УДК 338.3+004.056

© А. В. Балановская[1], А. В. Волкодаева[2], *2017*

Международный институт рынка (МИР), г. Самара, Россия

E-mail [1]:balanovskay@mail.ru
E-mail [2]: arina-21@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Статья посвящена рассмотрению основных аспектов информационной безопасности критически важных объектов в автоматизированных системах управления технологическими процессами на трех уровнях: организационном, правовом и технологическом. Анализируются проблемы, связанные с правовыми механизмами обеспечения защиты информации, организационно-структурным взаимодействием подразделений по обеспечению безопасности в автоматизированных системах управления технологическими процессами. Представлена статистика уязвимостей в автоматизированных системах управления технологическими процессами и продукты защиты современными средствами мониторинга событий и обнаружения атак. Основные выводы содержат предложения по комплексному обеспечению информационной безопасности критически важных объектов в автоматизированных системах управления технологическими процессами.

Ключевые слова: информационная безопасность, критически важные объекты, автоматизированная система управления, технологический процесс, уязвимость.

В настоящее время осуществляется активная работа по разработке и формированию механизмов сотрудничества компаний в области информационной безопасности критически важных объектов (КВО). Основные результаты работы ежегодно обсуждаются в рамках конференции «Информационная безопасность АСУ ТП КВО» [1] представителями предприятий топливно-энергетического комплекса, химической промышленности, транспорта, металлургии, машиностроения и оборонно-промышленного комплекса, ЖКХ и других отраслей, а также разработчиков средств промышленной автоматизации, производителей и интеграторов в области защиты информации. Таким образом, в настоящее время происходит фор-

мирование сообщества, выступающего совместно для решения вопросов информационной безопасности КВО и реагирования на угрозы в комплексной защите автоматизированных систем управления технологическими процессами (АСУ ТП).

Данная работа проводится на трех различных уровнях:

1. На организационном уровне создается Консультационный координационный центр по вопросам реагирования на компьютерные инциденты в рамках Организации Договора о коллективной безопасности (ОДКБ) [2].

2. На законодательном уровне со стороны Федеральной службы по техническому и экспортному контролю (ФСТЭК РФ) осуществляется реализация приказа от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления (АСУ) производственными и технологическими процессами (ТП) на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», реализация Федерального закона Российской Федерации от 21.07.2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса», приняты и реализуются «Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 г., № 803), а также исполняется Указ Президента Российской Федерации от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [3].

3. На технологическом уровне в части таких разработок, таких как «Квинт», «Phocus», «Торнадо», «Оператор», «Industrial Security Incident Manager» (ISIM), «AdminBastion» и многоих других, и их сопровождения.

Существующая система поддержки информационной безопасности КВО АСУ ТП имеет определенные трудности при реализации в практических условиях:

— не всегда удается сформировать единые требования к безопасности в рамках конкретной системы, что требует индивидуального подхода и дополнительного сопровождения;

— организационно-структурные особенности взаимодействия подразделений по информационным технологиям и подразделений

по обеспечению безопасности АСУ ТП обусловлено различиями в применении конкретных продуктов и нежеланием их согласовывать для конструктивного взаимодействия;

— проведение аудита информационной безопасности КВО с помощью АСУ ТП влечет существенные издержки в связи с необходимостью остановки производственного процесса.

Одной из самых важных проблем информационной безопасности КВО является проведение аудита, оптимальная организация которого как первоначальный этап работы в комплексной защите АСУ ТП определяет последующую эффективность всего механизма информационной защиты предприятия.

Статистика обнаружения уязвимости в АСУ ТП ежегодно проводится экспертами Positive Technologies [4], в составе которого функционирует один из крупнейших в Европе исследовательских центров в области информационной безопасности, содействуя устранению уязвимостей в различных информационных системах. На рисунке 1 приведено количество обнаруженных уязвимостей в АСУ ТП за период с 2010 по 2015 гг. Проведя анализ показателей, представленных экспертами центра, можно сделать вывод, что к концу рассматриваемого периода количество ежегодно обнаруживаемых уязвимостей в АСУ ТП увеличивается так же, как и в его начале, но темп роста существенно замедляется. Данный процесс объясняется возросшим интересом производителей оборудования к своевременному выявлению и устранению уязвимостей и взаимодействию с исследователями.

