InformationSecurity

www.itsec.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ № 1, март 2016

Издание компании Groteck

СПЕЦРАЗДЕЛ

SOC

XIII МЕЖДУНАРОДНАЯ ВЫСТАВКА

infosecurity

RUSSIA

27–29 сентября 2016

СПЕЦПРОЕКТ

ЗАЩИТА АСУ ТП

МНОГОУРОВНЕВАЯ ЗАЩИТА КВО

Александр Васильев,
директор Смоленской атомной электростанции,
филиал АО "Концерн Росэнергоатом"

powered by intersec

ТБ ФОРУМ®

Технологии Безопасности

БИЗНЕС В ТРЕНДЕ: ТЕНДЕНЦИИ. ИНВЕСТИЦИИ РЕШЕНИЯ. ЛИЧНОСТИ

ОТРАСЛЕВЫЕ РЕШЕНИЯ • КЕЙСЫ ПО ВЕРТИКАЛЬНЫМ РЫНКАМ • БЕЗОПАСНЫЙ УМНЫЙ ГОРОД • СОВЕЩАНИЕ СИТИ-МЕНЕДЖЕРОВ • ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ • ТРЕКИНГ И МОНИТОРИНГ • ТРАНСПОРТИРОВКА ВАЖНЫХ ГРУЗОВ • КИБЕРУГРОЗЫ СИСТЕМАМ БЕЗОПАСНОСТИ • КОНВЕРГЕНЦИЯ ИТ И СБ • БИЗНЕС-АНАЛИТИКА • УПРАВЛЕНИЕ РИСКАМИ • ПРЕДОТВРАЩЕНИЕ ПОТЕРЬ • МОДЕЛЬ УГРОЗ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ • РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ • ИНЖЕНЕРИЯ БЕЗОПАСНОСТИ • АРХИТЕКТУРА И ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ • НОВЫЕ ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ И ОЦЕНКА ПРОЕКТОВ • БЕЗОПАСНОСТЬ НАЦИОНАЛЬНЫХ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ • КРИТИЧЕСКИЕ И ОСОБО ВАЖНЫЕ ОБЪЕКТЫ • ЗАЩИТА ПЕРИМЕТРА • АНТИТЕРРОР • ИМПОРТОЗАМЕЩЕНИЕ • ЛОКАЛИЗАЦИЯ ПРОИЗВОДСТВА • СТАРТАПЫ В БЕЗОПАСНОСТИ • ПИЛОТНЫЕ ПРОЕКТЫ

КОВОРКИНГ ДЛЯ ПРОФЕССИОНАЛОВ

- Конечных заказчиков
- Промышленных предприятий
- Городских администраций
- Проектных организаций
- Монтажных организаций
- Инсталляторов
- Интеграторов
- Служб безопасности
- Специальных служб
- Министерств и ведомств

2017

КРОКУС ЭКСПО

Регистрация по ссылке GO.TBFORUM.RU

Groteck Business Media

www.tbforum.ru

Екатерина Данилина,
выпускающий редактор журнала "Информационная безопасность/ Information Security"

Защита автоматизированных систем управления технологических процессов, ставшая главной темой первого в новом году номера нашего журнала, – тема интересная, но сложная. Несмотря на развитие рынка, реального практического опыта по обеспечению защиты АСУ ТП в России очень мало. Но и его будет достаточно, чтобы выявить некоторые риски системного характера, возникающие при реализации проектов по обеспечению защиты.

К сожалению, не все представители предприятий, относящихся к КВО, готовы делиться своим опытом, но заинтересованность с их стороны, безусловно, есть, так как сейчас к основному и долгое время лидирующему риску – человеческому фактору – добавились еще и риски внешнего и удаленного несанкционированного доступа. Подобное вмешательство может привести не просто к остановке производства и потере прибыли, но и к серьезным последствиям вплоть до экологических катастроф.

Одной из причин столь высокой внешней вирусной активности и увеличения инцидентов в сфере информационной безопасности стало использование многими компаниями систем, управляющих производством, транспортом, водоснабжением и энергоресурсами, которые легко находятся поисковыми системами в Интернете. На январь 2015 года исследователи Positive Technologies обнаружили таким образом более 140 000 различных компонентов АСУ ТП.

Причем владельцы таких систем не осознают, насколько хорошо их ресурсы "видны снаружи".

Контуры управления современными промышленными предприятиями вышли за пределы охраняемых зон – устарела сама концепция периметра как локализованного объекта. Распространение мобильных устройств, облачных вычислений и различных технологий для удаленной работы – все это послужило обострению вопроса адаптации КВО к современным условиям.

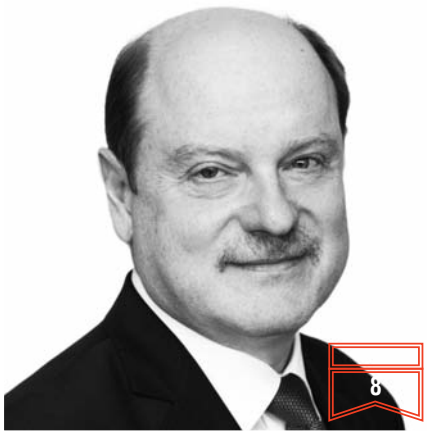
Эти и многие другие вопросы защиты АСУ ТП нашли свое отражение на страницах первого номера года.

Продолжением данной темы станет ежегодная конференция "Защита АСУ ТП" в рамках XIII Международной выставки InfoSecurity Russia 2016. Признанные эксперты рынка и заказчики поделятся опытом, обозначат основные тенденции и выработают стратегию борьбы с киберугрозами на 2016–2017 гг.

До встречи на страницах журнала "Информационная безопасность/Information Security"!

InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СОДЕРЖАНИЕ



СОДЕРЖАНИЕ

СПЕЦРАЗДЕЛ SOC

ТЕХНОЛОГИИ

КОНТРОЛЬ ДОСТУПА

ЗАЩИТА СЕТЕЙ

КРИПТОГРАФИЯ

УПРАВЛЕНИЕ

НОВЫЕ ПРОДУКТЫ И НЬЮСМЕЙКЕРЫ

Журнал "Information Security/Информационная безопасность" № 1, 2016
Издание зарегистрировано в Минпечати России
Свидетельство о регистрации ПИ № 77-17607 от 9 марта 2004 г.

Учредитель и издатель
компания "Гротек"

Генеральный директор ООО "Гротек"
Андрей Мирошкин

Издатель
Владимир Вараксин

Руководитель проекта
Наталья Рохмистрова, rohmistrova@groteck.ru

Выпускающий редактор
Екатерина Данилина, danilina@groteck.ru

Корректор
Ольга Михайлова

Дизайнеры-верстальщики
Анастасия Иванова, Ольга Пирадова

Фото на обложке
Алиса Урюпина

Группа управления заказами
Галина Скочко

Юрисконсульт
Кирилл Сухов, lawyer@groteck.ru

Департамент продажи рекламы
Наталья Рохмистрова

Рекламная служба
Тел.: (495) 647-0442, rohmistrova@groteck.ru

Отпечатано в типографии
Линтекст
Тираж 10 000. Цена свободная

Оформление подписки
Тел.: (495) 647-0442, www.itsec.ru

Департамент по распространению
Тел.: (495) 647-0442,
факс: (495) 221-0864
Для почты 123007, Москва, а/я 82
E-mail groteck@groteck.ru
Web www.groteck.ru, www.itsec.ru

Конференция ФСТЭК России на форуме "Технологии безопасности"

В рамках XXI Международного форума “Технологии безопасности” 11 февраля 2016 г. в МВЦ “Крокус Экспо” прошла 6-я ежегодная конференция “Актуальные вопросы защиты информации”. Организатор конференции – ФСТЭК России. Руководитель конференции – Виталий Лютиков, начальник Управления ФСТЭК России.

На конференции был представлен ряд новых инициатив и основополагающих документов в области защиты информации, крупнейшие разработчики и производители рассмотрели практические вопросы и подходы к обеспечению информационной безопасности, а представители регулятора поделились реальным опытом по некоторым сферам своей деятельности.

На повестке дня:

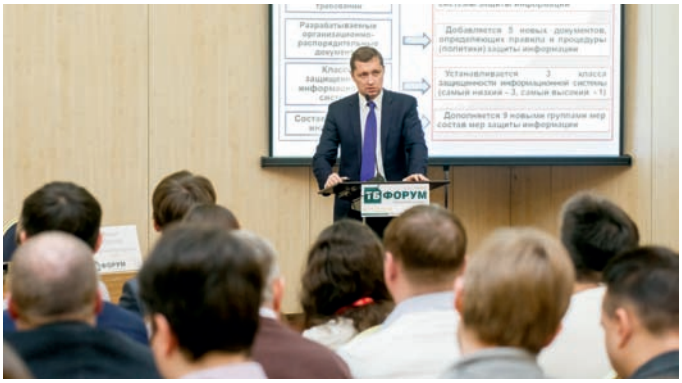
- совершенствование нормативно-правового и методического обеспечения вопросов защиты информации;
- угрозы безопасности информации и подходы к их моделированию;
- подходы к совершенствованию работ по сертификации средств защиты информации на соответствие требованиям безопасности информации;
- новые правила аккредитации органов по сертификации и испытательных лабораторий в сфере деятельности ФСТЭК России;
- лицензирование деятельности по технической защите конфиденциальной информации;
- новые методы и средства защиты информации.

Владимир Селин, директор Федеральной службы по техническому и экспортному контролю

"Уже много лет Форум "Технологии безопасности" является площадкой, объединяющей государство и бизнес и позволяющей наглядно демонстрировать возможности технических средств защиты информации, а также вести конструктивный диалог по проблемам рынка информационной безопасности в условиях совершенствующихся угроз безопасности информации. В связи с развитием информационных технологий тематика безопасности информационных систем становится как нельзя более актуальной. Форум во многом способствует развитию конкурентоспособности российских продуктов и технологий в отрасли безопасности, повышению качества услуг по защите информации".

Сергей Кузнецов, коммерческий директор ЦЗИ ГК "Конфидент"

"Наша компания уже не первый год поддерживает ТБ Форум. Это отлично организованная площадка для общения различных участников рынка информационной безопасности – регуляторов, разработчиков, конечных пользователей. На Форуме нередко бывают заложены основы сотрудничества по реализации новых интересных проектов.
Участие ФСТЭК России придает ТБ Форуму особый статус и значимость. Участники мероприятия имеют возможность напрямую от регулятора получить информацию о новых тенденциях, требованиях, изменениях в законодательной сфере, а также услышать ответы на все интересующие вопросы.
Со своей стороны, помимо новостей о продуктовой линейке Dallas Lock, мы поделились видением текущей ситуации с информационной безопасностью в госсекторе и прогнозами на 2016 год".



