

УДК 004.057.8.056.5

А.С. Шабуров, А.А. МироноваПермский национальный исследовательский политехнический университет,
Пермь, Россия

О ПОВЫШЕНИИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОТКРЫТОГО ТИПА

Проанализирована актуальная проблема обеспечения безопасности персональных данных в условиях открытости образовательного информационного пространства. Раскрыты особенности информационных систем открытого типа. Сформулировано основное противоречие между необходимостью доступа к информационным ресурсам и обеспечением их конфиденциальности и целостности. Проанализированы уязвимости процедур обработки информации и существующих систем защиты информации. Раскрыт состав подсистем, обеспечивающих информационное взаимодействие в образовательном учреждении. Представлена модель взаимодействия открытой образовательной системы с глобальным информационным пространством. Сформулировано понятие эффективности защиты персональных данных в информационных системах открытого типа. Определена задача построения оптимальной системы защиты информации через разрешение основного противоречия между требованием открытости информационной системы и минимизации времени доступа к информационным ресурсам для санкционированных пользователей. Приведены возможные направления деятельности по совершенствованию системы защиты информации: посредством внедрения более современных средств и способов защиты, использования технологий виртуализации, исследования процесса информационного обмена и поиска оптимальных решений по защите внутреннего образовательного пространства. Рассмотрены основные методы повышения эффективности защиты информации в информационных системах открытого типа. Перечислены основные типы критериев по оценке эффективности защиты информации. Предложен следующий критерий: средства защиты информации должны удовлетворять максимальному количеству требований по защите информации и при этом обеспечивать минимальное время доступа к информационным ресурсам. Разработана математическая модель выбора средств защиты информации в информационных системах открытого типа на основе решения задачи целочисленного линейного программирования. Предложены методы решения поставленной задачи.

Ключевые слова: информационная система персональных данных, система открытого типа, система защиты информации, информационный ресурс, подсистема образовательных услуг, административная подсистема, сетевая подсистема, подсистема удаленного доступа, подсистема обеспечения доступа к глобальным информационным ресурсам, угрозы безопасности, эффективность системы, требования по защите информации, средства защиты.

A.S. Shaburov, A.A. Mironova

Perm National Research Polytechnic University, Perm, Russian Federation

ON IMPROVING THE EFFICIENCY OF PII SECURITY IN INFORMATION SYSTEMS OPEN TYPE

Analyzed the pressing problem of security of personal data in an open educational information space. The features of the information systems of open type. It formulated the basic contradiction between the need for access to information resources and ensuring their confidentiality and integrity. We analyzed the vulnerability of information and procedures for the processing of existing information security systems. Disclosed is part of subsystems that provide information interaction in an educational institution. The model of interaction between the open education system with the global information space. Formulated the concept of the protection of personal data in information systems of the open type. It defines the tasks of constructing an optimal information security systems through a resolution of the basic contradiction between the requirements of the open information system and minimize the time access to information resources for authorized users. The possible directions for improvement of the system of information security: through the introduction of more modern means and methods of protection, the use of virtualization technology, the study of the process of information exchange and the search for optimal solutions to protect the domestic educational space. The main methods of increasing the effectiveness of information security in the information systems of open type. List the main types of criteria for assessing the effectiveness of information security. We propose the following criterion: data protection must meet the maximum number of requirements for data protection while providing minimum time access to information resources. A mathematical model of choice of means of protection of information in information systems based on open-solving integer linear programming problem. The methods of solving this problem.

Keywords: Personally Identifiable Information (PII) system, open systems, systems of information security, information resources, subsystem of educational services, administrative subsystem, network subsystem, remote access subsystem, subsystem providing access to global information resources, security threat, system efficiency, requirements of information security, security facilities.

В настоящее время проблема обеспечения безопасности персональных данных (ПДн) приобрела значительную актуальность. Особенно это характерно для информационных систем персональных данных (ИС ПДн), предназначенных для обработки в условиях открытости информационных ресурсов. К данному классу систем относятся ИС ПДн образовательных учреждений, для которых характерно построение открытого образовательного пространства [1].

Особенностями системы открытого типа являются широта взаимосвязи с внешним миром, высокая степень интеграции на основе информационных технологий. В то же время подобные системы, ориентированные на оказание образовательных услуг, сосредоточивают значительные объемы сведений конфиденциального характера. Это могут быть личные данные учащихся и работников, индивидуальные инновационные решения в организации учебного процесса, результаты

научной деятельности, полученные на договорной основе, что предполагает ограничение на доступ к информации.

