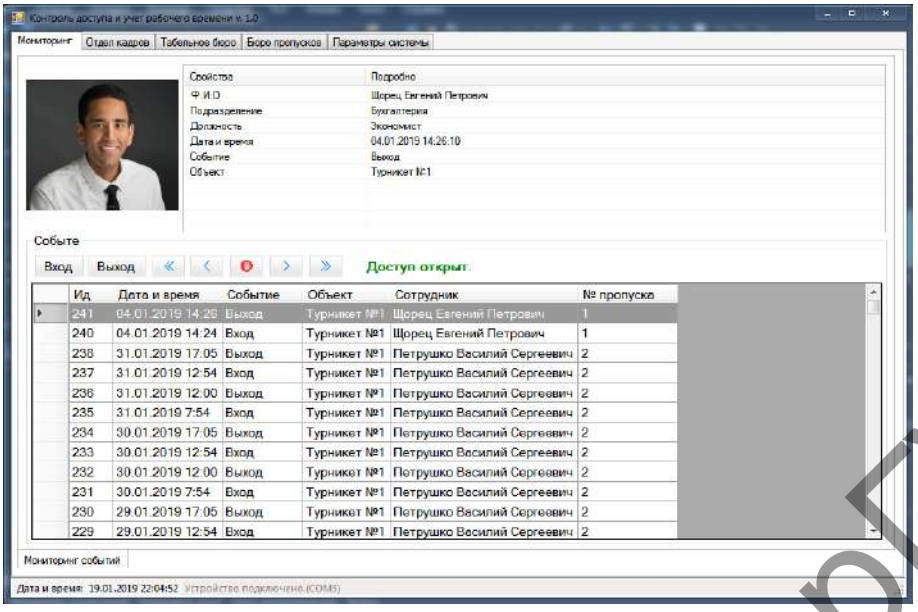

Рисунок 1 — Вид главного окна приложения

Заключение. В результате проделанной работы была спроектирована и реализована автоматизированная система контроля доступа и учета рабочего времени сотрудников предприятия. Преимущество данной системы: снижение вероятности проникновения посторонних лиц на территорию предприятия, повышение системы безопасности сотрудников предприятия, оперативность получения информации о времени прибытия или убытия с места работы сотрудников предприятия, автоматическое формирование табеля рабочего времени по сотрудникам предприятия.

Список цитируемых источников

1. Учет рабочего времени — контроль за сотрудниками [Электронный ресурс]. — Режим доступа: http://naim.guru/rabochee-vremay/uchet.html/ . — Дата доступа: 03.05.2019.

2. Автоматизированное управление электронной проходной [Электронный ресурс]. — Режим доступа: https://knowledge.allbest.ru /radio/2c0b65625b2ad68a5c43a88421306d36_0.html/ . — Дата доступа: 04.05.2019.

УДК 004.056.5+338.23:004.056

И. А. Толстик

Государственное научное учреждение «Институт экономики Национальной академии наук Беларуси», Минск

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ РАЗРАБОТКИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Введение. Актуальность темы исследования не вызывает сомнений в свете процессов, происходящих в международных отношениях, включая экономические, а также во внутренней жизни Республики Беларусь как государства — участника интеграционных объединений на постсоветском пространстве. Мировое развитие на современном этапе характеризуется высоким цензом вопросов защиты информации в качестве приоритетной цивилизационной парадигмы. Целям создания автоматизированных систем защиты информации следует дать оценку с позиций обеспечения перехода на новый этап промышленной революции путем структурного взаимодействия на уровне мировых и национальных факторов по всему периметру хозяйственных связей. Вырабатываются механизмы единого порядка прогрессивных технологических трансформаций различного толка, прежде всего цифровой, относительно экономик, развитых и динамично растущих. О масштабе самой тенденции позволяет судить многочисленность форумов, международных и национальных, в различных форматах, на которых декларируются и принимаются стратегически важные решения о путях развития и трансфера информационных технологий [1]. Необходимость систематизировать концептуальные основы этих решений обусловлена

© Толстик И. А., 2020

Репозиторий БарГУ

требованиями согласованности действий партнеров по экономической интеграции, которые на внешних рынках интеграционных объединений все чаще выступают консолидированно. Таким образом, научная новизна заявленной темы приобретает характер организационного обеспечения.