С ключевыми докладами выступили представители регулятора:

- "Совершенствование нормативного и методического обеспечения вопросов защиты информации" (В.С. Лютиков, начальник управления ФСТЭК России).
- "Проблемные вопросы сертификации средств защиты информации. Подходы по совершенствованию качества сертифицированных средств защиты информации" (Д.Н. Шевцов, заместитель начальника управления ФСТЭК России).
- "Особенности аккредитации испытательных лабораторий и органов по сертификации" (М.Е. Костенко, начальник отдела ФСТЭК России).
- "Совершенствование требований по защите информации, предъявляемых к межсетевым экранам" (К.А. Валентинович, советник отдела управления ФСТЭК России).
- "О мерах по повышению лицензионных требований к соискателям лицензий и лицензиатам на осуществление деятельности по технической защите конфиденциальной информации и по разработке и производству средств защиты конфиденциальной информации" (Н.И. Мищенко, начальник отдела ФСТЭК России).
- "Банк данных угроз безопасности информации и уязвимостей программного обеспечения: реалии и перспективы" (В.А. Минаков, начальник отдела "ФАУ "ГНИИИ ПТЗИ ФСТЭК России").

Новейшие практики, методы и подходы к решению проблем защиты информации представили руководители компаний ЗАО "Циско Системз", ЗАО "Крафтвей Корпорейшн ПЛС", ООО "Диджитал Секьюрити", ЗАО "Позитив текнолоджиз", ЗАО "Лаборатория Касперского", ООО "Конфидент", ЗАО "НПО Эшелон", ЗАО "Перспективный мониторинг", ООО "АРСИЭНТЕК".

Партнером конференции выступила компания "Конфидент".

22-й Международный форум "Технологии безопасности 2017"

ТБ Форум – площадка, на которой обсуждаются спрос и сбыт, требования и возможности, демонстрируются передовые технологии и решения, ведется реальный бизнес. Здесь формируется повестка дня и индустрия взаимодействует с потребителями и между собой. ●

До встречи на ТБ Форуме powered by Intersec 2017!
7–9 февраля 2017 г.
Крокус Экспо, павильон 3, зал 20.
www.tbforum.ru

В РАМКАХ «РОССИЙСКОЙ НЕДЕЛИ ВЫСОКИХ ТЕХНОЛОГИЙ»

СВЯЗЬ

10–13.05

2016

Информационные и коммуникационные технологии

ЭКСПОЦЕНТР

МКФ 2016

РАЭК

Организатор: ЗАО «Экспоцентр»

При поддержке:
• Федерального агентства связи (Россвязь)
• Российской ассоциации электронных коммуникаций (РАЭК)

Под патронатом Торгово-промышленной палаты РФ

12+

Реклама

Россия, Москва, ЦВК «Экспоцентр»

www.sviaz-expo.ru

Безопасен ли промышленный Интернет вещей?

Радж Самани (Raj Samani), *вице-президент, технический директор по безопасности компании McAfee (Intel Security) региона EMEA*

– Раньше ваша организация носила название McAfee, а сейчас идет активный ребрендинг в Intel Security. Радж, расскажите, пожалуйста, о причинах такого решения.

– В данный момент McAfee является частью Intel и была ею в течение определенного времени. Бренд Intel Security не оставляет отрасли никаких сомнений на этот счет.

Проблема с облачными технологиями сводится к тому, чтобы понять, у каких из них задействованы необходимые средства контроля безопасности.

– Компания Intel Security активно приобретала и другие известные компании. На российском рынке много шуму наделало приобретение компании StoneSoft в 2013 году. Как прошла интеграция решений этой компании в общий портфель Intel Security?

– Если говорить в более широком смысле, а не о конкретных продуктах, то мы сосредоточены на развитии сервисов, не ограничиваясь лишь своими собственными технологиями, однако разработки в области DXL (Data Exchange Layer) обеспечивают возможность полной интеграции сторонних продуктов с портфелем нашей компании.

– И в дополнение к предыдущему вопросу – удается ли поддерживать в актуальном состоянии сертификаты ФСБ и ФСТЭК, ранее выданные на продукцию компании StoneSoft, или заказчикам рекомендовано переходить на другие решения компании Intel Security?

– Мы имеем довольно обширную географию присутствия, в связи с чем с полной ответственностью подходим к вопросу сертификации наших решений, в соответствии с предъявляемыми требованиями.

По вопросу обеспечения безопасности среды IoT нет однозначного ответа. И это не только лишь техническая дискуссия, поскольку в игру вступает множество других факторов, в том числе сертификация от поставщика средств автоматизации. Кроме того, и цена становится реальной проблемой.

– Как вы оцениваете позиции Intel Security на российском и мировом рынках? Какие компании вы считаете своими основными конкурентами?

– Как я уже говорил, наше сотрудничество с компанией Intel позволяет предоставлять реальный фундамент в виде аппаратного обеспечения, который полностью заслуживает доверия. Это необходимо, поскольку как только мы пришли к рассмотрению вопроса об оцифровке важнейших элементов нашей инфраструктуры, слепо доверять механизмам аутентификации просто невозможно. Работа с компанией Intel подразумевает, что мы можем предложить эти решения нашим клиентам.

Реальную конкуренцию на сегодняшний день составляют киберпреступники, пытающиеся пробиться через редуты корпоративных защитных укреплений. Мы постоянно сталкиваемся с опасениями клиентов по части реализации инновационных решений на своих предприятиях. В данной связи мы полностью готовы к сотрудничеству с правоохранительными органами для решения вопросов такой конкуренции.

– Как вы оцениваете влияние санкций на работу компании на российском рынке? И какие тенденции развития этого рынка вы видите в ближайшей и среднесрочной перспективе?

– Мы работаем в глобальной среде и, следовательно, должны быть готовы к любым изменениям. От этого зависит безопасность современного общества.

– Концепция Интернета вещей для встроенных систем и в ИТ-секторе сейчас горячо обсуждается . В то же время, многие подходы IoT довольно расплывчаты. Как вы видите эту ситуацию?

– Что ж, я написал ряд книг на эту тему, но я хотел бы подчеркнуть, что по вопросу обеспечения безопасности среды IoT нет однозначного ответа. И это не только лишь техническая дискуссия, поскольку в игру вступает множество других факторов, в том числе сертификация от поставщика средств автоматизации. Кроме того, и цена становится реальной проблемой. Вы уже видели плоды наших партнерских программ, например с компанией Honeywell. Мы начали сотрудничество в целях усовершенствования защиты критически важной промышленной инфраструктуры и промышленного Интернета вещей (IIoT). В результате взаимоинтеграции заказчикам предлагается ПО, способное защитить их системы управления от вредоносных программ и ненадлежащего использования.

– Многие люди еще не доверяют IoT. Однако эта технология продолжает развиваться и внедряется на крупных промышленных предприятиях. Согласно исследованию, компании Ipsos Public Affairs, растущая угроза кибератак на подобного рода объекты является одной из самых актуальных проблем. Что нужно сделать для повышения уровня безопасности промышленных предприятий, не тормозя при этом их технологический прогресс?

– Безопасность и конфиденциальность на критически важных объектах – это, безусловно, одна из первостепенных задач, но отнюдь не единственная. Нужно постоянно анализировать ландшафт угроз, чтобы быть уверенным в наличии правильного средства защиты, ведь злоумышленники постоянно изменяют модель своего пове-

дения. Разведка, направленная на поиск реальных угроз, будет критически важным компонентом бизнеса.

– Должны ли будут все подключаемые устройства соответствовать определенному стандарту? Или на предприятиях будет использоваться несколько экосистем, со своими стандартами?

– Конечно, мы хотели бы единый стандарт, однако, как мы уже смогли убедиться, в будущем их будет немало. Даже многое из разрабатываемого сейчас имеет свою специфику, однако самое главное – убедиться в том, что наши разработки обладают всем необходимым для интеграции с различными системами.

– Не повысит ли IoT уровень уязвимости промышленных предприятий в вопросе безопасности?

– Риски определенно возникнут. Тем не менее, они, вероятно, будут новыми, являя собой и новые возможности. Будут ли риски выше, чем раньше? Время покажет.

– В 2014 году компания Intel приняла участие в инициативах по разработке стандартов и систем мониторинга "умных" сетей электроснабжения (Smart Grid). Речь идет о совместном проекте с энергетической компанией Westfalen Weser Energie. О каких результатах можно говорить уже сегодня?

– Да. Надеюсь, вы видели мою недавнюю книгу на эту тему, а также издание Whitepaper, которое мы опубликовали с Alstom. Вы можете рассчитывать, что в ближайшее время Вы определенно услышите много интересных подробностей об этом проекте.

– Говоря о новых технологиях, которые внедряют промышленные предприятия, нельзя не упомянуть и облачные технологии. Большинство экспертов считают идею внедрения публичного облака на предприятия, которые жизненно важны для нашего общества, абсурдной. С одной стороны, это экономит затраты, но с другой – последствия сбоя или нарушения работы могут быть катастрофическими. Видите ли вы какой-то альтернативный способ обеспечения безопасности сторонних сервисов, чем тот, который используется сегодня?

– Что ж, моя книга об облачных технологиях также готова *(смеется)*! Мне действительно нравятся облачные технологии, однако мы должны помнить, что понятие "облако" как таковое не существует. Есть компании, которые предлагают услуги: некоторые – безопасны, другие – нет. Проблема с облачными технологиями сводится к тому, чтобы понять, у каких из них задействованы необходимые средства контроля безопасности. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Реальную конкуренцию на сегодняшний день составляют киберпреступники, пытающиеся пробиться через редуты корпоративных защитных укреплений. Мы постоянно сталкиваемся с опасениями клиентов по части реализации инновационных решений на своих предприятиях.

Проблемы безопасности IoT в России

Григорий Сизов, *руководитель направления M2M ПАО "ВымпелКом"*

В России, на мой взгляд, сегодня недооценивают серьезность угроз, связанных с безопасностью решений IoT. Большинство отечественных разработчиков сейчас уделяет больше внимания предотвращению нецелевого использования SIM-карт, установленных в удаленных объектах инфраструктуры. Операторы связи планомерно и успешно ведут работу, предлагая системы защиты, но вопрос, как всегда, упирается в стоимость услуг. Некоторые разработчики, к сожалению, до сих пор выбирают базовый доступ в Интернет, предпочитая его защищенным решениям.

Операторы связи, наоборот, нацелены на массовые и глобальные решения, которые позволят нашим клиентам прозрачно и безопасно использовать и сто, и миллион SIM-карт, поэтому стараемся общаться с разработчиками на стадии реализации проекта для минимизации рисков в эксплуатации промышленных решений. Полагаю, в ближайшие 2–3 года отечественный рынок столкнется с угрозами совсем иного характера, когда надо будет уже защищать не саму SIM-карту от недоброжелателей, а самое важное – данные, передаваемые по сетям связи, тем более – все больше решений строится на базе SIM-чипов, которые просто физически невозможно использовать в других устройствах. Терминалы, модемы и роутеры, применяемые в сфере IoT, уже несут в себе системы защиты, но важно понимать, что уровень этой защиты должен соответствовать среде передачи данных. Равно как и сервер, общающийся с удаленными устройствами. В российской практике уже были случаи, когда злоумышленники узнавали протокол передающих устройств и IP-адреса серверов и начинали атаки с вымышленными данными, полностью выводя из строя весь сервис мониторинга удаленных объектов. Ущерб от таких действий оценить трудно, но в ближайшие годы к сети будут подключены многие автомобили с удаленным управлением, автоматизированные системы управления инфраструктурой и другие важнейшие объекты. И уже для этих решений использование публичной сети Интернет может быть опасно. Атаки на такие сервисы будут иметь очень серьезные последствия как для безопасности, так и для бизнеса компаний. Для таких решений операторы по всему миру уже давно рекомендуют отказываться от передачи данных через сеть Интернет и уходить в частные VPN, которые могут работать по всему миру, в том числе в роуминге.

