ИНТЕЛЛЕКТУАЛЬНЫЕ МЕХАНИЗМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СРЕДЕ ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА

Надеждин Е.Н.

Одной из ведущих тенденций в области автоматизации управления деятельностью образовательных учреждений (ОУ) является создание и развитие интегрированных систем управления (ИСУ) с распределенной сетевой инфраструктурой [2; 3; 9]. Технологический базис ИСУ составляют автоматизированные информационные системы (АИС), локальные вычислительные сети, системы коммуникации и средства обеспечения. Интеграция информационно-образовательных сетей (ИОС) ОУ в мировое образовательное пространство на фоне растущей киберпреступности стимулирует поиски новых подходов к решению проблемы обеспечения информационной безопасности (ИБ) личности, общества и государства [6; 7; 8].

Целью статьи является выявление особенностей обработки персональных данных в ИОС педагогического университета и обоснование интеллектуальных функций механизма защиты персональных данных (МЗПД) как перспективного способа обеспечения комплексной защиты информации в ИСУ ОУ в условиях вероятных информационных угроз.

Персональными данными (ПД) в соответствии со ст. 3 Закона № 152-ФЗ [7] является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе: фамилия, имя, отчество; год, месяц, дата и место рождения; адрес; семейное, социальное, имущественное положение, образование, профессия, доходы, информация о состоянии здоровья. В соответствии со ст. 85 Трудового Кодекса РФ к персональным данным работника относится также информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

В составе ИСУ педагогического университета можно выделить несколько относительно автономных АИС, функционалы которых в разной степени связаны с процессом сбора и обработки ПД обучающихся (студентов, слушателей, аспирантов) и штатных сотрудников (преподавателей, административных работников, вспомогательного персонала). К таким системам следует отнести: а) АИС «Студенты»; б) АИС «Кадры»; в) АИС «Финансы»; г) АИС «Делопроизводство». Учитывая специфику преобразуемой информации, указанные АИС в технической литературе называют информационными системами обработки персональных данных.

По современным взглядам [7], защита персональных данных представляет собой *комплекс мер правового, организационного, организационно-технического и технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных (работнику).* Конечной целью защиты персональных данных в подсистемах и компонентах ИСУ ОУ является защита прав и свобод каждого человека при автоматизированной обработке его персональных данных, в т.ч. защита декларированных Конституцией РФ прав и свобод гражданина на неприкосновенность частной жизни, личную и семейную тайну.

Используемая в ОУ ВПО система защиты персональных данных должна обеспечивать нейтрализацию всех актуальных угроз ПД. Система защиты ПД представляет собой комплекс аппаратных, программных, криптографических средств и организационных мер, учитывающих специфику защищаемого объекта и требования корпоративной политики ИБ. По функциональному признаку в составе системы защиты ПД выделяют ряд подсистем (рис. 1): подсистему антивирусной защиты; подсистему управления доступом; подсистему анализа защищенности: подсистему криптографической защиты, подсистему обнаружения вторжений; подсистему регистрации и учета (действий пользователей).