Цели и основные задачи комплексного изучения предмета исследования обусловлены вышеназванными обстоятельствами. Таким образом, будет дана оценка обеспечению достижения стабильного экономического роста в Беларуси в условиях цифровизации, когда формируется безопасность разработки и освоения новых объектов информатизации, к числу которых относятся и автоматизированные системы различного уровня, включая по защите информации, что, в свою очередь, приведет к повышению жизненного уровня населения, еще большему насыщению внутреннего рынка продукцией отечественного производства.

Основная часть. Единое экономическое пространство — необходимое условие реальной интеграции государств — участников объединений на постсоветской территории (ЕАЭС, СНГ, Союзное государство). В таком межгосударственном взаимодействии республиканские органы управления, субъекты хозяйствования руководствуются соображениями по защите информации, которые основаны на актуальных доктринальных документах. Наиболее емко особо значимые социально-экономические тренды среди них отображает Концепция информационной безопасности Республики Беларусь, которая принята Советом Безопасности Республики Беларусь 18 марта 2019 года [2]. С позиций разработки автоматизированных систем особенно важны положения концепции о геополитических интересах государства, а также относительно защиты информации и обеспечения информационной безопасности в целом: для Беларуси приоритетны соглашения о сотрудничестве в области обеспечения информационной безопасности государств — участников Содружества Независимых Государств, государств — членов Организации Договора о коллективной безопасности, двусторонних соглашений и иных обязательств. Республика Беларусь в области международной информационной безопасности учитывает основные положения актов международных организаций, в том числе резолюций Генеральной Ассамблеи Организации Объединенных Наций, рекомендаций Организации по безопасности и сотрудничеству в Европе.

Среди основных понятий и их определений в этой связи следует назвать следующие:

– защита информации — комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

– информационная безопасность — состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

– информационный суверенитет Республики Беларусь — неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность;

– информационная инфраструктура — совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации;

– международная информационная безопасность как состояние международных отношений, исключающее нарушение мирной стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

в Концепции подчеркнуто, что одним из главных направлений развития Республики Беларусь, важнейшей составляющей формирования информационного общества является цифровая трансформация экономики.

В контексте информационной безопасности, как известно, посредством технического применения автоматизированных систем (далее — АС) защиты информации решают ряд задач. Основными из них являются обеспечение сохранности конфиденциальных данных, препятствование доступу к такой информации, в том числе с помощью ее маскировки. Соответственно, предотвращается утечка данных, а также осуществляется переформатирование информации, перенаправление информационных потоков и др. Посредством АС предпринимаются технические меры по защите информации, по сути, обеспечивается анализ в реальном времени событий, иначе — происходит управление событиями и информационной безопасностью. Таким образом оказываются услуги по обеспечению клиентам состояния защищенности их информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений [3].

Согласно отечественному законодательству, разработанному на основании Концепции, АС различного уровня и назначения могут быть отнесены как объекты информатизации к критически важным (далее — КВОИ), и владелец таковых обязан обеспечить их безопасное функционирование [4]. Помимо своего основного технического и социально-экономического, а также политического предназначения в целях безопасности КВОИ предусмотрен мониторинг угроз безопасности объекта и принятие мер реагирования на угрозы его безопасности. Такой методологический принцип закреплен на бумаге при разработке эксплуатационной документации на КВОИ. Следовательно, в аналогичном подходе нуждаются и АС защиты информации, применение которых, кроме всего прочего, также должно основываться на технических нормативных и правовых актах. Законодательством предусмотрен внутренний и внешний контроль КВОИ. Первый из них осуществляется владельцем объекта не реже раза в год, результаты оформляются документально. Внешний контроль находится в компетенции Оперативно-аналитического центра (ОАЦ) при Президенте Республики Беларусь. Преду-

Репозиторий ВарГУ

смотрено осуществление таких мероприятий раз в пять лет. Кроме того, возможны исключения, проведение внешнего контроля по результатам внутреннего. Владелец КВОИ получает результаты контроля и обязан при необходимости устранить все недочеты, поставив в известность ОАЦ. Таким образом, использование объекта предусматривает как саморегулирование, так и контролируется централизованно, что свидетельствует о всеобъемлющих мерах по обеспечению информационной безопасности. Автоматизированные системы защиты информации в качестве КВОИ также целесообразно включать в аналогичные отношения. На этот счет предусмотрен определенный порядок отнесения объектов информатизации к КВОИ. Как правило, само решение исходит от руководства государственного органа, а в случае, когда владелец объекта информатизации не имеет такой подчиненности, — руководителя облисполкома, Минского горисполкома, отраслевого органа государственного управления.