Считаю, что действительно защищенные решения можно создавать уже сегодня, применяя все лучшие практики – от производителя оборудования и ПО до поставщика услуг связи. И самое важное, чтобы эти решения были масштабируемы, ведь рынок IoT – это миллиарды устройств. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Многоуровневая защита

Александр Васильев, *директор Смоленской атомной электростанции, филиал АО "Концерн Росэнергоатом"*

Смоленская АЭС – ведущее энергетическое предприятие Смоленской области, известное в нашей стране и за рубежом как один из лучших филиалов АО "Концерн Росэнергоатом". Несмотря на более чем 30-летний рабочий стаж, она продолжает устойчиво развиваться и ежегодно генерировать тремя энергоблоками-тысячниками порядка 20 млрд киловатт-часов электроэнергии. Сегодня наш диалог с директором атомной станции Александром Васильевым посвящен тому, как обеспечивают информационную безопасность на критически важном объекте.

В промышленной эксплуатации на САЭС находится три энергоблока с уран-графитовыми канальными реакторами РБМК-1000. Электрическая мощность каждого энергоблока – 1 ГВт, тепловая 3,2 ГВт. Энергоблоки с реакторами РБМК-1000 одноконтурные.

– Функционирование автоматизированных систем напрямую затрагивает интересы промышленных компаний. Вероятность атаки на подобные системы ниже, чем на многие другие, но ответственность, связанная с их защитой, в некоторых случаях несоизмеримо выше, особенно на промышленных предприятиях. Как Смоленская АЭС реализует защиту и обеспечивает работоспособность АСУ ТП?

– Обеспечение надежной и бесперебойной работы оборудования и программного обеспечения АСУ ТП – главный приоритет в деятельности обслуживающего их персонала. Работа по обеспечению информационной безопасности АСУ ТП непрерывно проводится по всему периметру потенциальных угроз.

АСУ ТП на Смоленской АЭС построены по принципу глубоко эшелонированной многоуровневой защиты. На всех этапах жизненного цикла АСУ ТП учитываются требования кибербезопасности.

Оборудование АСУ ТП размещено в помещениях с ограниченным доступом, предоставленным только определенному перечню доверенных лиц, а к особо важным элементам АСУ ТП одиночный доступ персонала запрещен вообще – такие места разрешается посещать группой не менее 2 авторизованных специалистов. Двери помещений и шкафов с оборудованием оснащены датчиками открытия, и при несанкционированном проникновении сигнализация выводится на пульты дежурного персонала и службы безопасности АЭС.

Различные АСУ ТП энергоблока Смоленской станции изолированы друг от друга и от компьютерных сетей общего пользования, а их связь с Интернетом исключена в принципе. В отдельных случаях при необходимости организации канала обмена информацией между двумя независимыми системами их взаимодействие реализуется с помощью специальных программно-технических средств межсетевого экранирования.

Программное обеспечение перед установкой на действующие АСУ ТП проверяется на стендах-имитаторах разработчиков систем и АЭС.

Важные для безопасности автоматизированные системы управления разделены на уровни. Для предотвращения кибератак на исполнительные механизмы связь между уровнями осуществляется однонаправленными оптическими связями.

Непременный атрибут современной АСУ ТП Смоленской АЭС – использование антивирусного программного обеспечения, которое является одним из последних барьеров на пути распространения вирусов и другого вредоносного программного кода.

При текущем обслуживании оборудования АСУ ТП использование съемных носителей информации минимизировано, а используемые носители учтены и подвергаются регулярному антивирусному контролю.

Несмотря на обширную географическую распределенность элементов АСУ ТП АЭС, все линии связи защищены от физического доступа, а критические связи дублированы по альтернативным маршрутам.

– В чем состоит специфика задач защиты АСУ ТП предприятий атомной отрасли? Чем она обусловлена?

– Специфика задач защиты АСУ ТП предприятий атомной отрасли обусловлена широким спектром применяемого контрольно-измерительного оборудования, линий связи, первичных преобразователей, контроллеров, разного типа и поко-

Смоленская АЭС – градообразующее, ведущее предприятие области, крупнейшее в топливно-энергетическом балансе региона. Ежегодно станция выдает в среднем 20 млрд кВт/ч электроэнергии, что составляет более 80 % от общего количества вырабатываемой энергопредприятиями Смоленщины.

ления оборудования АСУ ТП, передачей информации через гетерогенные среды, множественностью информационных связей и уровней. Каждый перечисленный аспект имеет свои особенности обеспечения информационной безопасности, соответствующей оценке потенциального риска для АСУ ТП, и, как следствие, для контролируемого ею технологического процесса энергоблока.

Объекты использования атомной энергии – источники повышенной опасности для населения и окружающей среды, поэтому и требования к надежности функционирования АСУ ТП предъявляются более строгие, чем для общепромышленных систем.

– Насколько усложняет задачу защиты АСУ ТП тот факт, что многие из таких систем уникальны, создавались давно и с использованием устаревших языков?

– На самом деле обеспечение информационной защиты оборудования АСУ ТП, разработанного в прошлом веке и имеющего встроенные операционные системы, в чем-то является менее сложной задачей, так как оно потенциально более устойчиво к воздействию современных угроз информационной безопасности, ориентированных на современные вычислительные платформы и интерфейсы.

Мы тесно сотрудничаем с разработчиками АСУ ТП. Если поддержка ранее установленных систем становится невозможна по какой-либо причине, системы проходят модернизацию с применением современных технических и программных решений, удовлетворяющих требованиям по кибербезопасности.

– Достаточно ли сейчас на рынке ресурсов, чтобы обеспечить полноценную защиту АСУ ТП, в том числе компетентных специалистов и технических средств защиты?

– Удаление объектов атомной энергии от крупных населенных пунктов – естественная причина дефицита компетентных специалистов в области информационной безопасности, однако наличие на Смоленской АЭС соответствующих структур, обеспечивающих подготовку необходимых специалистов как своими силами, так и в специализированных учебных центрах РФ, компенсирует этот дефицит.

Технические средства защиты информации представлены на рынке широким спектром различного оборудования и ПО, в том числе и отечественного производства, которым отдается предпочтение в первую очередь. Высокая насыщенность рынка позволяет оптимально подбирать необходимые средства защиты с учетом специфики решаемых задач. ●

Обеспечение безопасности в процессе производства электрической и тепловой энергии является приоритетной задачей Смоленской АЭС. Все энергоблоки оснащены системой локализации аварий, исключающей выбросы радиоактивных веществ в окружающую среду. Специальные системы обеспечивают надежный отвод тепла от реакторов даже при полной потере станцией электроснабжения с учетом возможных отказов оборудования.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

А увольнять-то некого!

Ольга Горюнова, *директор департамента по работе с клиентами кадрового агентства "Юнити"*

Затянувшаяся неопределенность на рынке вынуждает бизнес прибегать к сокращениям численности персонала. Выведение из штата наименее эффективных сотрудников — это антикризисная мера, которую выбирает подавляющее большинство компаний. Однако в процессе оптимизации они столкнулись с проблемой выбора: увольнять оказалось некого.

Осторожные сокращения персонала

В нынешней ситуации, в отличие от еще не забытого 2008 г., компании ведут процедуру сокращения более сдержанно. И этому есть объяснение:

- сегодня штаты не раздуты, после стабилизации ситуации компании набирали специалистов только под существующие запросы;
- работодатели в последние годы постоянно углубляли степень оценки кандидатов;
- компании стали больше инвестировать в обучение сотрудников и развитие эффективной команды.

Столкнувшись с необходимостью сокращения, компании встали перед нелегким вопросом: кого увольнять? Выбор стоит между теми, кого долго искали и тщательно отбирали, и теми, кого вырастили и в кого вложили много сил и денег. Чтобы принять решение, компании обычно ориентируются на три фактора.

Доля инженерных вакансий в "Юнити" росла на протяжении всего прошлого года. Поиск высококвалифицированных и узких технических специалистов по сложности для работодателей приблизился к поиску управленцев. Сейчас производственные компании должны принимать решение о сокращении с оглядкой на дефицит. Ведь потом найти другого кандидата будет крайне сложно.

Ситуация в отрасли

Сигналом, определяющим экономическое состояние отрасли, является проектный портфель компании (или объем заказов). По словам экспертов, именно этот фактор необходимо в первую очередь учитывать, выбирая меры по оптимизации. Мониторинг рынка труда показывает, что ситуация стабильнее в тех отраслях, которым государство обещало поддержку. Среди них АПК, пищевая промышленность, тяжелое машиностроение, энергетика. Относительно неплохо чувствуют себя те сферы, в которых уже действовали госпрограммы, например фармацевтика и ИТ-сектор. В этих направлениях сохраняется спрос на редких инженерных специалистов и квалифицированных управленцев. Правда, недавний секвестр госбюджета, вероятно, приведет к сокращению инвестиций в части отраслей.

Но, несмотря на серьезное снижение экономической активности, есть компании, готовые сейчас сделать рывок даже без поддержки со стороны государства.

Оценивая ситуацию в отрасли, необходимо учитывать наличие дефицита персонала, особенно если компания работает в каком-то узком сегменте.

Масштаб бизнеса компании

Кадровым трендом конца прошлого года стал рост доли заказов от ведущих российских компаний. Несмотря на проявления кризиса, они продолжали подбирать персонал. Сейчас крупные игроки, в том числе и госкомпании, обладают значительным "запасом прочности" и в случае затянувшегося кризиса имеют больше шансов на выживание.

Кадровым трендом конца прошлого года стал рост доли заказов от ведущих российских компаний. Несмотря на проявления кризиса, они продолжали подбирать персонал. Сейчас крупные игроки, в том числе и госкомпании, обладают значительным "запасом прочности" и в случае затянувшегося кризиса имеют больше шансов на выживание.

Именно поэтому крупные компании, как правило, идут по более длинному пути оптимизации. Приведем несколько последовательных шагов:

- анализ бизнес-процессов и их оптимизация;
- оценка эффективности работников;
- выведение из штата наименее эффективного персонала (если оценка подтвердит необходимость этой меры);
- замена низкопродуктивных работников на квалифицированных специалистов с рынка;
- сокращение штата и полная загрузка имеющихся специалистов.

Если же компания совсем небольшая, то вопрос оптимизации можно решать более гибко и на индивидуальном уровне.

Одним из способов сокращения расходов в малом бизнесе становится внедрение удаленных способов работы.