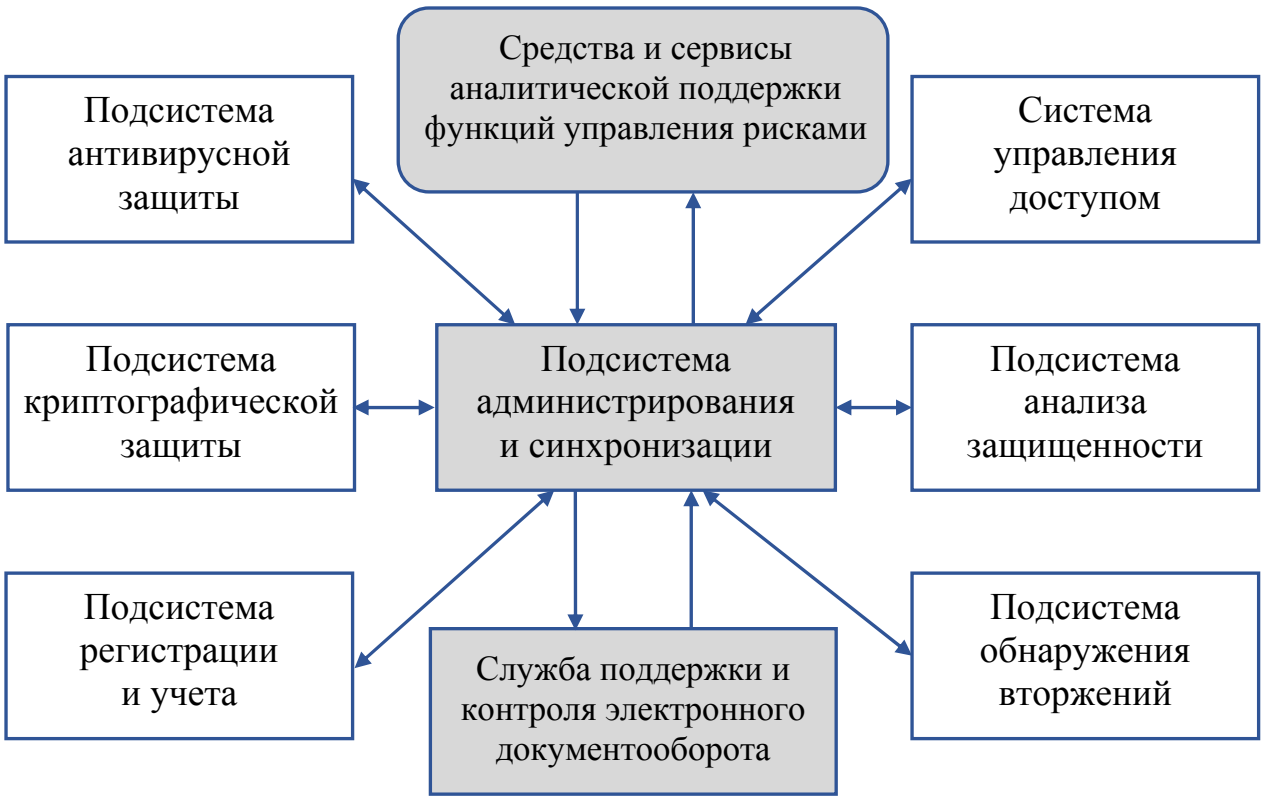

Рис. 1. Укрупненная блок-схема системы защиты ПД

С учетом требований действующих нормативных и правовых документов и накопленного опыта системного администрирования в области обеспечения информационной безопасности выделим основные этапы организационной работы должностных лиц педагогического университета по защите ПД:

1) определение всех ситуаций, когда требуется проводить обработку ПД;

2) выделение процессов, в которых обрабатываются ПД;

3) выбор ограниченного числа процессов для проведения аналитики, в том числе: формирование перечня подразделений и списка работников, участвующих в обработке ПД в рамках своей служебной деятельности;

4) определение режимов обработки и совокупности обрабатываемых ПД;

5) проведение категорирования ПД и типизации АИС;

6) разработка пакета организационно-распорядительных документов для обеспечения защиты ПД (положения, приказы, акты, инструкции и т.п.);

7) разработка плана создания и внедрения новой или модернизации существующей системы обеспечения безопасности ПД;

8) осуществление комплекса мероприятий по обеспечению процесса защиты ПД на различных уровнях (организационном, техническом, физическом, технологическом).

В общем случае защита ПД обучающихся и работников педагогического университета сводится к созданию и поддержанию специального режима автоматизированной обработки ПД, включающего:

1) создание и корректировку внутренней документации по работе с ПД;

2) организацию и поддержание в актуальном состоянии всех компонентов системы защиты ПД;

3) внедрение инновационных мер защиты и контроля конфиденциальности ПД, адекватных текущим и вновь возникающим угрозам.

Изучение предметной области информационной безопасности ОУ ВПО на этапе глобализации информационного образовательного пространства дало основание выделить наиболее вероятные угрозы персональным данным. К ним, прежде всего, следует отнести следующие угрозы [5; 6]:

1. Угрозы от утечки по техническим каналам: угрозы утечки акустической информации; угрозы утечки видовой информации; угрозы утечки информации по открытым каналам связи.

2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам АИС, носителям персональных данных, ключам и атрибутам доступа: кража и уничтожение носителей информации; кража физических носителей ключей и атрибутов доступа; утрата носителей информации; утрата и компрометация ключей и атрибутов доступа.

3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств: доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа; утечка информации через порты ввода/вывода; воздействие

вредоносных программ (вирусов); установка программного обеспечения, не связанного с исполнением служебных обязанностей; внедрение или сокрытие недекларированных возможностей системного программного обеспечения, а также программного обеспечения для обработки ПД; создание учетных записей «теневых» пользователей и неучтенных точек доступа в систему.

