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

УДК 004.056

Адериха
Александр Викторович

# Информационная безопасность в ERP-системах

**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**. ERP-системы предназначены для управления и планирования всей финансовой и хозяйственной деятельности предприятия. Они используются для оперативного извлечения информации, необходимой руководству предприятия информации для принятия управленческих решений, а также для создания инфраструктуры коммуникации предприятия с поставщиками и потребителями.

Огромный размер ERP-систем является одновременно и преимуществом, и проблемой. Недостаток квалифицированных SAP-специалистов по безопасности и огромное количество пользовательских настроек порождают множество уязвимостей. Поддерживать актуальность безопасности системы является достаточно сложно задачей и ее необходимо тщательно проанализировать и разработать меры по упрощению этой задачи.

В этих условиях систематизация и анализ состояния ИБ в SAP, а также разработка программного средства “Система рекомендации обновлений” **являются крайне актуальными.**

**Оценка современного состояния решаемой задачи**. Рост ERP-систем, информации находящейся в них, а также огромное количество внедряемых новых технологий с которыми приходится сталкиваться при обеспечении информационной безопасности порождает большое количество проблем. Для решения этих проблем их необходимо проанализировать и выработать комплексный подход к устранению.

**Задачи и назначение работы**. В этих условиях назначение этой работы – проведение комплексного анализа информационной безопасности в ERP-системах в условиях постоянно развивающихся систем и разработка программного продукта, оптимизирующего процесс анализа и применения выходящих обновлений, как наиболее простого и доступного средства по обеспечению информационной безопасности в системе.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Цели и задачи проводимых исследований**. Целью исследования является разработка комплексного подхода к поддержке актуальности безопасности системы. Учитывая огромные размеры системы это является достаточно сложно задачей. Необходимо тщательно проанализировать и разработать меры по упрощению её решения. Поэтому **целью этой работы** стало исследование угроз в ERP-системе SAP, разработка мер по оптимизации безопасности из стандартных, предлагаемых SAP, а также создание программного средства для упрощения работы с новыми обновлениями для системы, в том числе при наличии нескольких систем в одном ландшафте.

Для достижения поставленной цели в этой диссертации **решены следующие задачи**:

- проведен обзор существующих уязвимостей и кода в области информационной безопасности в ERP-системах;
- на основании исследования разработаны меры по парированию угроз информационной безопасности в SAP:
- разработана и отлажена компьютерная программа работы с обновлениями для SAP.

**Личный вклад магистранта в выполненную работу**. Работа полностью выполнена лично магистрантом на базе его исследований, начатых им будучи студентом БГУИР.

**Результаты работы опубликованы в:**

- Материалах XIX Междунар. науч.-техн. конф. «Информационные системы и технологии» (ИСТ–2013), Нижний Новгород (19 апреля 2013 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2013
- Тезисах докл. 49-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии, Минск: БГУИР, ИИТ, 4 мая 2013 года. – Мн.: ИИТ БГУИР, 2013.
- Материалах XVIII Междунар. науч.-техн. конф. «Современные средства связи», 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 (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014.

- Материалах XIX Междунар. науч.-техн. конф. «Информационные системы и технологии» (ИСТ–201к), Нижний Новгород (18 апреля 2013 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014

**Результаты работы апробированы на** 5 (пяти) научно-технических конференциях, в том числе 3 (трёх) международных:

- XIX МНТК «Информационные системы и технологии» (ИСТ–2013), Нижний Новгород (19 апреля 2013 г.). –Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2013
- 49-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии, Минск: БГУИР, ИИТ, 2013.
- 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.
- XX МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014

# КРАТКОЕ СОДЕРЖАНИЕ

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

В первой главе «ERP-системы» рассмотрен объект исследования – ERP-системы, и, в частности, наиболее распространённый их вариант – системы автоматизированного управления SAP R/3. Для последних проанализированы их достоинства и недостатки, а также предпосылки возникновения угроз информационной безопасности.

Во второй главе “Информационная безопасность в SAP” выделены наиболее вероятные общие угрозы информационной безопасности систем SAP R/3, к которым отнесены:

- атаки на клиентские рабочие станции;
- переполнения буфера в SAP GUI;
- переполнения буфера в ACTIVEX компонентах SAP GUI;
- рефлексивный межсайтовый скриптинг;
- перехват аутентификационных данных через XSS.