Стратегия компании

У всех компаний в кризисное время есть общая кадровая стратегия, связанная с выживанием. Снижение бизнес-активности стабильно повышает спрос на продажников, который стал заметно увеличиваться с середины прошлого года. Сейчас такие вакансии занимают первое место в рейтинге востребованности, и их доля составляет более трети всех предложений. В кризис портфель заказов уменьшается, и редкая компания остается довольна результатами отдела продаж. Даже те работодатели, кото-

Четко сформулированная стратегия, согласованная с менеджерским персоналом компании, должна являться отправной точкой для принятия решений об отсеивании других кандидатов. Ведь именно сотрудникам предстоит решать задачи, в которые и переносится принятая стратегия развития. Поэтому в процессе оптимизации необходимо учитывать, какое количество специалистов понадобится для решения той или иной задачи, а также какими компетенциями они должны обладать.

рые понимают, что обладают профессиональными специалистами, все равно пытаются найти более эффективных. Если у продажника есть недостаток квалификации, то он резко проявляется в снижении объемов. Тогда он становится претендентом номер один на замену.

Тактика отсева других специалистов зависит от индивидуальной стратегии.

Урезание зарплаты как альтернатива увольнению

Определенное высвобождение кадров уже заметно на рынке. Так, по данным hh.ru, в феврале на одну вакансию в среднем приходилось 2,9 резюме не работающих на данный момент соискателей (это более чем в полтора раза больше, чем год назад). Но серьезные сокращения большинство компаний пока старается отложить на крайний случай, пока эти меры носят точечный характер. Прошлый кризис показал, что буквально через 3–6 месяцев после увольнений компаниям пришлось подбирать персонал заново.

Чтобы сохранить коллектив, многие компании идут на корректировки заработной платы. Среди них может быть пропорциональное снижение вознаграждения и рабочего времени или объема работ, а также временное уменьшение зарплаты (это может быть урезание оклада и сохранение переменной части или сохранение оклада и снижение переменной части).

По первому пути чаще идут производственные предприятия, уменьшая количество смен или сокращая рабочий день. Также вынуждены меньше работать и, соответственно, меньше получать все фрилансеры.

В целом по рынку заметно небольшое снижение уровня оплаты труда. С середины прошлого года работодатели во многих сферах были ориентированы на нижнюю планку рыночных зарплат. А почувствовав в этом году наплыв соискателей, стараются еще больше снизить предложение. Кандидаты ощутили конкуренцию и сами умерили свои аппетиты. Среди них – даже наиболее востребованные продажники. Их суммарный доход напрямую зависит от объемов продаж, и, понимая ситуацию, они готовы на его снижение. Имеющимся же сотрудникам нередко ограничивают или убирают переменную часть. Так, в конце прошлого года многие даже крупные компании не стали выплачивать годовые премии.

Чем опасны урезания бюджетов

Работодатели понимают, что серьезное сокращение зарплат в условиях набирающей оборот инфляции – тоже опасный шаг, и стараются его избегать. Это сразу спровоцирует "паломничество" сотрудников – они же понимают, что все это "не от лучшей жизни". А уходить начинают самые лучшие, амбициозные, перспективные. Такие на рынке востребованы и долго без работы не останутся, и они понимают это. Вышеназванные меры приведут к потере важных ресурсов. А если не будет нужного количества сотрудников, то при низкой результативности оставшихся стремительно упадет прибыльность бизнеса, что еще больше усугубит положение.

Однако расчеты между контрагентами все затягиваются, что ведет к недостатку средств, и компании неизбежно приходят к необходимости задерживать выплаты сотрудникам. В этом случае необходимо предупредить персонал и хотя бы ориентировочно обозначить сроки, в которые деньги будут выплачены. Но, безусловно, "игры" с зарплатой могут плохо кончиться для самой компании.

Опыт ИТ-отрасли подтверждает актуальность последнего убеждения, считают рекрутеры. В прошлый кризис ИТ-компании вели активный подбор специалистов, которые высвобождались при сокращении подразделений предприятий. Это, в частности, послужило причиной серьезного дефицита данных специалистов в 2009–2010 гг., когда крупные компании решили наращивать и возрождать внутренние службы.

Сегодня некоторые работодатели снова используют ситуацию, чтобы выбрать с рынка качественных специалистов.

По данным hh.ru*, подобную тактику планируют использовать около 60% компаний, которые сообщили во время опроса, что планируют сохранить штат в нынешнем виде и искать интересных кандидатов. А значит, работодатели, которые вынуждены идти на временные сокращения зарплат и премий, несмотря на ситуацию, серьезно рискуют потерять персонал. Поэтому меры оптимизации должны быть тщательно продуманы, а все изменения должны поддерживаться регулярной коммуникацией с персоналом. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

* *http://hh.ru/article/16191.*

Негативного эффекта стоит опасаться и при задержке зарплаты, которая является одной из наиболее частых причин для смены работы даже в "мирное" время.

По данным hh.ru, в феврале на одну вакансию в среднем приходилось 2,9 резюме не работающих на данный момент соискателей (это более чем в полтора раза больше, чем год назад).

Прошлый кризис показал, что буквально через 3–6 месяцев после увольнений компаниям пришлось подбирать персонал заново.

В целом по рынку заметно небольшое снижение уровня оплаты труда. С середины прошлого года работодатели во многих сферах были ориентированы на нижнюю планку рыночных зарплат. А почувствовав в этом году наплыв соискателей, стараются еще больше снизить предложение.

Современные угрозы для индустриальных сетей и способы борьбы

Андрей Нуйкин, *начальник отдела обеспечения безопасности информационных систем, блок вице-президента по информационной безопасности, ЕВРАЗ*

В сегодняшнем мире индустриальные сети все больше развиваются. Происходит переход на IP-протоколы, индустриальные и корпоративные системы активно обмениваются информацией, что неизбежно ведет к их взаимной интеграции. Управление производством переходит в режим онлайн, а руководству необходимо четко понимать, что сейчас происходит на предприятии, планировать его работу и многое другое.

Такая интеграция несет и новые проблемы для индустриальных сетей, с которыми раньше специалисты по АСУ ТП не сталкивались. Возникают различные новые угрозы, устранять которые иногда весьма затруднительно. Индустриальные сети работают совершенно отлично от корпоративных, и казалось бы простые меры защиты, работающие в одних сетях, не всегда можно применить в других.

Например, установка обновлений в корпоративной среде осуществляется автоматически и практически не вызывает вопросов. В индустриальных же – установка обновления может привести к остановке производственного процесса. И поэтому очень часто специалисты АСУ ТП предпочитают не устанавливать их вовсе.

Проведя простое сканирование на уязвимости, можно обнаружить много интересного: от стандартных логинов и паролей до отсутствующих обновлений операционных систем. Соответственно, проникший вирус или злоумышленник получит гораздо больше возможностей вершить свои "темные дела".

Проведя простое сканирование на уязвимости, можно обнаружить много интересного: от стандартных логинов и паролей до отсутствующих обновлений операционных систем. Соответственно, проникший вирус или злоумышленник получит гораздо больше возможностей вершить свои "темные дела".

Человеческий фактор

В индустриальной сети используется зачастую такое же сетевое оборудование и серверы, как и в корпоративной. Все это оборудование требует обслуживания и настроек. А учитывая, что промышленные цеха могут быть разбросаны по большим территориям и обойти их пешком бывает весьма затруднительно, то системные и сетевые администраторы активно используют удаленный доступ. При этом даже если корпоративная и индустриальная сети разделены, то в настройках межсетевого экрана создаются проходы, чтобы программное обеспечение для удаленного администрирования могло беспрепятственно работать. А учитывая, что администраторы в большинстве случаев находятся в корпоративной сети и со своих компьютеров активно используют Интернет и корпоративную (не только) почту, они являются угрозой для индустриальной сети. Например, злоумышленник, проникнув в корпоративную сеть и выяснив топологию, может скомпрометировать компьютер администратора и воспользоваться им как шлюзом для проникновения в индустриальную.

Компрометация не представляет особых проблем, потому что люди склонны упрощать себе жизнь: используются слабые пароли, совпадающие на большинстве устройств, или системы удаленного управления со слабой защитой. К группе риска относятся также и разработчики. Они аналогично администраторам активно используют удаленные подключения (зачастую напрямую) к контроллерам и серверам управления технологическим оборудованием.

Многие из этих угроз проистекают из того факта, что корпоративные и индустриальные сети часто не имеют четкого разделения. Я сталкивался с различными вариантами раз-

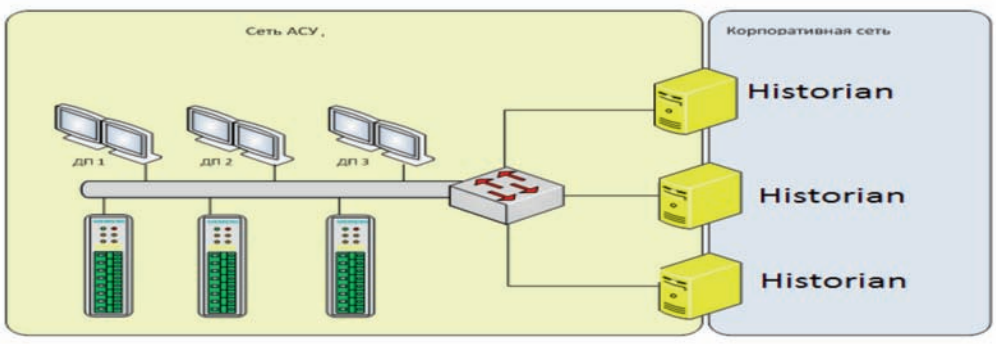


Рис. 1. Станции связи с двумя сетевыми картами

деления сетей: это могли быть некие станции связи с двумя сетевыми картами (рис. 1); есть вариант, когда сети разделены коммутатором и маршрутизатором с настроенными ACL (рис. 2); бывает даже вариант с разделением межсетевым экраном (рис. 3). Но все эти варианты страдают от человеческого фактора, описанного выше.

Как же бороться с такими угрозами?

На этот вопрос дают ответы различные стандарты по обеспечению индустриальных сетей. Все они в один голос утверждают о необходимости разделения сетей. Причем на всех уровнях.

На границе индустриальной сети необходимо строить демилитаризованную зону (ДМЗ), в которую выносятся все сервисы, взаимодействующие с корпоративной сетью. Если есть необходимость, в индустриальной сети должна использоваться своя инфраструктура MS AD, свой сервер антивирусной защиты и т.д.

Для разработки требований к защите индустриальной сети можно использовать требования стандарта PCI DSS, применяемого в банковской среде, так как идеологически они имеют много общего.

Строим типовую ДМЗ

Что для этого нужно? В первую очередь – разделить сети. Для этого используем межсетевые экраны. На их базе организуем ДМЗ и ограничиваем прямое взаимодействие сетей. В индустриальной сети установим серверы MS AD – это позволит отделить авторизацию в каждой из сетей. Далее для обеспечения работы администраторов с оборудованием индустриальной сети поставим в ДМЗ сервер VDI, чтобы каждый администратор получил вторую рабочую станцию для работы в этой сети.