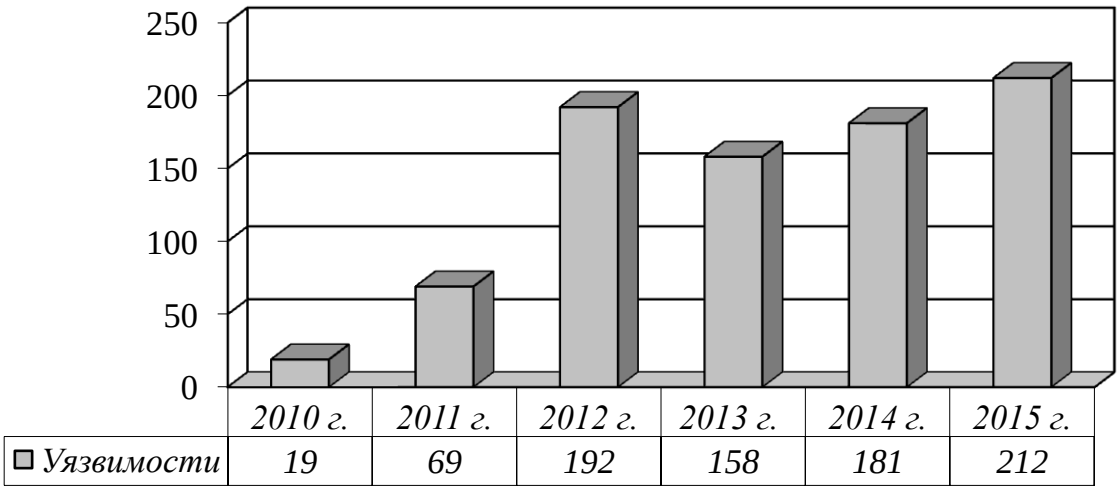

Рис. 1. Количество обнаруженных уязвимостей в АСУ ТП [5]

В рамках исследования были рассмотрены уязвимости компонентов порядка 500 производителей АСУ и выявлено более 700

уязвимостей (из которых 7 новых). Все выявленные уязвимости в АСУ ТП имеют преимущественно высокую и среднюю степень риска (рис. 2).

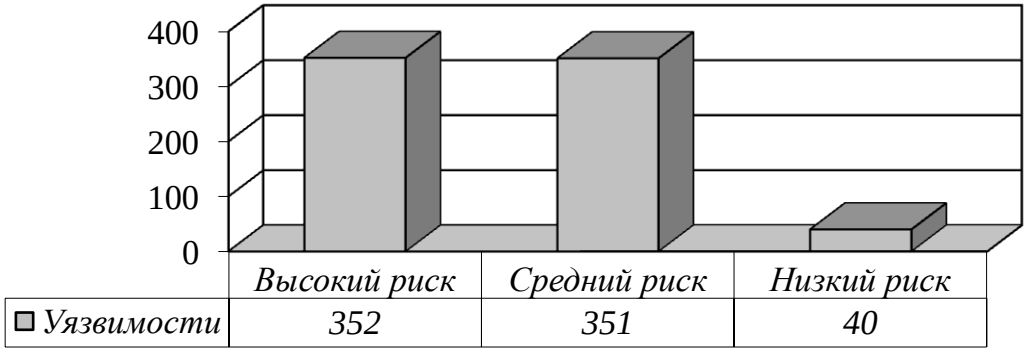

Рис. 2. Статистика уязвимостей АСУ ТП по степени риска [5]

Наиболее распространенные типы выявленных уязвимостей представлены на рисунке 3, из которых:

— 29% имеют такие уязвимости, как отказ в обслуживании (DoS);

— 21% — удаленное выполнение кода (Code Execution);

— 20% — переполнение буфера (Overflow);

— 31% — другие.