Информационное взаимодействие открытых образовательных систем, как правило, предполагает участие множества участников информационного обмена – пользователей информационных ресурсов: учащихся учебных заведений, преподавателей, специалистов административно-управленческого аппарата, работодателей. Информационный обмен также включает участие специалистов государственных и частных структур, родственников учащихся, иных заинтересованных лиц.

Вместе с тем в последнее время существенно обострилась ситуация с пропагандой экстремистской деятельности. Практика показывает, что значительное проникновение в студенческую среду материалов экстремистской направленности обусловлено открытостью информационной среды, развитием информационных технологий социального взаимодействия, доступностью ПДн учащихся для злоумышленников [2].

Таким образом, с одной стороны, открытость образовательной среды позволяет качественно повысить уровень взаимодействия участников образовательного процесса через интеграцию информационных систем. С другой стороны, возникает необходимость решения задач защиты информации, что в условиях открытости образовательного пространства зачастую носит нетривиальный характер.

Основными задачами в области обеспечения безопасности образовательного пространства могут являться [3]:

1. Разработка и внедрение нормативно-правовых, научно-методических и организационных основ деятельности системы образования по формированию безопасного образовательного пространства.
2. Нарращивание опыта межведомственного, комплексного и многоуровневого подходов к формированию безопасного образовательного пространства.
3. Совершенствование профессиональной компетентности и механизмов аттестации работников образования в области формирования безопасного образовательного пространства.
4. Совершенствование механизмов аттестации образовательного учреждения по созданию медико-социальных условий, обеспечивающих безопасность и сохранение здоровья участников образовательного процесса.

5. Разработка критериев эффективности деятельности образовательного учреждения по формированию безопасного образовательного пространства.

Повсеместное внедрение информационных технологий в открытом образовательном пространстве предполагает активную информационную поддержку всех процессов, происходящих в образовательном учреждении. Использование системного подхода предполагает внедрение нескольких традиционных подсистем, обеспечивающих информационное взаимодействие (рисунок):

- подсистему образовательных услуг;
- административную подсистему;
- сетевую подсистему;
- подсистему удаленного доступа;
- подсистему обеспечения доступа к глобальным информационным ресурсам.

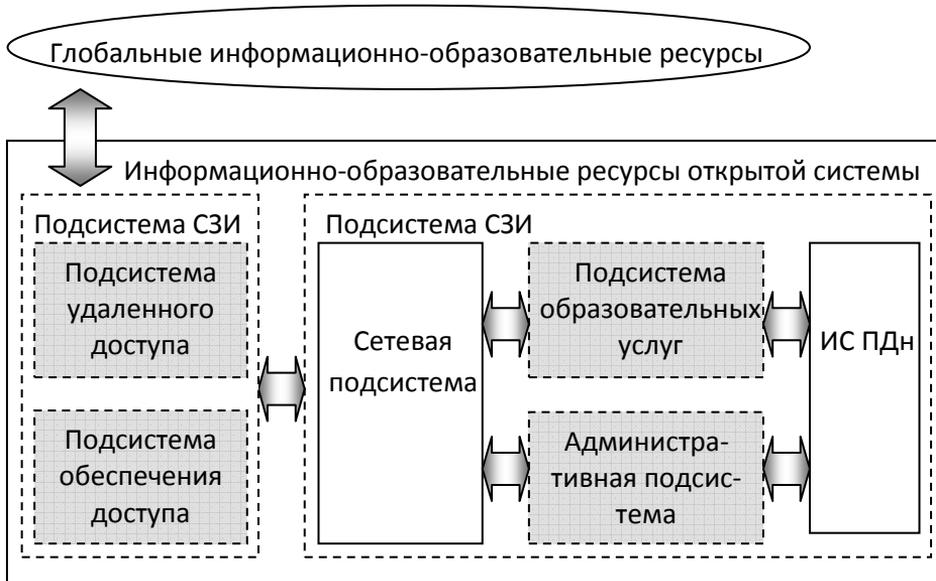


Рис. Взаимодействие открытой образовательной системы с глобальным информационным пространством

Для обеспечения стабильного функционирования подобной структуры система защиты информации должна быть интегрирована во все ее компоненты, предполагая выполнение основных сервисов безопасности, определенных политикой конкретной образовательной

среды. При этом ПДн являются неотъемлемой частью процесса информационного обмена.