На VDI-рабочих станциях они будут авторизоваться с использованием учетных записей из AD. Соответственно, компрометация корпоративной учетной записи администратора не приведет к автоматическому получению доступа в индустриальную сеть. А для повышения уровня безопасности введем еще и двухфакторную аутентификацию по одноразовым паролям.

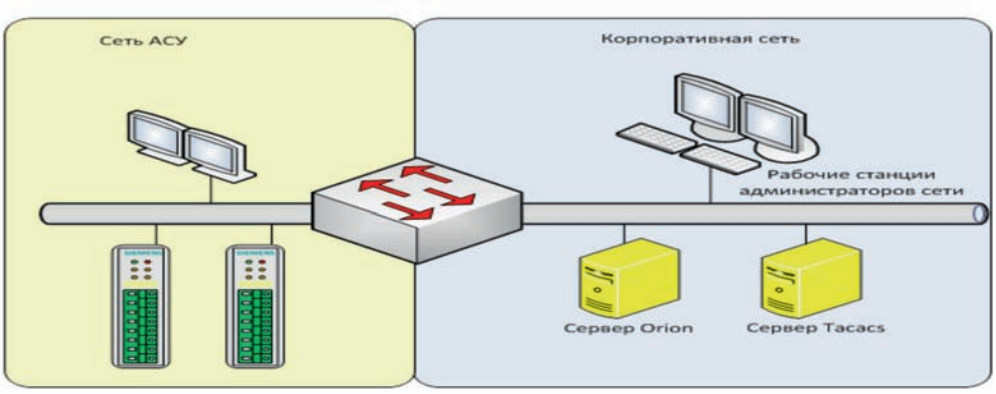


Рис. 2. Сети, разделенные коммутатором или маршрутизатором с настроенными ACL

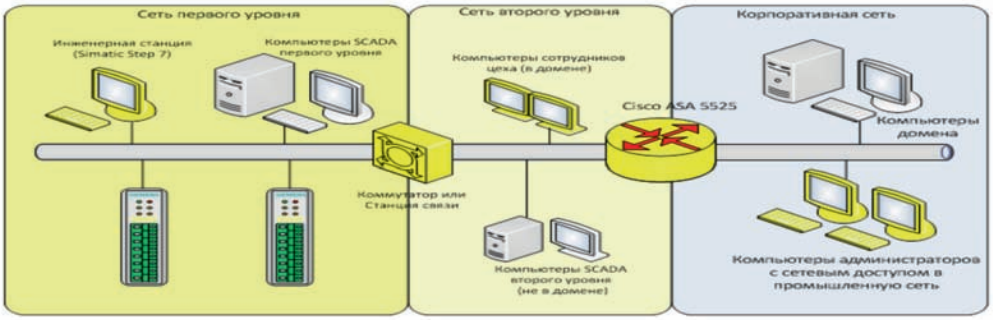


Рис. 3. Сети, разделенные межсетевым экраном

Вы спросите: "Почему по одноразовым?". На мой взгляд, если использовать, скажем, USB-токен, то сработает человеческий фактор: токен будет вставлен в порт и оставлен там навсегда. А одноразовый пароль меняется с определенным интервалом, так что даже в случае перехвата второй раз им уже не воспользуешься. Далее в ДМЗ выносим сервер антивирусной защиты. И на межсетевом экране обеспечиваем одностороннюю связь с корпоративным сервером обновлений, который также выносим. Это позволит нам получать обновления, при этом входящие подключения будут запрещены. Аналогично поступаем и со всеми другими сервисами типа Historian и т.д.

Если промышленных площадок много, то есть вариант создания централизованной ДМЗ. В данном случае на уровне ЦОДа формируется одна ДМЗ для всех площадок. В нее мы выносим единые для всех сервисы. Например, серверы MS AD, антивируса, обновления, двухфакторной аутентификации и т.д. На уровне площадок устанавливаются межсетевые экраны, обеспечивающие создание VPN-туннеля до центральной ДМЗ. При этом остается возможность создания локальных ДМЗ для серверов и сервисов, которые по каким-либо причинам не могут быть вынесены в центральную. Таким образом, возможна экономия на серверах для MS AD, антивируса и т.д.

Организовав такую ДМЗ, мы сможем значительно снизить угрозы, связанные с компрометацией учетных записей администраторов и разработчиков, затруднив распространение вирусов. В идеале мы получим самодостаточную индустриальную сеть, минимально зависящую от корпоративной. Хотя, на мой взгляд, в современном производстве этот идеал практически недостижим, т.к. в корпоративных системах зачастую формируются данные, необходимые для работы индустриальной сети. Например, различные паспорта или сертификаты на произведенную продукцию. Не имея такого сертификата, продукция не может быть передана заказчику. Что также является угрозой. Но это отдельная история. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Компрометация не представляет особых проблем, потому что люди склонны упрощать себе жизнь.

Компрометация корпоративной учетной записи администратора не приведет к автоматическому получению доступа в индустриальную сеть. А для повышения уровня безопасности введем еще и двухфакторную аутентификацию по одноразовым паролям.

Методы борьбы с киберугрозами АСУ ТП современного предприятия

Алексей Полетыкин, *Институт проблем управления им. В.А. Трапезникова РАН, г. Москва*
Виталий Промыслов, *Институт проблем управления им. В.А. Трапезникова РАН, г. Москва*

В работе приводятся сведения о результатах теоретических и прикладных исследований ИПУ РАН в области защиты от киберугроз современных промышленных предприятий: метод определения возможного ущерба, методика расчета и управления рисками, предложения по созданию автоматизированных систем внешнего сопровождения на этапах жизненного цикла, использование формальных моделей.
Данная статья призвана ознакомить инженеров и специалистов по защите информации с некоторыми результатами этих исследований.

Необходимость защиты АСУ ТП от киберугроз декларируется во многих нормативных документах, принятых в России и за рубежом. В РФ рабочим документом является Приказ ФСТЭК 31 [3], в котором приводятся правила оценки рисков, исходя из возможной тяжести ущерба, а для их парирования предлагается дифференцированный комплекс мер.

Для исполнения приказа требуется уметь решать две основные задачи:

1. Определять возможный ущерб от кибератаки на АСУ ТП для каждого из его компонентов.
2. Применять меры по защите в соответствии с присвоенным компоненту уровнем информационной безопасности.

Для решения первой задачи предлагается использовать подход, основанный на понятиях штатных и скрытых функций, которые были введены в теории киберустойчивости [4].

Процесс применения мер по защите предлагается реализовывать с помощью автоматизированных средств внешнего сопровождения (АСВС) [5].

Приказ [3] не носит обязательного характера. Это объяснимо, поскольку применение мер защиты для существующих систем может быть невозможным. В этом случае необходимо производить анализ угроз и оценку рисков индивидуально, учитывая источники угроз, уязвимости и возможные виды и тяжесть ущербов от кибератак. Для этого предлагается использовать методику оценки и управления рисками, основанную на анализе физических, информационных и иных барьеров, препятствующих кибератакам [6].

Независимо от того, как были выбраны и реализованы меры для функции ИБ, необходимо уметь доказывать их достаточность для противодействия киберугрозам и непротиворечивость со штатными функциями управления. Для этого предлагается применять формальные модели и основанные на них методы компьютерного моделирования [7, 8].

Определение возможного ущерба

С точки зрения разработчиков-технологов АСУ ТП служит для достижения четко выраженных единичных или множественных целей и выполняет определенные штатные функции, и их нарушение может привести к материальному ущербу. И защищать от киберугроз нужно именно эти функции. Это отличается от понимания специалистов по информационной безопасности (ИБ), которые чаще всего целью считают защиту конфиденциальности, целостности и доступности информации, содержащейся в вычислительных комплексах (пример 1).

Второй источник взаимного непонимания специалистов по АСУ ТП и специалистов по защите информации лежит в области понятия "отказ". Специалисты по АСУ ТП под этим понимают то, что штатные функции перестают выполняться, возможно, частично. Специалисты по ИБ пользуются понятием "вторжение", при котором АСУ ТП изменяет алгоритм работы, что может привести или не привести к изменениям выполняемых штатных функций, а может и привести к появлению новых, возможно, вредоносных функций (пример 2).

Для того, чтобы перейти к предмету раздела, расчета ущербов от кибератак на АСУ ТП, введем понятие скрытых функций, под которыми будем понимать те, что не входят в перечень штатных функций, но могут выполняться в силу физических особенностей объекта управления и наличия возможности внесения изменений в программно-технические комплексы АСУ ТП.

С учетом введенных понятий расчет возможного ущерба может проводиться по следующему алгоритму:

- составить перечень штатных функций;
- оценить возможный ущерб объекту управления от отказов каждой из них;

Пример 1

Для специалиста по защите информации полное уничтожение всей информации с последующим восстановлением из эталонной копии вряд ли покажется приемлемым. Однако для АСУ ТП это вполне приемлемый способ радикально избавиться от подозрений о вторжении.

● составить перечень скрытых функций;
● оценить возможный ущерб от активизации каждой из них;
● вычислить максимум из величин ущербов.

Составление перечней штатных и скрытых функций и оценка ущерба от нарушений каждой из них является сложной задачей, решение которой лежит целиком в зоне компетенций создателей объекта управления: проектантов, технологов, конструкторов технологического оборудования и АСУ ТП, экономистов, юристов и др. (пример 3).

Обеспечение кибербезопасности на различных этапах жизненного цикла (ЖЦ) АСУ ТП с использованием АСВС

Предположим, что возможные ущербы от кибератак оценены, и необходимо приступать к работе по внедрению мер, указанных в [3], по полному ЖЦ: технические требования, проектирование, изготовление, монтаж, наладка и эксплуатация. Какие для этого есть ресурсы? Методические материалы крайне скудные, специалистов с опытом работы почти нет. Насчет технического оснащения ситуация лучше: можно применять устройства и решения, опробованные в спец. системах, банках и т.п. Но, опять-таки, условия работы АСУ ТП иные, и опыт можно применять только выборочно.

ИБ АСУ ТП является типичным представителем областей, где обычные методы организации работы практически не применимы из-за ограниченности человеческих и методических ресурсов. Для этого предлагается использовать сетевые технологии, позволяющие концентрировать усилия экспертов с разной специализацией для решения сложных задач. Данный вид систем, АСВС, описан в [5], где приводится также пример применения для целей обеспечения ИБ.

Как средство автоматизации, АСВС может иметь целями достижение требуемых показателей по ИБ объекта на всех этапах ЖЦ.

