N.M. Kuznetsova // *Proceedings of Komsomolsk-upon-Amur State Technical University.* – 2015. – Vol.1. – No.4 (24). – pp. 33-37.
4. Karlova, T.V. Concept development for assurance of multi-level access to confidential information / T.V. Karlova, N.M. Kuznetsova // *Bulletin of MSTU "Stankin"*. – 2011. – No.2 (14). – pp. 87-90.
5. Karlova, T.V. Optimization of access to information resources / T.V. Karlova, N.M. Kuznetsova, A.Yu. Bekmeshov // *Bulletin of Bryansk State Technical University*. – 2015. – No.3 (47). – pp. 135-138.
6. RSS R ISO MEC 15408. *Common Criteria for IT Security Evaluation.*
7. Khorev, P.B. *Methods and Means for Information Protection in Computer Systems*: manual / P.B. Khorev. – 4-th Edition. – M.: Academy, 2008. – pp. 256.
8. Gorbatov, V.S. *Attestation Tests of Automated Systems against Unauthorized Access According to Requirements to Information Security:* manual / V.S. Gorbatov [et al.]; under the general editorship of Yu.N. Lavrukhin. – M.: NINU MEPI, 2014. – pp. 560.
9. Budnikov, S.A. *Information Security of Automated Systems*: manual / S.A. Budnikov, N.V. Parshin. – 2-d Edition, add. – Voronezh: Bolkhovitinov Publishing House, 2011.
10. Procedure for differentiation control of access to confidential information enterprise program projects / N.M. Kuznetsova, T.V. Karlova // *Problems of Enterprise Development: Theory and Practice: Proceedings of the 3-d Inter. Scientific-Pract. Conf.* / Penza State University, International Academy of Production Organization. – 2016. – pp. 32-36.
11. Karlova, T.V. Automated differentiation system of access to confidential information with control module based on updating crypto-analytical method of "brute force" method / T.V. Karlova, N.M. Kuznetsova // *Proceedings of Kabardino-Balkaria State University.* – 2012. – Vol. II. – No.4. – pp. 90-92.
12. *General-system Problems of Information Protection*: collective monograph / under the editorship of E.M. Sukharev. – M.: Radio-engineering, 2003. – B.1. – pp. 296. – (Series "Information Protection").

Статья поступила в редколлегию 5.07.17.
Рецензент: д.т.н., профессор ИКТИ РАН
Шептунов С.А.

Сведения об авторах:

Карлова Татьяна Владимировна, д.с.н., к.т.н., профессор, вед. ст. науч. сотрудник Института конструкторско-технологической информатики РАН, тел.: 8-(499)-978-99-62, 8-(903)-776-90-78, e-mail: karlova-t@yandex.ru.

Karlova Tatiana Vladimirovna, D. S., Can. Eng., Prof., Leading Senior Researcher, Institute of Design-Technological Informatics of RAS, e-mail: karlova-t@yandex.ru

Кузнецова Наталия Михайловна, к.т.н., ст. преподаватель кафедры «Автоматизированные системы обработки информации и управления» Московского государственного технологического университета «СТАНКИН», тел.: 8-(499)-972-94-37, 8-(903)-581-80-15, e-mail: knm87@mail.ru.

Kuznetsova Natalia Mikhailovna, Can. Eng., Senior Lecturer of the Dep. "Automated Systems of Information Processing and Management", Moscow State Technological University "STANKIN", e-mail: knm87@mail.ru.