Согласно концепции, повышение эффективности обеспечения безопасности КВОИ необходимо осуществлять с помощью интегрирования в государственную систему мониторинга национального сегмента сети Интернет отраслевых систем мониторинга и контроля киберугроз.

Тот факт, что в наше время большая часть информации хранится в цифровом виде, на компьютерных носителях, усложнят проблему защиты информации. Основной угрозой являются компьютерные вирусы, для борьбы с которыми принимаются определенные меры [3]. Для автоматизированных систем защиты информации такое обстоятельство означает необходимость разработки не только мер технической безопасности, но и ограничения физического доступа к используемой аппаратуре. Таким образом, комплекс услуг, которые оказываются при использовании АС защиты информации, должен сводиться к минимизации опасности и возможного ущерба, который может быть нанесен злоумышленниками, действиями самого пользователя или сбоем аппаратуры, следствием чего может оказаться внедрение в систему вредоносных программ.

Заключение. Концептуальные основы разработки АС защиты информации позволяют мировоззренчески обосновать необходимость реализации доктринальных документов из отечественного законодательства и обусловленность применяемых мер по обеспечению информационной безопасности, в чем заинтересовано государство и субъекты хозяйствования, а также физические лица как потребители информационных услуг.

Список цитируемых источников

1. *Лукашенко, А. Г.* Диалог во имя мира и безопасности : выступление Президента Александра Лукашенко на пленарной сессии «В поисках повестки мира и сотрудничества для Европы» международной конференции «Европейская безопасность : отойти от края пропасти» / А. Г. Лукашенко // СБ. Беларусь сегодня. — 2019. — 9 окт. — С. 2—5.
2. Концепция информационной безопасности Республики Беларусь // СБ. Беларусь сегодня : спецвып. — 2019. — 21 марта. — С. 1—5.
3. Защита информации [Электронный ресурс]. — Режим доступа: http://anyap97.blogspot.com/2013/11/blog-post.html . — Дата доступа: 15.10.2019.
4. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации [Электронный ресурс] : Указ Президента Респ. Беларусь, 25 окт. 2011 г. № 486 // Нац. реестр правовых актов Респ. Беларусь. — 2011. — № 121. — 1/13026.

УДК 004.934

Е. Г. Шапович[1], Я. Орсаг[2]

[1]Учреждение образования «Барановичский государственный университет», Барановичи

[2]Средняя промышленная школа машиностроения, Всетин, Чешская Республика

СОЗДАНИЕ АРХИТЕКТУРЫ ПРИЛОЖЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ КЛАССИФИКАЦИИ ДИАТОМОВЫХ ВОДОРОСЛЕЙ

Введение. Компьютерное зрение и искусственный интеллект являются одними из самых мощных компьютерных технологий в наше время. Они имеют возможность изменить мир, следовательно, помогают разрабатывать пути решения различных проблем в нашем обществе.

Эта работа ориентирована на изучение и применение обработки изображений, обнаружения и классификации, с использованием как традиционных, так и новых методов. Для применения этих методов были разработаны комплексные рабочие процессы к конкретной проблеме, т. е. к автоматическому распознаванию диатомовых водорослей.

Основная часть. Исторически так сложилось, что люди организовывали общины в местах, богатых природными ресурсами, чтобы развивать свою деятельность. Среди них вода была очень значительным ресурсом, так как является крайне необходимой и для сельского хозяйства, и животноводства, и собственного потребления. Следовательно, необходимо контролировать качество водных ресурсов.

Одним из наиболее перспективных методов для этого является изучение некоторых микроскопических организмов, известных как диатомовые водоросли. Эти существа принадлежат к группе одноклеточных водорослей, состоящих из большого числа видов. Конкретные виды, найденные в резерве воды, являются биоинди-

© Шапович Е. Г., Орсаг Я., 2020

Репозиторий БарГУ