Основными функциями АСВС на всех этапах ЖЦ являются:
● организация разработки, согласования и поддержки документов;

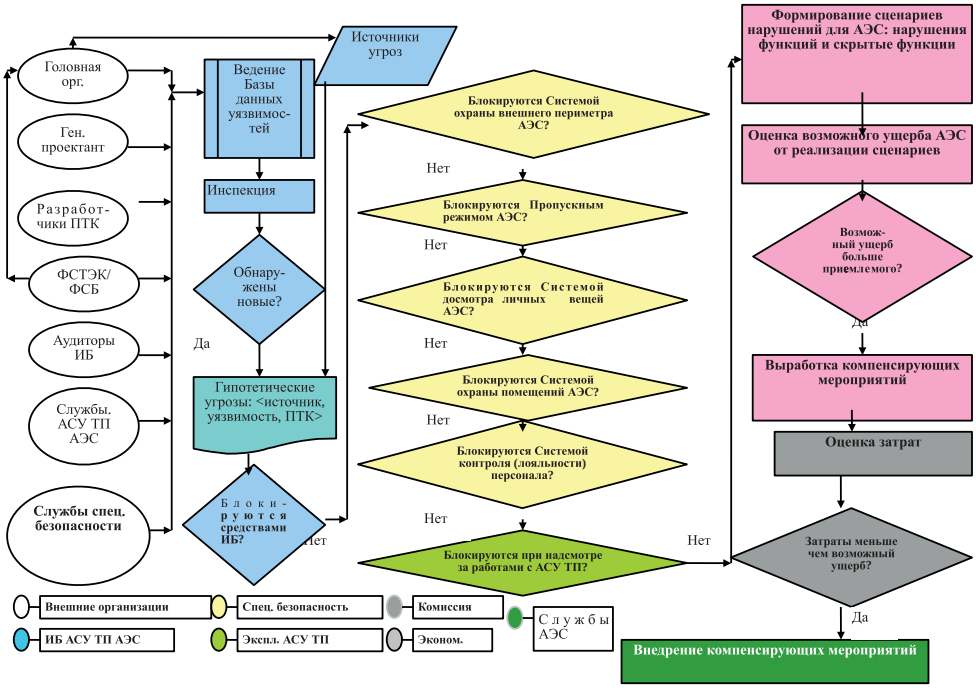


Рис. 1. Управление риском ИБ в АСУ ТП АЭС

● организация и поддержка работы целевых экспертных групп для решения проблем.

Основными специфическими задачами АСВС на этапе эксплуатации являются:
● периодический или инициированный операторами мониторинг и прогнозирование состояния объекта управления;
● классификация, установление причин инцидентов;
● прогноз состояния объекта управления вследствие действия причин инцидентов;
● выработка управляющих решений;
● мониторинг реализации управляющих решений.

Вспомогательными задачами АСВС являются:
● ведение базы данных о состоянии объекта управления;
● ведение базы данных инцидентов;
● создание, поддержание и расширение базы знаний о причинах, протекании, эффективности мер по противодействию инцидентов на основе автоматического, автоматизированного и экспертного анализа научно-технической литературы (данные об испытаниях, статьи и т.д.);
● ведение базы данных экспертов;
● организация интерсубъектного взаимодействия экспертов, собственных и внешних баз знаний и данных;
● организация удаленного взаимодействия через персонал и напрямую с компьютерными моделями объекта (при наличии и доступности).

Целью АСВС на этапе проектирования/конструирования является обеспечение качества документов, на этапе изготовления/испытаний – разработка способов тестирования на вторжения и др., на этапе эксплуатации – сохранение основных штатных и недопущение активизации вредоносных скрытых функций путем удаленного аудита, анализа инцидентов, консультирования и т.д.

Корневой алгоритм решения задач в АСВС представляет собой типовую последовательность действий, характерную для решения задач (подзадач) группами экспертов:
а) идентификация проблемы;
б) постановка задачи;
в) назначение ответственного (ведущего ЭГ);
г) решение задачи ведущим с использованием баз данных/знаний, пакетов прикладных программ или с привлечением экспертов-представителей компетентных организаций, в последнем случае:
● выбор ведущим ЭГ состава экспертов и метода работы с экспертами;
● составление ведущим с участием экспертов информационной базы;
● обсуждение проблемы в группе;
● подготовка решения ведущим или автоматическим алгоритмом;

Пример 2

Допустим, в АСУ ТП обнаружен вирус, который собирает информацию, но не влияет на работу.
С точки зрения специалистов по АСУ ТП никакого инцидента не произошло, и ничего предпринимать не нужно. Для специалистов по ИБ инцидент с вторжением налицо, и нужно применять меры. Мнение специалистов по АСУ ТП изменится, если будет установлено, что вирус способен выдавать ложные команды управления. Это показывает, что оценивать нужно не сам факт появления новых функций в АСУ ТП, а их возможный ущерб для объекта управления.

Рис. 2. Применение ФМ для ИБ

Пример 3

Приведем пример. Рассмотрим АСУ для управления сотовой связью. Штатными функциями для нее являются обеспечение телефонной связи, CMS, Интернет. Отказ этих штатных функций вызовет неудобство, но не аварию. Перечень скрытых функций не так прост. Приведем только одну: организация массовых сообщений о начале катастрофы, войны и т.п..Если ввести эту функцию в действие, то последствия могут быть гораздо серьезнее. Поэтому, АСУ ТП сотового оператора нужно присвоить не 3-й, а 2-й класс согласно приказу [3].

● согласование и утверждение решения экспертами.

Процесс решения задач в АСВС выглядит как выполнение корневого алгоритма один и более раз. Если исходная задача разбивается на независимые подзадачи, то корневой алгоритм может выполняться параллельно для всех подзадач. Могут быть случаи, когда задача может быть решена итеративным способом, при котором решения, полученные применением корневого алгоритма, затем используются для уточнения постановки задачи на последующих итерациях. Могут быть и смешанные случаи, когда часть итераций может быть выполнена параллельно.

Методика оценки управления рисками ИБ

ИБ АСУ ТП можно с достаточной степенью общности понимать как систему дополнительных барьеров, которые действуют совместно с другими (защитой труда, физической, технологической и др.) для того, чтобы исключить риски неприемлемых ущербов объекту управления. При этом барьеры

ИБ ориентированы на специфические сценарии умышленного или злонамеренного нанесения вреда: через отказы штатных и активизацию скрытых функций.

На рис. 1 представлена упрощенная блок-схема алгоритма расчета рисков на примере АСУ ТП АЭС, более подробно описанная в [6].

Формальные модели (ФМ)

Проведенные исследования ФМ на основе мультиграфов показали, что с их помощью можно эффективно описывать политику ИБ [7] (см. рис. 2). Это позволяет осуществить проектирование АСУ ТП с заданными характеристиками ИБ и обеспечить гарантии выполнения требований ИБ на последующих этапах ЖЦ.

На основе ФМ в ИПУ РАН разрабатывается программный сервис для моделирования, в частности, иерархической структуры и отношений доступа в АСУ ТП, пути распространения прав доступа [8].

Заключение

Главное отличие и источник сложностей ИБ АСУ ТП состоит в "междисциплинарности" и слабой формализованности проблемы, и для ее обеспечения необходимо вовлекать технических специалистов разной квалификации, которые имеют разные ценностные ориентиры, входят в разные организационные структуры, говорят на разных языках и не привыкли работать в единых командах.

ИПУ РАН планирует продолжать теоретические работы в данной области ИБ (см. www31.ipu.rssi.ru) и создавать новые аналитические продукты (см. пример прототип сервиса моделирования на основе ФМ [8]).

Литература

1. Менгазетдинов Н.Э. Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУ ТП для АЭС "Бушер" на основе отечественных информационных технологий / Н.Э. Менгазетдинов, М.Е. Бывайков, М.А. Зуенков, В.Г. Промыслов, А.Г. Полетыкин, В.Н. Прокофьев, И.Р. Коган, А.С. Коршунов, М.Е. Фельдман, В.А. Кольцов [Электронный ресурс]: монография. – М.: ИПУ РАН, 2013.

2. Промыслов В.Г., Полетыкин А.Г., Менгазетдинов Н.Э. Новые кибернетические угрозы и методы обеспечения кибербезопасности в цифровых системах управления // Энергетик. – 2012. – № 7. – С. 18–23.

3. Приказ ФСТЭК России 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".

4. Полетыкин А.Г. Критерии устойчивости объектов с цифровыми системами управления к воздействиям кибератак на основе анализа штатных и скрытых функций / Материалы Седьмой международной конференции "Управление развитием крупномасштабных систем (MLSD'2013)". – М.: ИПУ РАН, 2013. – Т. 1. – С. 104–105.

5. Полетыкин А.Г. Автоматизированные системы внешнего сопровождения и пример применения для обеспечения кибербезопасности / Труды восьмой международной конференции "Управление развитием крупномасштабных систем MLSD'2015". – М.: ИПУ РАН, 29 сентября – 1 октября 2015 г. – Т. 2. – С. 123–129.

6. Полетыкин А.Г. Формализованный метод оценки и управления рисками для обеспечения кибербезопасности больших систем управления / Материалы восьмой международной конференции "Управление развитием крупномасштабных систем MLSD'2015". – М.: ИПУ РАН, 29 сентября – 1 октября 2015 г. – Т. 1, Пленарные доклады. – С. 123–129.

7. Промыслов В.Г., Полетыкин А.Г. Формальная иерархическая модель безопасности верхнего уровня АСУ ТП АЭС // Ядерные измерительно-информационные технологии. – 2012. – Т. 4 (44). – С. 39–53.

8. Сервис моделирования кибербезопасности CybersMod [online]. Доступ через http://193.232.208.45/. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Эволюция индустриальной кибербезопасности

Построение интеллектуальных систем обеспечения защиты АСУ ТП промышленных предприятий

2015 год стал временем массовых аудитов безопасности систем АСУ ТП. Статистика инцидентов также впечатляет. Специалисты ISC-CERT зафиксировали 108 кибератак в первой половине 2015 года. Треть эпизодов пришлась на энергетику, 20% были направлены на компании в области водоснабжения, другие 20% – на критически важные предприятия. В Chatham House сообщали о 50 киберпреступлениях против АЭС, в Dell – о двукратном росте атак на SCADA за год.

В 2016 г. предприятиям требуется решение, способное снизить риск системных сбоев и техногенных катастроф, связанных с кибератаками. Чтобы ответить на эти вызовы, был задействован весь потенциал компании Positive Technologies. Наши специалисты выявили свыше 250 уязвимостей нулевого дня в системах АСУ, и это самый высокий показатель по отрасли.

Воздушный зазор

На предприятии часто придерживаются консервативной точки зрения: лучший файрвол – это "воздушный зазор". Нет подключения технологических сегментов к Интернету – значит, отсутствует и опасность. Не надо тратить силы на исправление уязвимостей и подвергать производственный процесс риску остановки.

Так ли все просто? "Изолированность" АСУ ТП не случайно называют мифом. На объектах с несколькими сотнями сотрудников неизбежно возникают паразитные каналы в результате воздействия человеческого фактора и конвергенции различных систем. Забытый Web-интерфейс для общения с подрядчиком, IP-камера или роутер в поисковой выдаче Shodan, подключенный к АРМ смартфон диспетчера. Множество проблем безопасности несет и интеграция с АСУ ТП систем ERP и MES, которые помогают снизить затраты предприятий и оперативно планировать производственный цикл.