Решения в области информационной безопасности традиционно предполагают управление выбранными способами и средствами защиты информации путем обеспечения ее конфиденциальности, целостности и доступности. Защита информации должна работать как инструмент достижения вышеназванных критериев для того, чтобы избежать или снизить соответствующие риски злоумышленного нанесения ущерба электронному контенту образовательной среды или ее пользователю, обеспечивая необходимый уровень доступности информации [4].

Взаимосвязь государственных и частных сетей и совместное использование информационных ресурсов увеличивают трудность достижения поставленных целей защиты и управления доступом. Переход на технологию распределенной обработки данных также ослабляет результативность централизованного, специализированного управления, снижает эффективность использования традиционных методов и средств защиты информации, в частности ПДн.

Как правило, реализуемый комплекс мероприятий по обеспечению безопасности ПДн при их обработке в ИС ПДн включает в себя перечень определенных требований по обработке и защите информации, регламентирует порядок допуска лиц к процедурам обработки данных и утверждается внутренним локальным актом образовательного учреждения [5].

В то же время несовершенство процедур обработки информации и существующие уязвимости системы защиты приводят к утечкам информации, размещению ПДн в открытых источниках. Это, в свою очередь, снижает эффективность, реализуемых на практике требований, может создавать потенциальную опасность для участников информационного обмена, что требует поиска новых решений по повышению эффективности защитных мероприятий.

Под эффективностью защиты ПДн в информационных системах открытого типа понимается ее качественное состояние, обеспечивающее необходимую степень открытости образовательного информационного пространства, с учетом выполнения требований по защите информации для участников информационного обмена.

Построение оптимальной системы защиты информации (СЗИ) предполагает разрешение основного противоречия между требованием

открытости информационной системы и минимизации времени доступа к информационным ресурсам для санкционированных пользователей. При этом предполагается выполнение требований по защите информации и ограничению доступа в ИС ПДн для злоумышленника и блокированию каналов утечки информации [6].

Повышение эффективности предпринимаемых мер может осуществляться на основе совершенствования технологий обработки информации и внедрения более современных средств и способов защиты с использованием технологий виртуализации [7], исследования процесса информационного обмена и поиска оптимальных решений по защите внутреннего образовательного пространства [8].

Задачу повышения эффективности СЗИ ИС ПДн можно представить как задачу выбора необходимого состава средств защиты информации, которые позволяют получить наиболее рациональную структуру и в ее рамках сформировать оптимальный состав средств, обеспечивающих перекрытие всех выявленных угроз безопасности, требуемый уровень защищенности ПДн.

Во многих случаях качественных оценок оказывается недостаточно, кроме того, количественные методы более точны. Однако для «измерения» эффективности необходимо иметь обоснованный критерий (показатель оценки эффективности системы). На практике встречаются следующие типы критериев [9]:

- критерии типа «эффект – затраты», позволяющие оценивать достижение целей функционирования СЗИ при заданных затратах (так называемая экономическая эффективность);

- критерии, позволяющие оценить качество СЗИ по определенным показателям и исключить те варианты, которые не удовлетворяют заданным ограничениям. При этом используются методы многокритериальной оптимизации, восстановления функций и функционалов, методы дискретного программирования;

- искусственно сконструированные критерии, позволяющие оценивать интегральный эффект (например, «линейная свертка» частных показателей, методы теории нечетких множеств).

Следует учитывать, что СЗИ в целом является сложным объектом, выполняющим множество функций. Для каждого структурного элемента СЗИ и выполняемой функции возможно применение различных программных и технических средств как представленных на

рынке, так и перспективных. Следовательно, в конкретном случае можно построить множество вариантов СЗИ, отличающихся структурой, составом, технико-экономическими показателями (быстродействие, надежность, стоимость и т.д.). Поскольку подобные показатели нередко бывают взаимно противоречивы, то выбор конкретного комплекса средств защиты информации приводит к необходимости решать оптимизационную задачу, требующую наличия показателей эффективности ЗИ и соответствующих критериев построения защиты.

Применительно к рассматриваемой задаче выбора средств защиты информации ИС ПДн будем использовать следующий критерий: средства защиты информации должны удовлетворять максимальному количеству требований по защите информации и при этом обеспечивать минимальное время доступа к информационным ресурсам.

Пусть исходная i -я система при заданной вероятности защиты $P_{\text{защ}}(0)$ и времени доступа $T(0)$ может быть спроектирована в различных вариантах: $i_1, i_2, i_3, \dots, i_j$, с применением различных средств защиты информации. При этом защищенность информации оценивается по приращению вероятности ее защиты Δp_i и по приращению времени доступа к ресурсам Δt_i из-за необходимости преодоления рубежей безопасности. Параметром системы также может быть ее стоимостная характеристика C_i .

