# Теория и практика современной науки

№10(52), октябрь, 2019

ISSN 2412-9682

МЕЖДУНАРОДНЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

# *«Теория и практика современной науки»*

http://www.modern-j.ru

**ISSN 2412-9682**

Свидетельство о регистрации
средства массовой коммуникации
Эл № 61970 от 02.06.2015г.



Выпуск № 10(52) (ОКТЯБРЬ, 2019). Сайт: http://www.modern-j.ru

Журнал размещается на сайте Научной электронной библиотеки
на основании договора 435-06/2015 от 25.06.2015

***Нарзуллаев Д.З., к.т.н., с.н.с.***
***Центр развития инноваций и трансфера технологий***
***при хокимияте Ташкентской области***
***Шадманов К.К., к.х.н.***
***заведующий кафедрой***
***Ташкентский фармацевтический институт***
***Усмонов А., с.н.с.***
***Центр развития инноваций и трансфера технологий***
***при хокимияте Ташкентской области***
***Узбекистан, г. Ташкент***

# ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ФЕРМЕРСКИМ ХОЗЯЙСТВОМ

*Аннотация: В статье предлагаются пути обеспечения информационной безопасности автоматизированной системы управления фермерским хозяйством.*

*Ключевые слова: информационно-коммуникационные технологии, информационная безопасность, автоматизированная система управления, база данных.*

***Narzullayev D., Cand. tech. Sci., Senior Researcher***
***Center for the Development of Innovation and Technology***
***Transfer at the Khokimiyat of Tashkent Region***
***Uzbekistan, Tashkent***
***Shadmanov K., Cand. chem. Sci., Head of Department***
***Tashkent pharmaceutical institute***
***Uzbekistan, Tashkent***
***Usmonov A., Senior Researcher***
***Center for the Development of Innovation and Technology***
***Transfer at the Khokimiyat of Tashkent Region***
***Uzbekistan, Tashkent***

# ENSURING INFORMATION SECURITY OF AN AUTOMATED FARM MANAGEMENT SYSTEM

*Abstract: The article suggests ways to ensure information security of an automated farm management system.*

*Key words: Information and communication technologies, information security, automated control system, database.*

В настоящее время общемировые процессы глобализации диктуют не только необходимость повсеместного внедрения информационно-коммуникационных технологий (ИКТ) во всех сферах жизни, но и условия обеспечения безопасности автоматизированных систем управления, в том числе, фермерских хозяйств. Узбекистан одним из первых в Центральной Азии присоединился к международной системе безопасности в сфере ИКТ.Создан Центр обеспечения информационной безопасности (ИБ) при

Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан, основная задача которого – обеспечение ИБ комплексов информационных систем (ИС), ресурсов и баз данных (БД) системы «Электронное правительство», а также оказание содействия в разработке и реализации политики ИБ соответствующих систем и ресурсов государственных органов.Сотрудники этого центра занимаются сбором, анализом и накоплением данных о современных угрозах ИБ, выработкой рекомендаций и предложений по эффективному принятию организационных и программно-технических решений, направленных на предотвращение актов незаконного проникновения в ИС, ресурсы и БД системы «Электронное правительство».

По мере развития и усложнения методов, средств и форм автоматизации процессов обработки информации повышается зависимость пользователейИС от степени безопасности используемых им ИКТ.

Перечислим факторы, обуславливающие актуальность и важность проблемы обеспечения ИБ:

- современные уровни и темпы развития средств ИБ значительно отстают от развития ИКТ;
- высокие темпы роста парка персональных компьютеров, применяемых в различных сферах человеческой деятельности;
- резкое увеличение количества пользователей, имеющих прямой доступ к ИС и БД;
- значительное увеличение объёмов информации;
- многочисленные уязвимости в программных и сетевых платформах.

Обеспечение ИБ предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования ИС, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов, то есть защиту аппаратных средств, программного обеспечения, данных и персонала ИС.

Основные составляющие информационной безопасности[1]:

- Доступность информации – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними. ИС создаются для получения определенных информационных услуг. Особенно ярко ведущая роль доступности проявляется вразного рода системах управления – производством, транспортом, сельским хозяйством и т.п.

- Целостность информации – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. Целостность можно подразделить на статическую и динамическую. Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом информационной

безопасности в тех случаях, когда информация служит «руководством к действию».

- Конфиденциальность информации – свойство информации быть известной и доступной только правомочным субъектам системы.