Потребность в идеях

Часть крупнейших вендоров по сетевой безопасности уже представили решения для промышленного сектора. Большинство средств заимствуют опыт из корпоративной среды, добавляют поддержку протоколов, но не всегда учитывают сценарии использования. Например, часть из этих продуктов неинформативна даже для инженеров, не говоря уже об операторах, которым может понадобиться быстро принимать решения без согласования с отделом ИБ. Другие решения не защищают от распределенных во времени атак, а значит, пропускают все APT-атаки.

Принцип работы PT ISIM

При выявлении уязвимостей и хакерских атак на промышленную сеть предприятия PT ISIM не влияет на технологический процесс, на сеть и оборудование клиента, поскольку подключается однонаправленным способом. Это гарантирует передачу данных только в одну сторону – от сети АСУ к системе управления инцидентами.

Система собирает и анализирует копию сетевого трафика, выделяя события безопасности и выявляя их взаимосвязи (корреляции). Если ряд событий является шагами потенциальной хакерской атаки, PT ISIM объединит их и представит в виде наглядной цепочки.

Кроме того, система визуализирует атаки на топологии сети и на схеме промышленного оборудования. Сохраненная копия трафика позволяет в любой момент провести ретроспективный анализ и расследование инцидента.

PT ISIM помогает бороться с различными угрозами безопасности, включая несанкционированное подключение, подбор пароля, неправомерные управляющие команды, подмену прошивки промышленного оборудования. Система выявляет и внутренние угрозы – потенциально опасные действия персонала, ошибки конфигурации и др.

Знакомьтесь: PT ISIM

Система управления инцидентами Positive Technologies Industrial Security Incident Manager призвана вывести индустриальную безопасность на новый уровень.
В отличие от других решений PT ISIM визуализирует развитие атаки на сетевой и технологической карте предприятия, а также в виде цепочек атак. Благодаря этому наши клиенты успевают обнаружить действия злоумышленника и вмешаться до того, как будет нарушен технологический процесс, нанесен невосполнимый ущерб оборудованию или появится опасность физического вреда людям.
PT ISIM записывает копию всего сетевого трафика, что позволяет в любой момент проводить ретроспективный анализ и расследовать инциденты в случае подозрения на взлом или заражение. Прерывать технологический процесс ради сбора и анализа данных недопустимо, и PT ISIM дает возможность скопировать запись без остановки системы.

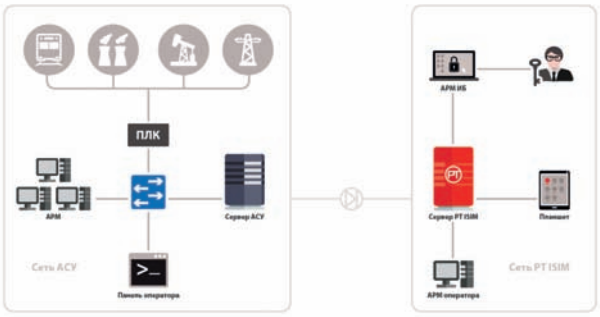


Схема внедрения PT ISIM: без влияния на технологический процесс

В начале 2016 год одна из трех крупнейших транспортных компаний мира выбрала PT ISIM для повышения уровня безопасности движения поездов, что подтверждает эффективность заложенных в продукт механизмов. В настоящее время, помимо транспортной отрасли, PT ISIM может быть внедрен на нефтедобывающих предприятиях и в энергетике. ●

Российские регуляторы проделали значительную работу по актуализации требований к защите промышленных систем: приказ ФСТЭК № 31, законопроект по безопасности критических информационных инфраструктур. Дело за разработчиками.

**На правах рекламы*

NM ●
АДРЕСА И ТЕЛЕФОНЫ КОМПАНИИ POSITIVE TECHNOLOGIES
см. стр. 56

Безопасность промышленных систем управления

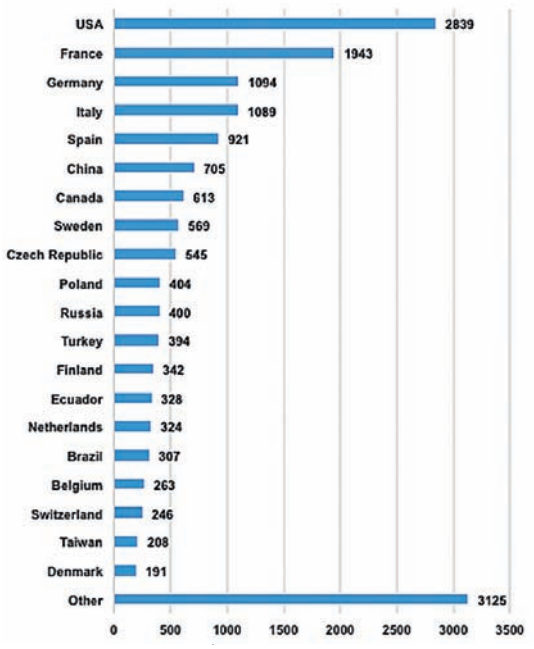
Алексей Андреев, *технический маркетинг, компания Positive Technologies*

Статьи о безопасности принято начинать со "страшилок". Защита промышленных систем управления не исключение: вы обязательно прочитаете в них про Stuxnet или сталелитейный завод в Германии, которому нанесен огромный ущерб в результате хакерской атаки. К сожалению, за перечислением фактов не всегда следует анализ причин подобной ситуации. Попробуем разобраться, чего же не хватает в защите АСУ ТП.

Три кита атаки

Среди тенденций, которые мы наблюдаем последние два года в процессе работ по анализу защищенности промышленных систем управления, можно отметить три базовые проблемы.

1. Неосознанная открытость. Ко многим системам – особенно это касается систем автоматизации зданий – можно легко получить доступ через Интернет. На январь 2015 г. исследователи* обнаружили таким образом более 140 000 доступных АСУ ТП компонент. Примерно каждая десятая – уязвима (см. рис.).



Распределение уязвимых компонент АСУ ТП по странам. Из исследования "Уязвимости промышленных систем управления в 2014 году"

При этом отсутствие прямого подключения к Интернету уже не спасает: хакеры используют многоступенчатые схемы таргетированных атак. Так, троян Havex в 2014 г. распространялся через сайты производителей ПО: зараженные дистрибутивы устанавливались на предприятиях, что позволило злоумышленникам собирать данные из систем управления ряда крупных компаний Европы. В ходе тестов мы нередко обнаруживаем возможности для атак на АСУ ТП через различные сенсоры, физические порты, промышленный Wi-Fi, смартфоны сотрудников и др. виды доступа, которые зачастую вообще не рассматриваются как угрозы.

2. Медленное реагирование. Требование непрерывности технологических процессов приводит к тому, что базовые компоненты систем управления (промышленные протоколы управления, ОС, СУБД) устаревают, но не обновляются, так что даже известные уязвимости не устраняются годами.

С другой стороны, автоматизация значительно упрощает работу хакеров.

3. Методология безопасности далека от практики. Нет даже согласованного определения базовых понятий: что является объектом защиты и в чем состоит безопасность. Для создания средств защиты АСУ ТП используются устаревшие модели угроз, которые не учитывают возросшее влияние "кибернетической" составляющей.

К чему это ведет? Многие уязвимости АСУ ТП позволяют злоумышленникам не только обходить механизмы функциональной безопасности, снижая эффективность производства, но и проводить атаки, которые напрямую влияют на промышленную безопасность – могут стать причиной техногенных катастроф. При этом исследованные системы зачастую соответствуют стандартам функциональной и промышленной безопасности, имеют необходимые международные и государственные сертификаты.

С другой стороны, классические подходы ИБ не всегда стыкуются с практикой промышленной безопасности: здесь и специфические протоколы АСУ ТП, и требование функционирования систем в неблагоприятных физических условиях, и мн.др. особенности, которые характерны для конкретной отрасли или для отдельной системы.

Что делать: не только ИБ

С учетом выше описанных проблем возникает целый ряд специфических требований к средствам защиты АСУ ТП. Выделим только самые базовые:

1. Максимально глубокий анализ уязвимостей, характерных для различных компонент АСУ ТП.

2. Возможность выявления многоступенчатых таргетированных атак: корреляционный анализ событий безопасности, разнесенных во времени и пространстве.

3. Удобное представление результатов не только для экспертов по безопасности (инциденты, цепочки атак), но и для специалистов в области автоматизации, например визуализация угроз на схеме промышленного оборудования.

4. Учет специфики промышленного сектора и используемых компонент АСУ ТП в конкретной индустрии, включая невмешательство системы безопасности в бизнес-процессы.

Конечно, это слишком общая теория. Поэтому напоследок стоит сказать о таком важнейшем условии, как практическое сотрудничество разработчиков АСУ ТП и разработчиков средств защиты. Такая разработка "снизу вверх" уже не является продуктом ИБ в чистом виде, а представляет собой результат новой гибридной дисциплины – кибербезопасности АСУ ТП. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

* *Исследование Positive Technologies "Уязвимости промышленных систем управления в 2014 году" (habrahabr.ru/company/pt/blog/258039/).*

ИБ АСУ ТП: тайна начала проекта

Даниил Тамеев, *руководитель направления по работе с ПиТЭК Центра информационной безопасности компании "Инфосистемы Джет"*

Популярность темы обеспечения информационной безопасности промышленных предприятий набирает обороты с каждым днем. Почти каждый уважающий себя отечественный производитель средств защиты (по крайней мере из числа крупных игроков рынка) уже успел так или иначе заявить свое участие в ней: кто-то адаптирует уже существующие решения, кто-то создает новые, кто-то комбинирует чужие и заявляет об их полной оптимизации под специфику промышленной ИБ.

Тем не менее, несмотря на уже ставшую понятной рынку актуальность проблемы, одним из ключевых вопросов на конференциях и других профильных мероприятиях (да и просто в беседах специалистов между собой) остается причина старта проектов ИБ АСУ ТП в промышленных компаниях. Казалось бы, тема актуальная, и защищать технологический сегмент, безусловно, надо. Но в каждой компании, подошедшей вплотную к решению этой задачи, история возникновения такого интереса очень индивидуальна.

Закон не писан

Зная особенности нашего менталитета, логичным является предположение о том, что основным драйвером должны являться регуляторы. Однако, к сожалению, на текущий момент законодательная база так и не пополнилась соответствующими требованиями по безопасности КВО – мы все ждем вступления в силу соответствующего законопроекта с начала 2014 г. Помимо этого, еще в середине 2015 г. представителями ФСТЭК были озвучены планы по разработке четырех новых документов в дополнение к 31-му приказу, которые должны внести большую конкретику. Что ж, год только наступил, и нам пока остается ждать. Тем временем многие компании мотивируют нежелание заниматься проблемами ИБ своих промышленных объектов именно отсутствием жестких требований со стороны государства.