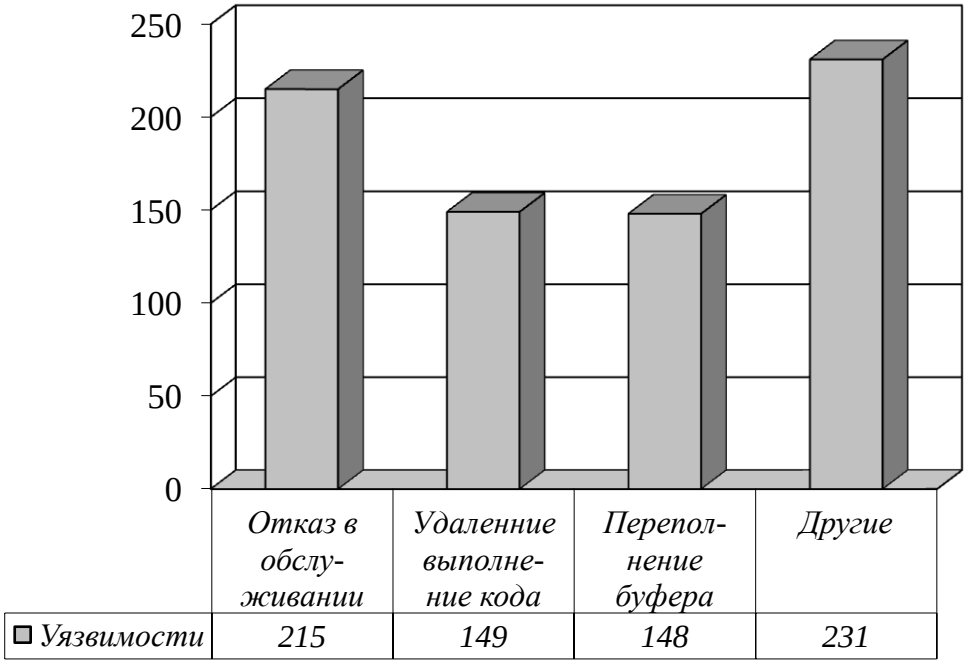

Рис. 3. Наиболее распространенные типы уязвимостей АСУ ТП [5]

В связи с отсутствием публикаций результатов устранения уязвимостей существует определенная трудность поиска путей по-

вышения эффективности используемых АСУ ТП на основе анализа работы существующих на предприятии систем. Однако результаты анализа распространенности типов уязвимостей дают возможность проведения разработок по повышению качества используемых АСУ ТП на предприятии.

На современном российском рынке существует большое разнообразие продуктов защиты КВО АСУ ТП (табл. 1).

Таблица 1

Продукты защиты КВО АСУ ТП

Продукт защиты КВО АСУ ТП	*Назначение продукта*	*Разработчик*
Industrial Security Incident Manager (ISIM)	Защита промышленных сетей	Positive Technologies
DATAPK	Мониторинг промышленного сегмента АСУ ТП	Уральский центр систем безопасности
AdminBastion	Контроль действия производителей АСУ ТП и сотрудников их партнеров, которые занимаются техническим сопровождением промышленных решений, а также действия собственных администраторов и операторов АСУ ТП	Компания «АйТи Бастион»
Siemens SICAM PAS	Управление энергосистемами	Компания «Siemens»
Niagara Framework	Технология, позволяющая объединить в единую вычислительную сеть все известные протоколы и способы передачи данных	Компания «Honeywell»
Sunny WebBox	Система для автоматизации зданий и управления электроэнергией	Компания «SMA Solar Technology»
WebRTU (2130) и Solar-Log (820)	Компоненты в области энергетики	Компания«Solare Datensysteme»

Наибольшее распространение получили устройства, выполняющие функции SCADA/ЧМИ и ПЛК/ТУД (RTU) (25250 единиц).

Это объясняется распространенностью многофункционального продукта Niagara Framework компании Honeywell.

Например, современная модель управления качеством социально-экономической среды (КСЭС) является актуальной и эффективной базой для применения технологий обработки, хранения и анализа разнородных массивов данных в режиме реального времени. Встроенные в нее алгоритмы и механизмы работы с потоковой информацией позволяют выявлять критические значения функции, риски и потенциальные точки роста. Путем мониторинга Интернет-пространства становится возможным определение значимости выявленных индикаторов дистанционно и без привязки к конкретному субъективному мнению, что во многом увеличивает достоверность получаемых результатов. Кроме того, становится возможным определять, что именно оказывает наиболее существенный эффект в увеличении критических отклонений результирующего значения КСЭС — сам индикатор или его значимость, а это, в свою очередь, может служить обоснованием для выбора управленческого воздействия [6].