4. Угрозы несанкционированного доступа к информации по каналам связи: угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны; угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций АИС, топологии сети, открытых портов и служб, открытых соединений и др.; угрозы выявления паролей по сети; угрозы типа «Отказ в обслуживании»; угрозы внедрения по сети вредоносных программ; утечка информации, передаваемой с использованием протоколов беспроводного доступа; перехват, модификация закрытого ключа ЭЦП; угрозы удаленного запуска приложений.

5. Угрозы антропогенного характера: разглашение информации; сокрытие ошибок и неправомерных действий пользователей и администраторов; угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей; угроза нарушения политики предоставления и прекращения доступа; непреднамеренная модификация (уничтожение) информации; непреднамеренное отключение средств защиты.

6. Угрозы воздействия непреодолимых сил: стихийное бедствие; выход из строя аппаратно-программных средств; аварии (пожар, потоп, случайное отключение электричества).

Рассмотрим общие угрозы сетевой и информационной безопасности. Как известно, активы (ресурсы) сервисов и других электронных сервисов ОУ ВПО должны быть в достаточной степени защищены для сохранения подлинности, конфиденциальности, целостности и доступности этих сервисов.

Активы данных электронных сервисов включают в себя:

- данные о юридических и физических лицах, использующих электронные сервисы;
- активы (ресурсы), использующиеся при предоставлении сервисов научной и образовательной деятельности ОУ и коммерческой деятельности организации, предоставляющей эти сервисы (например, трафик, компьютерные системы, сети, информацию);
- данные и информация, связанные с удаленным управлением подключенной к сетям стендовой аппаратуры, бытовой техники, а также оборудования, находящегося в местах проживания пользователей;
- аутентификационная информация пользователей электронных сервисов.

Опыт показывает, что безопасность каждого пользователя (студента, слушателя, преподавателя) АИС, его здоровье, репутация и финансовое благосостояние являются важными активами ОУ, которые могут привлекать внимание злоумышленников, нередко являющихся представителями криминальных структур. Угрозы активам сервисов управления персоналом и, в целом, деятельностью ОУ и других электронных сервисов разделим на две категории: первая – системные и прикладные угрозы и вторая – угрозы инфраструктуре. Такая градация позволит проиллюстрировать разнообразие типов угроз и активов, которые могут пострадать при реализации этих угроз.

Д1. Данные, передаваемые по электронным каналам связи, которые могут быть перехвачены, скопированы или модифицированы. Это может нанести ущерб людям из-за того, что подробности их частной жизни станут известны кому-то еще, а перехваченные данные использованы во вред им; например, несанкционированная модификация и искажение перехваченных данных может угрожать служебной карьере и имиджу пользователей.

Д2. Несанкционированный доступ в компьютеры и компьютерные сети обычно выполняется злоумышленниками с намерением скопировать, изменить или уничтожить данные и может осуществляться не только в

обычные компьютеры, но и в различные локальные сети и автоматическое оборудование или в мобильные устройства (мобильные телефоны и планшетные компьютеры).

Д3. Вредоносное программное обеспечение (вирусы) может отключить компьютеры или мобильные устройства, уничтожить или модифицировать данные или изменить настройки электронного оборудования. Статистика компьютерных преступлений показывает, что некоторые вирусные атаки на сайты научных и образовательных учреждений могут весьма разрушительными.

Д4. Обман людей или организаций с целью заставить их выполнить нужные злоумышленнику действия (социальная инженерия) может принести существенный ущерб. Например, пользователи могут загрузить вредоносное программное обеспечение с виртуального web-сайта, который выдает себя за доверенный web-сайт организации-поставщика программного обеспечения; люди могут стать жертвой «кражи личности» (хищения информации, содержащейся в удостоверяющих личность документах, для совершения мошенничества) или «фишинга» (незаконного получения конфиденциальной информации через электронную почту при помощи запросов, которые выглядят как официальные письма, например, от банка, будто бы желающего уточнить данные клиента); клиенты организации могут расторгнуть с ней контракты; конфиденциальная информация может быть отправлена посторонним лицам.

Д5. Непредвиденные и непреднамеренные инциденты безопасности, такие как аппаратные или программные отказы, техническая ошибка неопытного пользователя, неадекватное поведение пользователей, или стихийные бедствия (отключение электричества) могут привести к потере или повреждению активов учреждения.