Рассмотрим систему защиты информации, характеризующуюся рядом параметров:

$$F_i = f(\Delta p_i, \Delta t_i, \Delta c_i), \quad i = \overline{1, m}. \quad (1)$$

В общем случае алгоритм функционирования системы задан, при котором алгоритм доступа представляет собой q этапов, на каждом из которых может быть применена некоторая совокупность средств $n_k \in N, k = \overline{1, q}$ из множества допустимых. Если оптимизация проводится по одному или двум критериям, то остальные рассматриваются как ограничения.

Пусть часть критериев СЗИ $i = \overline{1, r}$ улучшается, а остальная часть $i = \overline{r+1, m}$ ухудшается в случае применения одного из средств защиты. Обозначим: α_{kj} – относительное изменение i -го параметра $i = \overline{r+1, m}$ на k -м этапе в случае применения j -го средства защиты;

S_{kij} – эффективность применения j -го средства на k -м этапе по i -му критерию $i = \overline{1, r}$; b_i – требуемое значение i -го критерия.

В случае многокритериальной оптимизации, применение которой имеет смысл тогда, когда ухудшение по одному из параметров приводит к улучшению по другим параметрам, имеет смысл задача целочисленного программирования с несколькими целевыми функциями:

$$\left. \begin{aligned} F_i &= \sum_{k=1}^q \sum_{j=1}^{n_k} S_{kij} x_{kj} \rightarrow \max \\ F_i &= \sum_{k=1}^q \sum_{j=1}^{n_k} S_{kij} x_{kj} \rightarrow \min \end{aligned} \right\} \begin{aligned} i &= \overline{r+1, m} \\ i &= \overline{1, r} \end{aligned} \quad (2)$$

при ограничениях:

$$\sum_{k=1}^q \sum_{j=1}^{n_k} a_{kij} x_{kj} \neq b_i, \quad (3)$$

$$x_{kj} = \begin{cases} 1 & \text{– если } j\text{-е средство применяется на } k\text{-м этапе,} \\ 0 & \text{– если } j\text{-е средство не применяется на } k\text{-м этапе,} \end{cases}$$

где $j = \overline{1, n_k}$; $k = \overline{1, q}$.

В результате решения подобной задачи должен быть определен оптимальный выбор структуры СЗИ, т.е. набор способов защиты ПДн, обращающий в экстремум целевые функции, при выполнении ограничений.

Таким образом, получим задачу целочисленного линейного программирования, для решения которой может быть использован ряд методов [10]:

- методы отсечения, базирующиеся на использовании процедуры линейного программирования для последовательности задач, в которую по мере решения вводятся особые дополнительные ограничения;

- комбинаторные методы, в которых вместо процедуры линейного программирования используют сокращение поиска возможных решений с помощью анализа исходного множества решений;

- приближенные методы, применяющиеся для задач большой размерности, решение которых в значительной степени может быть затруднено дефицитом временных и технических ресурсов;

– человеко-машинные методы, требующие значительных вычислений.

Таким образом, совершенствование образовательной среды и ее интеграция в глобальное информационное пространство приводят к повышению открытости информационных образовательных систем, что, в свою очередь, обуславливает появление уязвимостей ИС ПДн. Повышение эффективности защиты конфиденциальной информации в информационных системах открытого типа предполагает постоянное совершенствование предпринимаемых мер по обеспечению информационной безопасности на основе внедрения современных технологий защиты, а также поиска оптимальных решений для совершенствования системы защиты информации.

Библиографический список

1. Данилов А.Н., Шабуров А.С. О проблеме информационной безопасности открытых образовательных систем // Информационные войны. – 2013. – № 1(25). – С. 89–94.

2. Коренева Е.Н., Косолапов А.Н. Экстремизм как явление и формирование в студенческой среде ценностной установки на толерантность [Электронный ресурс]. – URL: http://www.rusnauka.com/29_DWS_2011/Pedagogica/2_95292.doc.htm (дата обращения: 10.08.2015).

3. Пилипенко В.Ф., Ерков Н.В., Парфенов А.А. Обеспечение комплексной безопасности в образовательном учреждении. Теория и практика. – М.: Айрис-пресс, 2006. – 192 с.