В отдельную группу выделены угрозы информационной безопасности веб-приложений SAP. Проанализированы стандартные способы парирования этих угроз.

В третьей главе “Безопасность разработок” рассмотрена информационная безопасность разработок систем SAP R/3, в том числе наиболее вероятные ошибки в клиентском коде (обход каталога, ошибки авторизации, бэкдоры) и поиск ошибок, а также результаты анализа кода (SQL инъекции, несанкционированный доступ к таблицам БД, динамические вызовы, обход каталога, инъекции в системные вызовы, межсайтовый скриптинг, инъекции в ABAP вызовы, бэкдоры). Даны стандартные рекомендации по повышению информационной безопасности разработок систем SAP R/3

В четвёртой главе “Администрирование и внутренние угрозы” исследованы стандартные средства защиты информации в SAP с помощью системного администрирования (AGS Security Service – обновления, EWA – анализ и ключевые системные отчеты, SOS service – оптимизация и валидация конфигурации). Проанализированы внутренние угрозы SAP (угрозы социальной инженерии вследствие атак несанкционированного доступа к информации или системам хранения информации без использования технических средств, но с помощью недобросовестного персонала SAP-системы). Даны стандартные рекомендации по парированию внутренних угроз.

В пятой главе “Угрозы облачных вычислений sap и методы их защиты” рассмотрены стандартные угрозы облачных вычислений SAP (трудности при перемещении обычных серверов в вычислительное облако, динамичность виртуальных машин, уязвимости внутри виртуальной среды и др.) и методы защиты от них. Для последних проанализированы их достоинства и недостатки, а также предпосылки возникновения угроз информационной безопасности. Проанализированы возможные атаки на облака (традиционные атаки на ПО, функциональные атаки на элементы облака, атаки на клиента, атаки на гипервизор, атаки на системы управления) и решения по их устранению.

В шестой главе исследованы достоинства и недостатки программного обеспечения одного из важнейших стандартных средств защиты информации в SAP – средства для анализа регулярно поступающих обновлений системы. Установлено, что это ПО не позволяет работать со всеми системами в ландшафте одновременно, а только с одной из них, а также не обладает достаточным набором пользовательским параметров для кастомизации требований.

Разработано программное средство, свободное от перечисленных недостатков. Средство отлажено, протестировано и пригодно к эксплуатации.

