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

УДК 004.056.53(476)

Щурко
Алексей Леонтьевич

Методика обнаружения инсайдерских атак на объектах информатизации средств вычислительной техники на примере РУП «Минскэнерго»

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
Утин Леонид Львович
к.т.н, доцент

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

При современной всеобщей информатизации деятельности организаций неоспоримо актуальным является вопрос защиты информации. Особо при этом следует выделить инсайдерские угрозы, исходящие от собственных сотрудников, а не извне. Их особенность заключается в том, что сотрудники, например, могут иметь легкий легализованный доступ к информации и активам организации, у них зачастую есть информация о методах безопасности, им не надо обходить внешнюю систему защиты.

Недооценка этих угроз может обернуться для предприятия большими убытками и даже банкротством.

По данным статистики компаний, специализирующихся на вопросах защиты информации, инсайдерство может быть как случайным, так и преднамеренным.

В одних случаях вредительские по отношению к компании действия совершаются инсайдерами в силу уязвленного самолюбия, желания отомстить, ярости, в других – из-за желания заработать, преследования финансовой выгоды. Неосведомленность и игнорирование правил также могут нанести непреднамеренный, но не меньший ущерб.

Организации могут сталкиваются с целым рядом инсайдерских рисков. Однако пока нет ни одного комплексного решения, которое позволяло бы полностью защитить компанию от воздействия всех этих угроз.

Тем не менее, можно сократить вероятность нанесения ущерба инсайдерами. Для этого необходим грамотный наем сотрудников, комбинирование организационных и технических методов. В каждом конкретном случае эти методы будут носить специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью данной магистерской работы является расширение профессиональных знаний, полученных в процессе обучения в магистратуре, формирования практических умений и навыков ведения самостоятельной научной работы и исследования. Для этого необходимо разработать методику обнаружения инсайдерских атак для РУП «Минскэнерго».

Основными задачами являются:

1 Определение наиболее важных факторов, влияющих на обнаружение и идентификацию инсайдерских атак;
2 Анализ исходной информационной защищенности на РУП «Минскэнерго»;
3 Разработка методики обнаружения инсайдерских атак для РУП «Минскэнерго».

Тема является актуальной, так как связана с исключением угроз безопасности информации от внутреннего нарушителя на энергетическом предприятии, от стабильной работы которого зависит развитие общественного производства.

Для обеспечение информационного взаимодействия в интересах эффективного и бесперебойного удовлетворения потребности народного хозяйства и населения в электрической и тепловой энергии в РУП «Минскэнерго» создана информационная система.

Информатизация хозяйственной деятельности способствует её облегчению, интенсификации и, как следствие, повышению экономической эффективности. Но наряду с передачей, обработкой и хранением информации, важно обеспечить её целостность, конфиденциальность и доступность. Исключить как внешние, так и внутренние угрозы.

Личным вкладом автора является разработка методики обнаружения инсайдерских атак для РУП «Минскэнерго».

Результаты работы были апробированы на XX Международной научно-технической конференции «Современные средства связи» в БГАС докладом в секции «Информационные технологии и защита информации» на тему «Разработка плана защиты информации от инсайдерских атак для организации».

КРАТКОЕ СОДЕРЖАНИЕ

В первой главе рассмотрена актуальность проблемы на конкретных примерах, произошедших в 2015 году.

Проанализирована статистика компаний, специализирующихся на вопросах защиты информации.

Приведена классификация инсайдеров, проанализированы причины инсайдерства. Рассмотрены виды инсайдерских угроз.

Сделаны выводы о том, что сотрудники бывают разные и что если бы были методы определения предрасположенности к инсайдерству, то можно было бы изначально отобрать только добросовестных сотрудников и решить,

таким образом, проблему.

Показано, что инсайдерство подразумевает различные угрозы. Защита (противодействие) во многом будет зависеть от целей инсайдера – от вида угрозы.

Рассмотрены существующие методы обнаружения и противодействия инсайдерским атакам:

1 Обеспечение грамотного найма кадров, отслеживание атмосферы взаимоотношений в коллективе, разрешение конфликтов (мероприятия психологического плана);
2 Регламентирование деятельности сотрудников, ознакомление их с ответственностью за нарушение этого регламента (организационные мероприятия);
3 Обеспечение системы безопасности как комплекса программно-аппаратных средств для информационной системы (технические мероприятия).

Отмечено, что можно применять отдельные средства защиты для каждого возможного канала утечки информации, а также, что можно воспользоваться комплексами, подразумевающими централизованное управление и единую базу инцидентов информационной безопасности для анализа. Рассмотрены виды таких комплексов.