Д6. Несанкционированная расшифровка научного и образовательного контента, защищенного авторскими правами (патентов, учебников, тестов, методических разработок, заданий олимпиад и конкурсов) и/или его

копирование и/или его распространение в Интернете угрожают авторским правам и платным службам предоставления контента.

Д7. Внешние угрозы осуществлению образовательной деятельности в конкретном ОУ за счет введения дезинформации, фиктивных жалоб и заявлений от пользователей глобальной сети.

Д8. Разрушительные атаки в Интернете стали весьма распространены. Телефонные сети (как фиксированной, так и мобильной связи) становятся более уязвимыми из-за перехода их на использование Интернет-технологий (например, IP-телефонии – VoIP). Эти атаки включают: спам с помощью VoIP, отказ в обслуживании (DOS) и распределенный отказ в обслуживании (DDoS –атаки).

Угрозам ***Д1…Д8*** можно противостоять с помощью целого ряда сервисов безопасности. Каждый из этих сервисов безопасности включает в себя ряд технических, организационных и управленческих механизмов защиты.

Выделим основные сервисы обеспечения ИБ [5].

1. Регистрация, аутентификация и управление доступом. Эти сервисы обеспечивают гарантированную идентификацию пользователей и предоставление им доступ только к тем активам, к которым им разрешен доступ. Общая безопасность сервисов ОУ и их активов зависит в конечном счете от возможности аутентифицировать пользователей системы. Эти сервисы также включают в себя аутентификацию всех других сущностей, помимо человека, таких как организации, системы, устройства, приложения/службы, или их компоненты.

2. Сервисы конфиденциальности и защиты персональных данных. Эти сервисы обеспечивают функционирование средств, с помощью которых защищенным образом хранится и передается информация сервисов научной, образовательной и других видов деятельности (включая идентификаторы пользователей, участвующих в передаче такой информации). Сервисы

гарантируют защищенность ПД (таких как биографические и медицинские данные) в соответствии с законодательством.

3. Сервисы доверия. Эти сервисы требуются, например, для обеспечения гарантии того, что финансовые транзакции (в финансовой деятельности ОУ) протоколируются и можно установить ответственных за них аутентифицированных пользователей, и эти пользователи не могут отказаться от совершенных ими транзакций. Такие сервисы позволяют поставщикам электронных услуг и их клиентам совершать сделки в электронной форме.

Типовая операция враждебного воздействия (злоумышленника) в общем случае содержит следующие этапы [6; 5]:

1) подготовительный;

2) несанкционированный доступ;

3) основной (разведывательный или диверсионный);

4) скрытая передача информации (основной или вспомогательной);

5) сокрытие (маскировка) следов воздействия.

Чем раньше по времени будет обнаружена и идентифицирована информационная угроза инструментами системы комплексной защиты информации, тем менее значительным будет ущерб для ОУ. Именно поэтому при разработке СКЗИ особое внимание уделяют вопросам разработки методов и средств осуществления информационно-аналитических функций механизмов защиты ПД (МЗПД). Отметим, что основу системы защиты ПД, составляют, как правило, организационные и организационно-технические методы защиты.

На практике используют следующие организационные меры защиты: физический, телевизионный или электронный контроль доступа в контролируемую зону, установка охранной сигнализации, фиксация входа с помощью электронного замка, установка решеток на первых и последних этажах зданий; учет используемых носителей информации; особый режим хранения носителей информации; назначение сотрудника, ответственного за обеспечение безопасности ПД; периодические внутренние проверки режима

безопасности ПД; введение парольной политики, устанавливающей сложность ключей и атрибутов доступа (паролей), а также их периодическую смену; проведение инструктажа пользователей о порядке работы и защиты ПД; резервное копирование защищаемой информации; установка пожарной сигнализации в помещениях, где расположены элементы АИС; использование источников бесперебойного питания.

В настоящее время в подсистемах ИСУ ОУ успешно реализуется концепция комплексной защиты информации, которая заключается в рациональном комплексировании методов и средств, построенных на различных физических и технологических принципах. Непредсказуемость и неопределенность характеристик угроз информации вынуждает искать новые способы реализации известных требований к системе защите информации:

а) универсальность;

б) гибкость;

в) адаптивность;

г) активность;

д) иерархичность;

е) непрерывность.