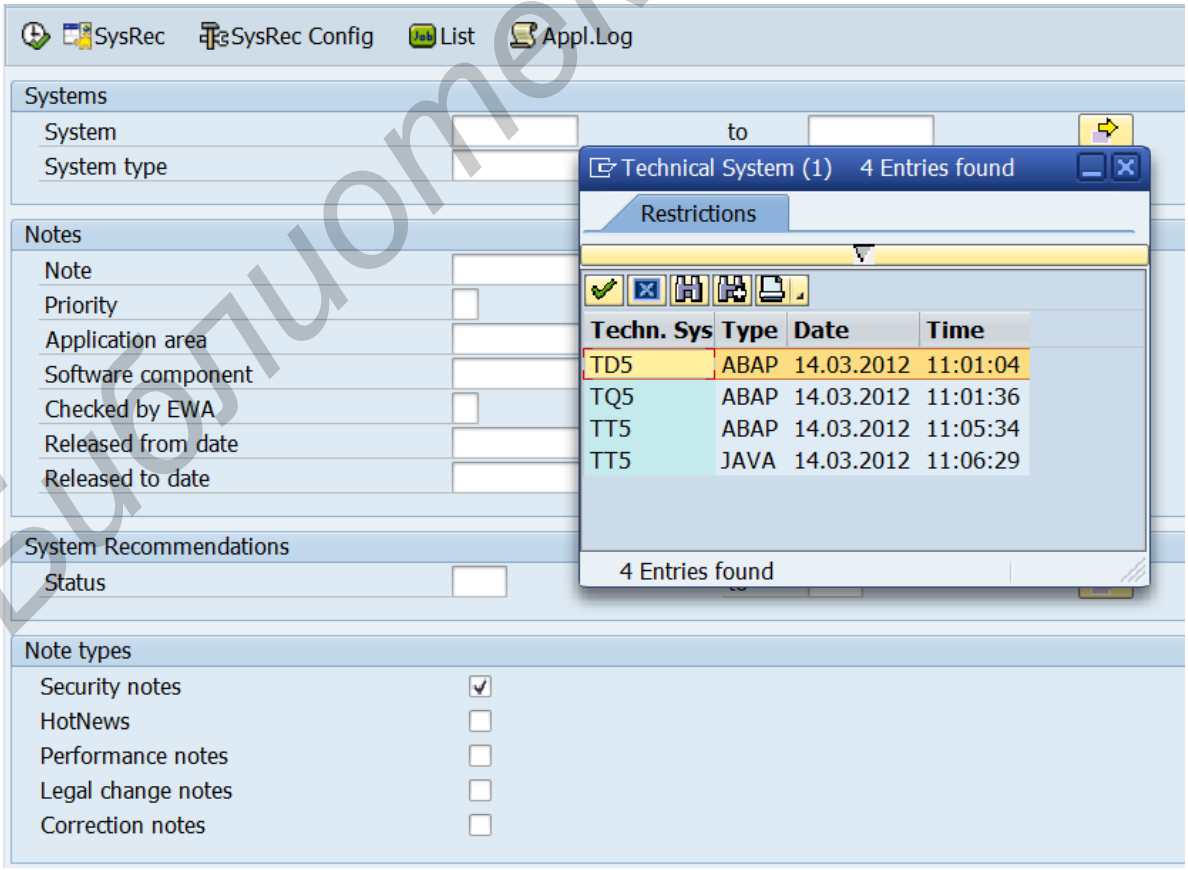
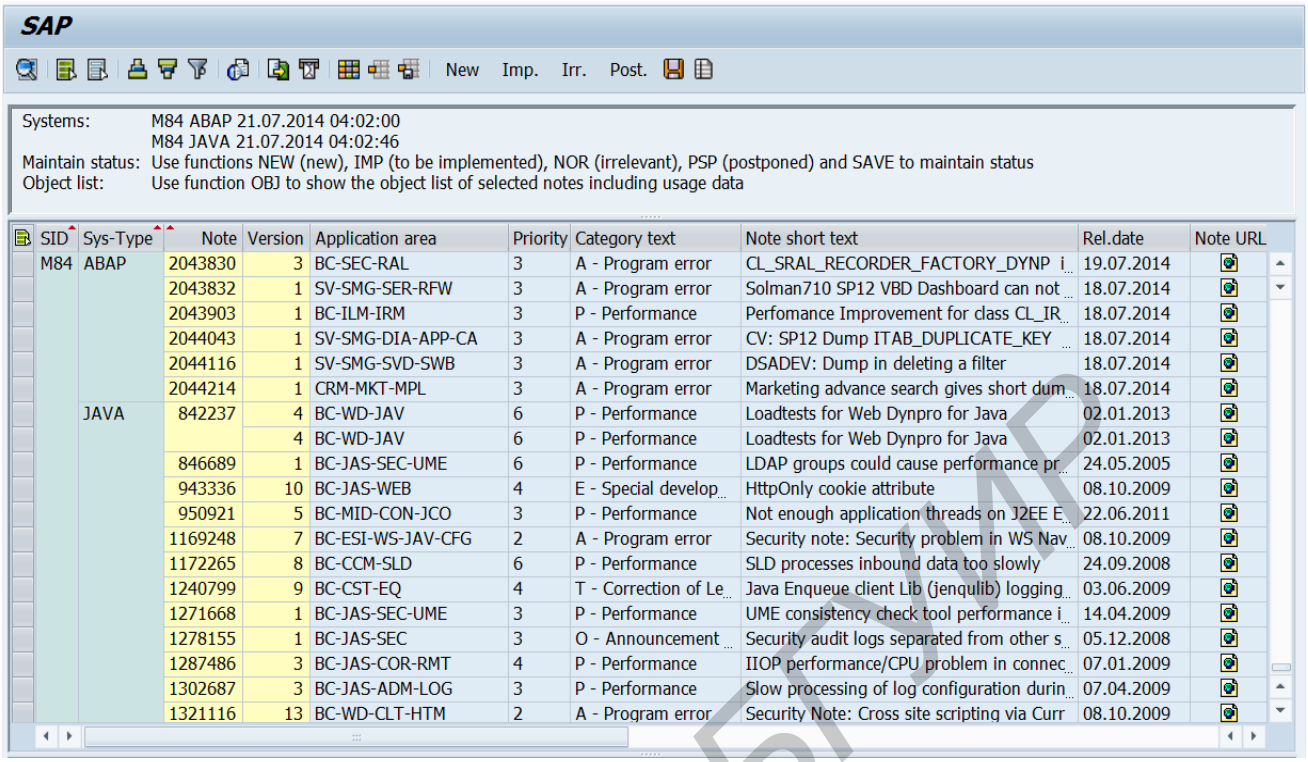