Сделан вывод о комплексности подхода к минимизации вероятности нанесения ущерба инсайдерами.

Во второй главе разработана методика обнаружения инсайдерских атак для РУП «Минскэнерго».

Определены наиболее важные факторы, влияющие на обнаружение и идентификацию инсайдерских атак.

Описана существующая информационная система, проведена классификация всей внутренней информации с разделением на категории по уровню доступа.

Определено, где может произойти утечка: где информация хранится, в каких процессах используется, кто имеет к ней доступ и какие точки выхода (каналы утечки) следует защитить.

Проанализирована исходная информационная защищенность на предприятии. Выявлены недостатки.

На основе выявленных недостатков, разработана усовершенствованная методика обнаружения инсайдерских атак для РУП «Минскэнерго».

ЗАКЛЮЧЕНИЕ

В данной магистерской диссертации разработана методика обнаружения инсайдерских атак для РУП «Минскэнерго».

В рамках поставленной цели, были выполнены все задачи в полном объеме.

Показана актуальность проблемы на конкретных примерах. Проанализированы причины инсайдерства, виды инсайдерских атак.

Сделаны выводы о том, что сотрудники бывают разные и что если бы были методы определения предрасположенности к инсайдерству, то можно было бы изначально отобрать только добросовестных сотрудников и решить, таким образом, проблему.

Показано, что инсайдерство подразумевает различные угрозы. Защита (противодействие) во многом будет зависеть от целей инсайдера – от вида угрозы

Рассмотрены методы обнаружения и противодействия данному виду нарушений.

Отмечено, что можно применять отдельные средства защиты для каждого возможного канала утечки информации, а также, что можно воспользоваться комплексами, подразумевающими централизованное управление и единую базу инцидентов информационной безопасности для анализа. Рассмотрены виды таких комплексов.

Определены наиболее важные факторы, влияющие на обнаружение и идентификацию инсайдерских атак на предприятии:

1 Понимание хозяйственной деятельности предприятия, построения и функционирования информационной системы предприятия;
2 Классифицированность информации по категориям доступа и распространения;
3 Знание, где информация ограниченного распространения хранится, в каких процессах используется, кто имеет к ней доступ и какие есть точки выхода (каналы утечки);
4 Идентифицированность каждого сотрудника в сети.

Конкретно для РУП «Минскэнерго» проанализирован документооборот, проведена инвентаризация информации, определены потенциальные инсайдеры – сотрудники предприятия, имеющие доступ к информации распространение и (или) предоставление которой ограничено – и каналы утечки информации (usb порты, интернет на их рабочих местах, доступные им принтеры).

Проанализирована исходная информационная защищенность. Для предприятия выявлены возможные источники угроз, проанализированы вероятности возникновения этих угроз и их опасность, оценена актуальность обеспечения защиты.

К актуальным отнесены:

1 Проблема несанкционированного физического и логического доступа, несмотря на существующие меры;
2 Угроза выявления паролей для аутентификации;
3 Отсутствие контроля выполняемых операций на соответствие установленным правилам.

На основе выявленных недостатков, разработана усовершенствованная методика обнаружения инсайдерских атак для РУП «Минскэнерго»

Выполнены следующие мероприятия:

1 Выработаны рекомендации по разработке инструкций касательно организационных моментов, необходимых для обнаружения инсайдерских атак и привлечения виновных к ответственности (определены порядок парольной, антивирусной защиты, доступа к ресурсам, обязанности и ответственность пользователей);
2 Доработано логическое разграничение доступа в системе 1С;
3 Дополнены существующие меры физической защиты опломбированием системных блоков и выставлением пароля на BIOS компьютеров;
4 Выбрана система контроля для выявления попыток противоправных действий с учетом особенностей информационной системы предприятия (Symantec DLP 12.5).

Предлагаемые решения должны обеспечить приемлемый уровень защиты от инсайдеров для РУП «Минскэнерго».

Теоретическая значимость данной работы заключается в анализе законов, нормативных актов в области защиты информации от инсайдеров, современной научной литературы касательно данной темы.

Практическая значимость данной работы заключается в возможности реализации на объекте исследования – РУП «Минскэнерго».

Данная работа может быть полезна специалистам занимающимся защитой информации на предприятиях, так как демонстрирует методику защиты в конкретных условиях.

СПИСОК ПУБЛИАЦИЙ СОИСКАТЕЛЯ

1-А. Щурко А. Л. Разработка плана защиты организации от инсайдерских атак / А. Л. Щурко // Современные средства связи : материалы XX Междунар. науч.-техн. конф., 14–15 окт. 2015 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск : УО ВГКС, 2015. – с. 209