4. Данилов А.Н., Шабуров А.С. Основные направления обеспечения информационной безопасности открытых образовательных систем // Информационные войны. – 2013. – № 1(25). – С. 77–82.

5. Положение о порядке обработки и обеспечении безопасности персональных данных Пермского национального исследовательского политехнического университета [Электронный ресурс]. – URL: http://pstu.ru/files/file/oksana/2012/universitet/osnsovnye_dokumenty/polozhenie_o_poryadke_obrabotki_i_obespecheniya_bezopasnosti_pdn.pdf (дата обращения: 16.07.2015).

6. Шабуров А.С., Юшкова С.А., Бодерко А.В. Моделирование оценки угроз безопасности информационных систем персональных данных // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2013. – № 7. – С. 149–159.

7. Шабуров А.С., Рашевский Р.Б. Практическое применение VMWARE VSHIELD APP для обеспечения безопасности виртуального веб-сервера // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2014. – № 11. – С. 94–101.

8. Шабуров А.С., Рашевский Р.Б. Реализация отказоустойчивого распределенного межсетевоего экрана // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2014. – № 11. – С. 129–136.

9. Булдакова Т.И., Глазунов Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота // Доклады ТУ-СУРа. – 2012. – № 1(25), ч. 2.

10. Палий И.А. Линейное программирование: учеб. пособие. – М.: Эксмо, 2008.

References

1. Danilov A.N., Shaburov A.S. O probleme informatsionnoi bezopasnosti otkrytykh obrazovatel'nykh sistem [On the issue of information security of public educational systems]. *Informatsionnye voiny*, 2013, no. 1(25), pp. 89-94.

2. Koreneva E.N., Kosolapov A.N. Ekstremizm kak iavlenie i formirovanie v studencheskoi srede tsennostnoi ustanovki na tolerantnost' [Extremism as a phenomenon and the formation of tolerance value system among students], available at: http://www.rusnauka.com/29_DWS_2011/Pedagogica/2_95292.doc.htm (accessed 10 August 2015).

3. Pilipenko V.F., Erkov N.V., Parfenov A.A. Obespechenie kompleksnoi bezopasnosti v obrazovatel'nom uchrezhdenii. Teoriia i praktika [Integrated safety and security arrangements at educational institution. Theory and practice]. Moscow: Airis-press, 2006. 192 p.

4. Danilov A.N., Shaburov A.S. Osnovnye napravleniia obespecheniia informatsionnoi bezopasnosti otkrytykh obrazovatel'nykh sistem [The principle directions of information security supply of public educational systems]. *Informatsionnye voyny*, 2013, no. 1(25), pp. 77-82.

5. Polozhenie o poriadke obrabotki i obespechenii bezopasnosti personal'nykh dannykh Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta [Regulations on the procedure of Perm National Research Polytechnic University personal data processing and security], available at: http://pstu.ru/files/file/oksana/2012/universitet/osnsovnye_dokumenty/polozhenie_o_poryadke_obrabotki_i_obespecheniya_bezopasnosti_pdn.pdf (accessed 16 July 2015).

6. Shaburov A.S., Iushkova S.A., Boderko A.V. Modelirovanie otsenki ugroz bezopasnosti informatsionnykh sistem personal'nykh dannykh [The risk assesment modelling of personal data information systems security]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2013, no. 7, pp. 149-159.

7. Shaburov A.S., Rashevskii R.B. Prakticheskoe primenenie VMWARE VSHIELD APP dlia obespecheniia bezopasnosti virtual'nogo veb-servera [Practical application of VMWARE VSHIELD APP for the virtual web server safety supply]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2014, no. 11, pp. 94-101.

8. Shaburov A.S., Rashevskii R.B. Realizatsiia otkazoustoichivogo raspredelennogo mezhsetevogo ekrana [Implementation of the distributed failover network firewall]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2014, no. 11, pp. 129-136.

9. Buldakova T.I., Glazunov B.V., Liapina N.S. Otsenka effektivnosti zashchity sistem elektronnoho dokumentooborota [The assesment of e-document management systems performance security]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki*, 2012, no. 1(25), part 2.

10. Palii I.A. Lineinoe programmirovaniye [Linear programming]. Moscow: Eksmo, 2008.

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматизации и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Миронова Анна Алексеевна (Пермь, Россия) – студентка Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: mir550@yandex.ru).

About the authors

Shaburov Andrey Sergeevich, (Perm, Russia) is a Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Mironova Anna Alekseevna (Perm, Russia) is a student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: mir550@yandex.ru).

Получено 05.10.2015