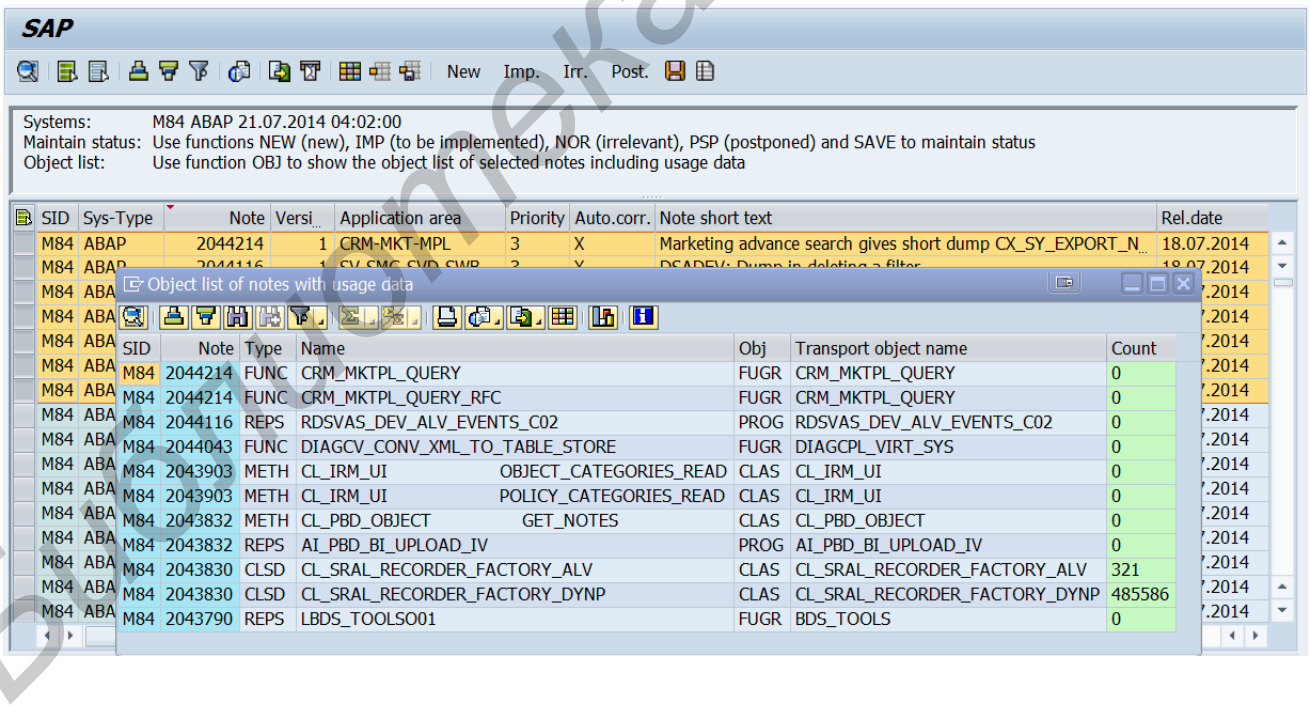