Перечислим средства защиты информации:

- Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от ИС, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).

- Аппаратные средства - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в ИС или сопрягаемые с ней специально для решения задач защиты информации.

- Программные средства - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

- К специфическим средствам защиты информации относятся криптографические методы. В ИС криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

Одной из самых опасных на сегодняшний день угроз ИБ являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак. В последние годы существенно увеличилась их частота и уровень ущерба. По мнению экспертов, это можно объяснить появлением новых каналов проникновения вирусов. На первом месте по-прежнему остается почта, но, как показывает практика, вирусы способны проникать и через программы обмена сообщениями, такие как Telegram и другие. Увеличилось и количество объектов для возможных вирусных атак. Если раньше атакам подвергались в основном серверы стандартных веб-служб, то сегодня вирусы способны воздействовать и на межсетевые экраны, коммутаторы, мобильные устройства, маршрутизаторы. В последнее время особенно активны стали так называемые вирусы-шифровальщики.

В настоящее время комплексный подход к ИБ, основанный на решении совокупности частных задач по единой программе, является основным для создания защищенной среды обработки информации в ИС и сводит воедино различные меры противодействия угрозам: морально этические, правовые,

организационные, технические ипрограммные способы обеспечения ИБ. Комплексный подход позволил объединить целый ряд автономных систем путем их интеграции в так называемые интегрированные системы безопасности [2-4].

Применительно к ИБ наиболее очевидными следует считать задачи технического и криптографического закрытия информации, ограничения доступа к информации, ограничения уровней паразитных излучений технических средств, охраны и тревожной сигнализации.

Обеспечение ИБ должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы ИБ. Любая утечка информации может привести к серьезным проблемам для компании — от значительных финансовых убытков до полной ликвидации.

Одним из решений проблем безопасности подключения к сети Интернет является применение межсетевых экранов(МЭ) - программно-аппаратных систем, находящихся в точке соединения внутренней сети организации и интернета и осуществляющих контроль передачи данных между сетями.МЭ обеспечивают защиту ИС организации от несанкционированного вмешательства и являются необходимым средством обеспечения ИБ. При приобретении МЭ необходимо выбрать нужную архитектуру и компоненты, правильно настроить программное обеспечение и протестировать конфигурацию программного продукта.

Благодаря прозрачной аутентификации МЭ получает учетные данные пользователя из клиентской операционной системы без постороннего вмешательства. Строгий контроль внешнего доступа пользователей и групп осуществляется без запроса учетных данных пользователя.

Следующим обязательным пунктом обеспечения ИБ является использование антивирусного программного обеспечения для серверов и клиентских компьютеров ИС фермерского хозяйства. При этом необходимо применять именно лицензионные продукты, обеспечивающие ежедневное обновление антивирусных баз и приложений выбранного программного обеспечения (ПО). Обладатель нелицензионного ПО не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Вместе с ним он покупает и вирусы, способные нанести вред системе компьютерной безопасности. По данным исследования Microsoft, в 7% изученных нелицензионных программ было найдено специальное программное обеспечение для кражи паролей и персональных данных.

Среди средств информационной защиты можно выделить физические средства защиты информации. К ним относятся: ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами. Большое распространение получили HID-карты для контроля доступа. Например, при внедрении этой системы,

пройти в серверную или другое важное подразделение компании могут лишь те, кому такой доступ предоставлен по протоколу. Базовые средства защиты электронной информации являются незаменимым компонентом обеспечения ИБ компании. К ним относятся, помимо многочисленных антивирусных программ, системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции. Корпоративные почтовые ящики обязательно должны быть оборудованы такими системами. Кроме того, необходима организация дифференцированного доступа к информации и систематическая смена паролей.

Из сказанного выше можно сделать вывод о том, что обеспечение ИБ информационных систем различного направления, в том числе автоматизированных систем управления фермерскими хозяйствами, является обязательным условием при проектировании и создании таких ИС.

**Использованные источники:**

1. Галатенко В.А. Основы информационной безопасности.М.: Национальный Открытый Университет "ИНТУИТ", 2016. - 267 с.
2. БондаревВ. Введение в информационную безопасность автоматизированных систем. Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.
3. Бирюков А.Информационная безопасность: защита и нападение. 2-е изд. - М: Издательство: ДМК-Пресс, 2017. – 434 с.
4. Баранова Е., Бабаш А. Информационная безопасность и защита информации. 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.