Характерной особенностью современных систем комплексной защиты информации в ИСУ педагогического университета является осуществление концепции управления рисками информационной безопасности. В этом отношении приоритетными следует считать задачи разработки методик и инструментальных программных средств, поддерживающих функции сбора и интеллектуального анализа текущей информации о состоянии информационных и вычислительных ресурсов подсистем ИСУ. Выделим группу специальных задач, решение которых направлено на автоматизацию процесса управления рисками информационной безопасности:

а) анализ и ранжирование информационных угроз;

б) анализ уязвимостей в системе защиты;

в) анализ (моделирование, оценивание и прогнозирование) рисков ИБ;

г) оптимизация характеристик МЗПД в соответствии с заданным уровнем защищенности информации.

Отметим, что перечисленные выше процедуры с полным основанием можно отнести к нестандартным, поскольку не существует общепринятых унифицированных алгоритмов их технической реализации. Для осуществления аналитических функций (обучение, самообучение, идентификация, дальновидение и др.) необходимо применять специальные математические и эвристические методы и модели, опирающиеся на достижения в теории искусственного интеллекта. На практике интеллектуализация МЗПД может заключаться в том, что в их состав дополнительно включаются программные компоненты, на которые возлагаются функции поддержки системного администрирования и оперативного управления рисками ИБ в условиях ограниченных временных, информационных и вычислительных ресурсов [4]. Учитывая специфику обработки персональных данных в ИСУ педагогического университета, интеллектуализация МЗПД будет заключаться в том, что в состав классической структуры будут введены средства и сервисы аналитической поддержки функций управления рисками

В общем случае интеллектуальный МЗПД, поддерживающий схему ситуационного управления рисками ИБ, по аналогии с классическими интеллектуальными системами будет *содержать* [4; 6]: базу знаний предметной области, модуль идентификации проблемной ситуации; модуль ранговой оценки и прогнозирования рисков; модуль логического вывода; модуль выбора оптимальной стратегии (базового варианта) защиты; модуль оптимизации механизма защиты; модуль оперативного управления и контроля; модуль аналитической поддержки функций управления рисками ИБ; модуль поддержки и контроля электронного документооборота; интерфейс связи с администратором. В нашей интерпретации интеллектуальный МЗПД представляет собой некоторую

мета-информационную систему, поддерживающую автоматизированный режим системного администрирования ИБ ПД.

Таким образом, реализация интеллектуальных механизмов защиты персональных данных в АИС ИСУ педагогического университета отвечает возросшим требованиям к безопасности образовательных учреждений на этапе интеграции корпоративных информационных сетей образовательных учреждений и развития средств глобальной массовой коммуникации.

Литература

1. *Бочаров М.И., Бочарова Т.И.* Глобальное коммуникативное пространство: проблемы безопасности общения // Национальная безопасность. 2012, № 4 (21). С. 47-51.

2. *Касторнова В.А.* Современное состояние научных исследований и практико-ориентированных подходов к организации и функционированию образовательного пространства. Череповец: ЧГУ, 2011. 461 с.

3. *Крюков В.В, Шахгельдян К.И.* Развитие информационной инфраструктуры вуза для решения задач управления // Университетское управление: практика и анализ. 2004. №4. С. 67-77.

4. *Надеждин Е.Н.* К вопросу создания интеллектуальных информационных систем образовательного назначения // Материалы Всероссийской научной Интернет-конференции с международным участием «Современные системы искусственного интеллекта и их приложения в науке» / Сервис виртуальных конференций Pax Grid; сост. Д.Н. Синяев. Казань: ИП Синяев Д.Н., 2013. С. 49-53.

5. *Надеждин Е.Н., Смирнова Е.Е., Шершакова Т.Л.* Математические основы моделирования и анализа интегрированных систем защиты информации: учебное пособие. Тула: НОУ ВПО «Московский институт комплексной безопасности». Изд-во ТулГУ, 2013. 206 с.

6. *Надеждин, Е.Н.* Научно-методические основы автоматизации процессов обеспечения информационной безопасности в сфере образования // Ученые записки ИИО РАО. 2012. Вып. 41. С. 56-74.

7. О персональных данных: Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 ФЗ // Российская газета. 29 июля 2006 г. №4131.

8. Об информации, информационных технологиях и о защите информации: Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Российская газета. 29 июля 2006 г. №4131.

9. *Роберт И.В.* Теория и методика информатизации образования (психолого-педагогический и технологический аспекты). 3-е изд. М.: ИИО РАО, 2010. 356 с.