**Рис. 1.1 Стартовый экрана программы**




| SID | Sys-Type | Note | Version | Application area | Priority | Category text | Note short text | Rel.date | Note URL |
|---|---|---|---|---|---|---|---|---|---|
| M84 | ABAP | 2043830 | 3 | BC-SEC-RAL | 3 | A - Program error | CL_SRAL_RECORDER_FACTORY_DYNP i | 19.07.2014 | |
| | | 2043832 | 1 | SV-SMG-SER-RFW | 3 | A - Program error | Solman710 SP12 VBD Dashboard can not | 18.07.2014 | |
| | | 2043903 | 1 | BC-ILM-IRM | 3 | P - Performance | Perfomance Improvement for class CL_IR | 18.07.2014 | |
| | | 2044043 | 1 | SV-SMG-DIA-APP-CA | 3 | A - Program error | CV: SP12 Dump ITAB_DUPLICATE_KEY | 18.07.2014 | |
| | | 2044116 | 1 | SV-SMG-SVD-SWB | 3 | A - Program error | DSADEV: Dump in deleting a filter | 18.07.2014 | |
| | | 2044214 | 1 | CRM-MKT-MPL | 3 | A - Program error | Marketing advance search gives short dum | 18.07.2014 | |
| | JAVA | 842237 | 4 | BC-WD-JAV | 6 | P - Performance | Loadtests for Web Dynpro for Java | 02.01.2013 | |
| | | | 4 | BC-WD-JAV | 6 | P - Performance | Loadtests for Web Dynpro for Java | 02.01.2013 | |
| | | 846689 | 1 | BC-JAS-SEC-UME | 6 | P - Performance | LDAP groups could cause performance pr | 24.05.2005 | |
| | | 943336 | 10 | BC-JAS-WEB | 4 | E - Special develop | HttpOnly cookie attribute | 08.10.2009 | |
| | | 950921 | 5 | BC-MID-CON-JCO | 3 | P - Performance | Not enough application threads on J2EE E | 22.06.2011 | |
| | | 1169248 | 7 | BC-ESI-WS-JAV-CFG | 2 | A - Program error | Security note: Security problem in WS Nav | 08.10.2009 | |
| | | 1172265 | 8 | BC-CCM-SLD | 6 | P - Performance | SLD processes inbound data too slowly | 24.09.2008 | |
| | | 1240799 | 9 | BC-CST-EQ | 4 | T - Correction of Le | Java Enqueue client Lib (jenqulib) logging | 03.06.2009 | |
| | | 1271668 | 1 | BC-JAS-SEC-UME | 3 | P - Performance | UME consistency check tool performance i | 14.04.2009 | |
| | | 1278155 | 1 | BC-JAS-SEC | 3 | O - Announcement | Security audit logs separated from other s | 05.12.2008 | |
| | | 1287486 | 3 | BC-JAS-COR-RMT | 4 | P - Performance | IIOP performance/CPU problem in connec | 07.01.2009 | |
| | | 1302687 | 3 | BC-JAS-ADM-LOG | 3 | P - Performance | Slow processing of log configuration durin | 07.04.2009 | |
| | | 1321116 | 13 | BC-WD-CLT-HTM | 2 | A - Program error | Security Note: Cross site scripting via Curr | 08.10.2009 | |

**Рис 1.2 Результат программы**




| SID | Sys-Type | Note | Versi | Application area | Priority | Auto.corr. | Note short text | Rel.date |
|---|---|---|---|---|---|---|---|---|
| M84 | ABAP | 2044214 | 1 | CRM-MKT-MPL | 3 | X | Marketing advance search gives short dump CX_SY_EXPORT_N | 18.07.2014 |

| SID | Note | Type | Name | Obj | Transport object name | Count |
|---|---|---|---|---|---|---|
| M84 | 2044214 | FUNC | CRM_MKTPL_QUERY | FUGR | CRM_MKTPL_QUERY | 0 |
| M84 | 2044214 | FUNC | CRM_MKTPL_QUERY_RFC | FUGR | CRM_MKTPL_QUERY | 0 |
| M84 | 2044116 | REPS | RDSVAS_DEV_ALV_EVENTS_C02 | PROG | RDSVAS_DEV_ALV_EVENTS_C02 | 0 |
| M84 | 2044043 | FUNC | DIAGCV_CONV_XML_TO_TABLE_STORE | FUGR | DIAGCPL_VIRT_SYS | 0 |
| M84 | 2043903 | METH | CL_IRM_UI OBJECT_CATEGORIES_READ | CLAS | CL_IRM_UI | 0 |
| M84 | 2043903 | METH | CL_IRM_UI POLICY_CATEGORIES_READ | CLAS | CL_IRM_UI | 0 |
| M84 | 2043832 | METH | CL_PBD_OBJECT GET_NOTES | CLAS | CL_PBD_OBJECT | 0 |
| M84 | 2043832 | REPS | AI_PBD_BI_UPLOAD_IV | PROG | AI_PBD_BI_UPLOAD_IV | 0 |
| M84 | 2043830 | CLSD | CL_SRAL_RECORDER_FACTORY_ALV | CLAS | CL_SRAL_RECORDER_FACTORY_ALV | 321 |
| M84 | 2043830 | CLSD | CL_SRAL_RECORDER_FACTORY_DYNP | CLAS | CL_SRAL_RECORDER_FACTORY_DYNP | 485586 |
| M84 | 2043790 | REPS | LBDS_TOOLSO01 | FUGR | BDS_TOOLS | 0 |

