

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:681.5

Бацека
Андрей Владимирович

Информационная безопасность оборудования для контроля устройств
автоматики

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты, информационная
безопасность

Научный руководитель
Пачинин Виталий Иванович
кандидат технических наук, доцент

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

Обоснование актуальности темы магистерской диссертации. Компания «Неро Электроник» уверенными шагами разрастается. Начиная с нескольких человек и ручного производства, она выросла до полутора сотен работающих, которые обслуживают десятки автоматизированных линий на производственных и арендных площадях завода компании. Теперь Компания «Неро Электроникс» стала независимой, построила собственное здание, увеличила штат сотрудников и производственные мощности. В таком быстро разрастающемся темпе сложно уделять внимание таким вещам, как вопросы информационной безопасности (ИБ), которые с первого взгляда кажутся излишними. В этих условиях **актуальность** исследования ИБ и создания рекомендаций в области ИБ для компании, в особенности использования автоматизированных систем управления для контроля производимых устройств автоматике **не вызывает сомнений**.

Оценка современного состояния решаемой задачи. Как указано выше, на сегодня в АСУ ТП Компании «Неро Электроникс» множество различных угроз информационной безопасности предприятий и множество различных методов их парирования. В этих условиях важно определить названные угрозы применительно к Компании «Неро Электроникс» и подобрать для них оптимальные способы парирования.

Задачи и назначение работы. В соответствии с вышесказанным назначение этой работы – мониторинг информационной безопасности Компании «Неро Электроникс», выявление существующих и потенциальных угроз и определение рекомендаций руководству компании по парированию угроз ИБ.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований. В последнее время компания «Неро Электроникс» уверенно идет вверх, повышая свое материальное состояние, охватывая новые области на рынке электронных устройств автоматизации и учетной тематики, расширяя штат сотрудников. С увеличением компании растет ценность информации, накопленной большим опытом. Интеллектуальная собственность компании нуждается в проверке и, возможно, в изменениях условий хранения, использования и защиты. Согласно существующим условиям и отсутствию специальных людей, следящих за интеллектуальной собственностью компании, вопрос по информационной безопасности становится одним из главных на обсуждении руководством компании.

Поэтому **целью настоящей работы** стало исследование компании «Неро Электроникс» на возможные уязвимости, слабые места и потенциально опасные участки в области информационной безопасности при использовании автоматизированных систем управления технологическими процессами. А так же поиск методов парирования найденных уязвимостей. Для достижения поставленной цели в этой диссертации **решены следующие задачи:**

- проведен обзор накопленного опыта в области использования автоматизированных систем управления технологическими процессами (АСУ ТП);
- проведены исследования в области информационной безопасности компании «Неро Электроникс», выявлены существующие и потенциальные угрозы информационной безопасности;
- разработаны рекомендации для руководства компании «Неро Электроникс» по увеличению защищенности в области информационной безопасности.

Положения, выносимые на защиту. Рекомендации Компании «Неро Электроникс» направленные на внедрение мероприятий по обеспечению информационной безопасности компании.

Теоретическая и практическая значимость. Теоретическая значимость работы заключается в исследовании угроз информационной безопасности АСУ ТП и их методов парирования. Практическая ценность работы заключается в использовании проведенных теоретических исследований для обеспечения информационной безопасности Компании «Неро Электроникс».

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом на базе его исследований, проводимых в Компании «Неро Электроникс» и на кафедре ЗИ БГУИР.

Результаты работы опубликованы в:

- Материалах XVIII Междунар. науч.-техн. конф. «Современные средства связи» – Анализ угроз и уязвимостей АСУ технологическими процессами, 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013.
- Тезисах докл. 50-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии – Основные проблемы информационной безопасности АСУ ТП КВО (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014.
- Материалах XIX Междунар. науч.-техн. конф. «Современные средства связи» – Безопасность информации в АСУТП контроля устройств автоматике, 14–15 окт. 2014 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2014.

Результаты работы апробированы на 3 (трех) научно-технических конференциях, в том числе 4 (четырёх) международных:

- 48-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии (Минск, 7 – 11 мая 2012 года). – Мн.: ИИТ БГУИР, 2012.
- XVIII Междунар. науч.-техн. конф. «Современные средства связи», 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.].
- 50-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014.
- XIX Междунар. науч.-техн. конф. «Современные средства связи», 14–15 окт. 2014 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.].

По результатам апробации на 48-й грамота научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии и доклад отмечен грамотой руководства БГУИР, а на 50-ой – благодарностью.

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из общей характеристики работы, введения, трех глав и заключения.

В первой главе «Анализ оборудования для контроля устройств автоматики» рассмотрена Компания «Неро Электроникс», описан жизненный цикл выпускаемой продукции, приведена структура и описание оборудования для контроля приборов автоматики, его роль и важность в процессе производства приборов автоматики.

Во второй главе «Анализ угроз информационной безопасности» проводится исследование выявленных и потенциальных угроз. Вначале приводится терминология и классификация угроз и уязвимостей информационной безопасности, далее проводится исследование угроз информационной безопасности автоматизированной систему управления технологическими процессами в Компании «Неро Электроникс», исследуется угроза вредоносного программного обеспечения, угроза несанкционированного доступа к операционной системе и данным, угроза недостаточного уровня знаний пользователей.

В третьей главе «Методы парирования угроз» приведены различные способы противостояния найденным угрозам. В главе описано парирование угрозы вредоносного программного обеспечения, блокировка несанкционированного доступа к операционной системе автоматического рабочего места и доступа к данным на таком месте, способы повышения знаний пользователей и персонала автоматизированной системы управления технологическими процессами. Так же составлены рекомендации для руководства Компании «Неро Электроникс» направленные на внедрение мероприятий по обеспечению информационной безопасности компании.

ЗАКЛЮЧЕНИЕ

По результатам проведенного исследования можно сделать следующие выводы:

✓ В связи со сложностью АСУ ТП для контроля приборов автоматизации, установленной в Компании «Неро Электроникс» и наличием большого числа уязвимостей в ней, заниматься информационной безопасностью этой АСУ ТП необходимо. С другой стороны, в Компании «Неро Электроникс» выделенных специалистов по информационной безопасности нет. Причина этого общеизвестна [7]: банальная нехватка средств и, как следствие этого, экономия на информационной безопасности.

✓ Проведенный анализ угроз ИБ в АСУ ТП Компании «Неро Электроникс» позволил выявить для парирования наиболее значимые для Компании «Неро электроникс» угрозы:

- вредоносное программное обеспечение (ВПО), в том числе отсутствие блокировки АРМов на физическом уровне и хакерские атаки;

- несанкционированный доступ к ОС АРМов и данным;

- недостаточный уровень знаний пользователей и персонала АСУ ТП, в том числе малограмотность в области владения компьютером и низкий общий уровень знаний всех сотрудников Компании «Неро Электроникс» в области защиты информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1 Бацека А.В., Пачинин В.И. Безопасность информации в АСУТП контроля устройств автоматики // Современные средства связи: материалы XIX Междунар. науч.-техн. конф., 14–15 окт. 2014 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2014. – 299 с. – С. 210-211.

2 Бацека А.В. Основные проблемы информационной безопасности АСУ ТП КВО // 50-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014. – 78 с. с ил. – С. 6.

3 Бацека А.В., Пачинин В.И. Анализ угроз и уязвимостей АСУ технологическими процессами // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 211-212.