Приведенные выше продукты являются современными средствами мониторинга событий и обнаружения атак. Их использование, а также систематическое совершенствование позволит обеспечить информационную безопасность КВО АСУ ТП и снизить рост атак на корпоративные инфраструктуры предприятий.

Возвращаясь к вопросу обеспечения информационной безопасности КВО АСУ ТП, следует комплексно осуществлять работу в данном направлении, используя механизмы организационного, правового и технологического уровней.

Так, на правовом уровне необходимо соблюдать рекомендации в части приказа ФСТЭК РФ от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», а также принимать участие в их совершенствовании.

На организационном уровне основными механизмами, на наш взгляд, должны являться: обмен опытом; создание структур по анализу данных в области обеспечения информационной безопасности; совершенствование механизмов взаимодействия подразде-

лений предприятия, непосредственно осуществляющих обеспечение безопасности КВО АСУ ТП; подготовка высококвалифицированных специалистов в данной области.

На технологическом уровне необходимо усилить работу предприятий по использованию современных АСУ ТП, а разработчиков и производителей — включать в свои планы работы над совершенно новыми продуктами в данной области.

В условиях серьезных перемен в российской экономике, вызванных применяемыми против России санкциями и необходимостью развития импортозамещения, компании вынуждены искать принципиально новые подходы к ведению бизнеса, к организации производственного процесса, к выстраиванию отношений с партнерами и клиентами. Поэтому большое значение имеет необходимость использования и развития современных российских разработок обеспечения безопасности. Необходимо отдавать им предпочтение и стимулировать производителей на их модернизацию и сопровождение [7]. Использование стратегии устойчивого развития как комплекс административных и хозяйственных решений, сбалансированных с точки зрения имеющегося потенциала и направленных на стабильное долгосрочное функционирование социально-экономической системы, позволит снизить неопределенности и использовать научную основу для нахождения управляющих воздействий, способствующих устойчивости функционирования системы [8].

Результаты исследования показали отсутствие снижения числа уязвимостей КВО АСУ ТП и отсутствие адекватной защиты, несмотря на осуществление разработок в области информационной безопасности на технологическом, организационном и правовом уровнях, которые, в свою очередь, должны быть соответствующим образом организованы и обеспечить информационную безопасность КВО АСУ ТП. Информационная безопасность служит функциональным элементом системы обеспечения стратегического развития предприятия, поэтому ее основная задача — обеспечить стабильность существования предприятия в настоящем и перспективы его устойчивого развития в будущем.

Литература

1. Сайт конференции «Информационная безопасность АСУ ТП КВО». URL: http://www.ибкво.рф/.

2. Семкин С. Н. Основы организационного обеспечения информационной безопасности объектов информатизации: учеб. пособие / С. Н. Семкин, Э. В. Беляков, С. В. Гребенов, В. И. Козачок. М.: Гелиос АРВ, 2005. 192 с.

3. СПС «Консультант Плюс». URL: http://www.consultant.ru.

4. Positive Technologies. URL: http://www.securitylab.ru/news/tags/positive%20technologies/.

5. Промышленные системы управления — 2016: уязвимость и доступность. URL: https://habrahabr.ru/company/pt/blog/306202.

6. Нестерова С. И., Рамзаев М. В., Чумак В. Г. Управление качеством социально-экономической среды с использованием технологии Big Data // Информационные технологии и нанотехнологии: материалы Международной конференции и молодежной школы: ИТНТ-2016 (Самара, 17-19 мая 2016 г.). Самара: Самарский государственный аэрокосмический университет, 2016. С. 1084-1089.

7. Горбунова О. А., Мавлявеева Ю. О. Основные направления повышения конкурентоспособности промышленного предприятия на примере ООО «Ортопласт» // Вестник Международного института рынка. 2015. № 1. С. 65-72.

2. Дровянников В. И., Чумак Е. А. Модельный аппарат оценки потенциала устойчивости социальной системы // Вестник Международного института рынка. 2016. № 1. С. 36-43.

8. Казакова А. В., Балановская А. В. Роль информационной безопасности в деятельности предприятий // Достижения ученых XXI века. 2010. № 6. С. 44-46.

Статья поступила в редакцию 27.01.17 г.
Рекомендуется к опубликованию членом Экспертного совета д-ром техн. наук, доцентом И. Н. Хаймович