**Рис 1.3 Статистика использования**

# ЗАКЛЮЧЕНИЕ

- Рассмотрен объект исследования – ERP-системы, и, в частности, наиболее распространённый их вариант – системы автоматизированного управления SAP R/3. Для последних проанализированы их достоинства и недостатки, а также предпосылки возникновения угроз информационной безопасности.
- Выделены наиболее вероятные общие угрозы информационной безопасности систем SAP R/3, к которым отнесены:
  - атаки на клиентские рабочие станции;
  - переполнения буфера в SAP GUI;
  - переполнения буфера в ACTIVEX компонентах SAP GUI;
  - рефлексивный межсайтовый скриптинг;
  - перехват аутентификационных данных через XSS. В отдельную группу выделены угрозы информационной безопасности веб-приложений SAP. Проанализированы стандартные способы парирования этих угроз.
- Рассмотрена информационная безопасность разработок систем SAP R/3, в том числе наиболее вероятные ошибки в клиентском коде (обход каталога, ошибки авторизации, бэкдоры) и поиск ошибок, а также результаты анализа кода (SQL инъекции, несанкционированный доступ к таблицам БД, динамические вызовы, обход каталога, инъекции в системные вызовы, межсайтовый скриптинг, инъекции в ABAP вызовы, бэкдоры). Даны стандартные рекомендации по повышению информационной безопасности разработок систем SAP R/3.
- Кратко исследованы стандартные средства защиты информации в SAP с помощью системного администрирования (AGS Security Service – обновления, EWA – анализ и ключевые системные отчеты, SOS service – оптимизация и валидация конфигурации). Проанализированы внутренние угрозы SAP (угрозы социальной инженерии вследствие атак несанкционированного доступа к информации или системам хранения информации без использования технических средств, но с помощью недобросовестного персонала SAP-системы). Даны стандартные рекомендации по парированию внутренних угроз.
- Рассмотрены стандартные угрозы облачных вычислений SAP (трудности при перемещении обычных серверов в вычислительное облако, динамичность виртуальных машин, уязвимости внутри виртуальной среды и др.) и методы защиты от них. Для последних проанализированы их достоинства и недостатки, а также предпосылки возникновения угроз информационной безопасности. Проанализированы возможные атаки на

облака (традиционные атаки на ПО, функциональные атаки на элементы облака, атаки на клиента, атаки на гипервизор, атаки на системы управления) и решения по их устранению.

- Детально исследованы достоинства и недостатки программного обеспечения одного из важнейших стандартных средств защиты информации в SAP с помощью системного администрирования – AGS Security Service – средства для анализа регулярно поступающих обновлений системы. Установлено, что это ПО не позволяет работать со всеми системами в ландшафте одновременно, а только с одной из них, а также не обладает достаточным набором пользовательским параметров для кастомизации требований.

Разработано программное средство, свободное от перечисленных недостатков. Средство отлажено, протестировано и пригодно к эксплуатации.

# СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А Адериха А.В., Николаенко В.В., Сечко Г.В. Практическая проверка возможностей технологии SAP HANA // Материалы XIX МНТК «Информационные системы и технологии» (ИСТ–2013), Нижний Новгород (19 апреля 2013 г.). –Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2013. – С. 92.

2-А Адериха А. В. Миграция SAP R/3 4.7C Non-unicode на ECC 6.0 Unicode с использованием системы PANAYA // 49-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 4 мая 2013 года). – Мн.: БГУИР, 2013. – 91 с. с ил. – С. 58.

3-А Адериха А.В., Николаенко Е.В. Анализ уязвимостей SAP // 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. 172-173.

4-А Адериха А. В., Скворчевская Я. А. Защита программных продуктов SAP // 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. 5.

5-А Адериха А.В., Пачинин В.И. Защита программных продуктов SAP // Материалы XX МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014. – С. 264.

.