Проект на опережение

Единичные компании запустили проекты по ИБ АСУ ТП, основываясь на серьезной озабоченности рисками, которые несет в себе угроза атак со стороны "хактивистов" и конкурентов. Основным опасением является размер ущерба, который может понести компания при атаке даже со стороны слабо подготовленного специалиста по взлому. Как показывает практика, квалифицированному хакеру достаточно непродолжительного времени, чтоб разобраться в основах специфики промышленных сетей и решений, чтоб получить нелегитимный доступ к слабозащищенной инфраструктуре предприятия и нарушить его работоспособность. Ломать – не строить.

А мы чем хуже?..

Однако чаще всего от представителей компаний можно услышать, что инициатива старта проекта пошла от топ-менеджмента компании, почувствовавшего модные веяния на тему ИБ промышленности на различных западных конгрессах либо тенденции к повышенному вниманию со стороны руководства страны. И на основании этого проекты действительно стартуют! Представителям служб ИБ приходится разбираться с незнакомой до этого спецификой промышленного сегмента предприятия – многие ранее занимались только "корпоративной" безопасностью. Налаживаются контакты между службами ИБ, ИТ и тех. эксплуатации – именно из них формируется, как правило, рабочая группа по проекту.

Вывод

Безусловно, то, что от теоретических разговоров об информационной безопасности промышленности компании начинают переходить к реальным делам, – уже положительный результат. Даже несмотря на своеобразность причин. Стоит отметить, что проекты по данному направлению почти всегда проходят сложно, долго и дорого. К сожалению, многие компании, даже при соответствующем желании со стороны специалистов службы ИБ, еще не могут себе позволить выделить существенные средства, требуемые для решения данной задачи. А топ-менеджменту в большинстве случаев пока все еще сложно доказать, что сценарии популярных фантастических фильмов про крах компаний, городов и целых стран по вине одного хакера уже стали суровой реальностью. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Защита АСУ ТП
Прежде чем что-то внедрять

Дмитрий Даренский, *начальник отдела промышленных систем департамента комплексных решений компании "Информзащита"*

В течение 2015 г. наблюдался рост количества проектов, каким-либо образом связанных с обеспечением кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП). Подобные проекты стартовали практически во всех отраслях промышленности.

Тем не менее, говорить о том, что тема кибербезопасности АСУ ТП активно развивается в нашей стране, пока рано. Она активно обсуждается на всевозможных форумах, крупные компании-разработчики периодически объявляют о релизах специализированных продуктов для обеспечения безопасности АСУ ТП. Но реальные проекты стартуют с большими сложностями. Отдельные проекты готовились в течение полутора–двух лет и практически сразу после старта признавались провальными. Результаты же успешных проектов нигде не опубликованы. В основном из-за того, что никто не хочет предавать огласке те проблемы, которые вскрываются в рамках обследований и аудитов.

Специалисты компании "Информзащита" попытались обобщить весь спектр доводов "за" и "против", которые высказывались как владельцами АСУ ТП, так и производителями решений в области автоматизации и информационной безопасности.

Аргументы "против"

- АСУ ТП имеют высокие показатели функциональной надежности.
- АСУ ТП строят в отказоустойчивых конфигурациях.
- Параллельно строятся системы противоаварийной автоматики.
- Предусматривается возможность перехода на ручные режимы управления.
- АСУ ТП принято физически отделять от корпоративных сетей и систем.
- Уровень компетенций и производственной дисциплины в подразделениях АСУ выше.
- Критически важные объекты оснащены системами физической защиты (защита периметра, видеонаблюдение, охранная сигнализация, контроль доступа персонала и т.д.).
- Деструктивное воздействие извне трудно реализовать ввиду сложности самого технологического процесса и систем управления.
- Наличие уязвимостей не говорит о том, что есть возможность их эксплуатации.
- Раньше инцидентов ИБ в АСУ ТП не было, с какой стати им появиться сейчас?
- Руководству предприятия обычно сложно доказать, что функционирующая без сбоев система или предприятие действительно уязвимы, и еще сложнее обосновать стоимость возможного ущерба при инцидентах.
- Сложно доказать эффективность инвестиций в ИБ АСУ ТП.

Основные аргументы "за"

- Согласно отчету ICS-SERT, в 2015 г. из 295 инцидентов ИБ в АСУ ТП в 12% атак зафиксировано проникновение в технологические сети систем управления производством.
- Регуляторы и МВД уже ведут проверки объектов на предмет соответствия требованиям нормативно-правовой базе.
- Основной тип нарушителя – внутренний, а не внешний, поэтому реализованные на предприятии меры защиты периметра систем бесполезны.
- Микропроцессорные системы защиты и контроллеры АСУ ТП взламываются за несколько часов.
- Основной объем компонентов – иностранного производства, и большинство не сертифицированы по требованиям защиты информации (например, на НДВ).
- Встроенные механизмы защиты компонентов либо слабо реализованы, либо не используются на местах.
- Контроль качества проектирования АСУ ТП в части разработки решений ИБ не ведется либо ведется формально.
- Фактическая реализация АСУ ТП и физическая защита объекта сильно отличаются от проектных решений и защиту от информационного воздействия не обеспечивают.
- Решения для защиты систем от производителей компонентов АСУ ТП, как правило, не закупаются в целях экономии бюджетов либо не реализуются в целях упрощения эксплуатации системы.

Приведен далеко не полный перечень аргументов. При этом есть определенная закономерность в обеих группах аргументов. Аргументы "против" ориентированы в основном на более глубокое понимание функциональных и технических возможностей АСУ ТП. Но аргументы "за" основаны прежде всего на опыте исследований компонентов систем и имеющейся сегодня (хотя и не такой большой) статистике по инцидентам в АСУ ТП различных отраслей, а также результатах аудитов систем, которые, в свою очередь, показывают реальную ситуацию с безопасностью на реальных объектах.

Проектный опыт компании "Информзащита" показывает, что, несмотря на заверения специалистов в области автоматизации об устойчивости и надежности их систем, повышение уровня защищенности от киберугроз АСУ ТП большинства предприятий во всех ключевых отраслях промышленности сегодня является уже необходимостью, а не просто "распиаренным трендом". ●

Многие компании в настоящий момент данную тему "поставили на паузу". Причина в большинстве случаев одна – отсутствие понимания необходимости защиты своих АСУ ТП. И это понятно, аргументы как "за", так и "против" довольно весомые.

NM
АДРЕСА И ТЕЛЕФОНЫ ЗАО НИП "ИНФОРМЗАЩИТА" см. стр. 56

Актуальные вопросы защиты АСУ ТП

С каждым днем количество угроз и атак киберпреступников увеличивается. Страшно представить, что доступ к крайне сложным технологическим системам, чей выход из строя может привести к ужасным последствиям вплоть до экологической катастрофы, может попасть в руки "не тем" людям. Поэтому обеспечение информационной безопасности критически важных объектов является приоритетной задачей. Какие средства защиты используются сегодня на объектах критически важной инфраструктуры и как не допустить несанкционированного проникновения в системы предприятий, редакция узнала у экспертов:

Евгений Генгринович, *советник генерального директора ПАО "International IT Distribution"*

Дмитрий Даренский, *главный архитектор департамента комплексных решений компании "Информзащита"*

Егор Литвинов, *ведущий исследователь департамента безопасности АСУ ТП, Digital Security*

Алексей Полетыкин, *заместитель руководителя проектов, Институт проблем управления им. В.А. Трапезникова РАН, д.т.н.*

Даниил Тамеев, *руководитель направления по работе с ПиТЭК Центра информационной безопасности компании "Инфосистемы Джет"*

Антон Шипулин, *руководитель проектов по информационной безопасности компании "КРОК"*

– В чем заключается специфика задач защиты АСУ ТП и чем она обусловлена?

Евгений Генгринович

АСУ ТП сама выполняет роль обеспечения безопасности производственного процесса. Обычно любые задержки в ее работе могут отрицательно сказаться на самом производственном процессе. Уровень ответственности решаемых задач таков, что допустить вмешательство в свою работу внешних систем (например, систем информационной безопасности) не представляется возможным. С другой стороны, в АСУ ТП проникли и заняли достойное место стандартные IP-устройства, данные АСУ ТП используются множеством различных IP-систем, и количество информационных угроз растет в геометрической прогрессии.

Дмитрий Даренский

Специфичных моментов много. Начиная с того, что АСУ ТП – это не ИТ-система в стандартном понимании, и заканчивая пониманием степени критичности АСУ ТП и ИТ-систем. АСУ ТП напрямую взаимодействует с "физическим миром" и сама по себе должна быть надежной. Но исторически сложилось, что при создании автоматизированной системы управления в расчетах показателей надежности не учитывалась возможность деструктивного информационного воздействия.

Даниил Тамеев

Без ложной скромности стоит отметить, что в защите технологического сегмента предприятий ключевым аспектом является отсутствие права на ошибку. Задачи по обеспечению ИБ технологического сегмента особенно актуальны именно предприятиям КВО. Поэтому надо понимать, что объектами защиты выступают системы, выход из строя или даже нештатная работа которых может привести к катастрофическим последствиям. Не говоря уже об огромных финансовых потерях для владельцев предприятий.

Антон Шипулин

Специфика задачи защиты АСУ ТП от угроз информационного характера заключается в том, что необдуманное применение меры защиты может приводить к снижению общей надежности системы. Соответственно, нужно тщательно выбирать средства информационной безопасности и подходы к защите и оценивать последствия их применения. Меры защиты должны не создавать новых проблем нормальному функционированию АСУ ТП, а устранять существующие.

Алексей Полетыкин

С точки зрения защиты информации АСУ ТП специфика состоит в расстановке приоритетов: наивысший должен быть для защиты "доступности", далее "целостности" и потом "конфиденциальности".

С точки зрения безопасности целью является не защита АСУ как таковой, а защита объекта автоматизации: оборудования, людей и функций. В частности, взлом частей АСУ ТП с полной потерей "доступности", "целостности" и "конфиденциальности" не будет рассматриваться как инцидент, если дублирующие системы АСУ (не цифровые) не позволят ухудшить функциональную безопасность, надежность и выпуск продукции.

Поэтому в качестве одних из популярных радикальных мер для защиты применяются "обесточивание", "выключение" и "перезагрузка". Не только при инцидентах, но и как профилактические меры.

В Росатоме торжествует точка зрения, что наиболее критичные цифровые системы нужно дублировать релейными.

– С какими проблемами приходится сталкиваться при реализации АСУ ТП?

Евгений Генгринович

Настройка оборудования под конкретные схемы управления заказчика, интеграция в АСУ ТП существующих каналов передачи данных. Проверка соответ-

ствия конфигураций и параметров, установленных на объектах компонентов АСУ ТП.

Алексей Полетыкин

Основные проблемы, с которыми приходится сталкиваться, – это слабость научной и методической базы, расплывчатость и противоречивость требований.

Даниил Тамеев

Одна из главных особенностей в проектах по обеспечению ИБ технического сегмента – работа с системами реального времени и сложными технологическими процессами, не допускающими даже кратковременной остановки в работе. Специалистам, знакомым с принципами работы подобных систем, хорошо известно, что даже регламентные работы могут проводиться лишь в запланированные технологические окна и по предварительно согласованному со всеми задействованными структурами компании плану.

– Какие существуют риски безопасности реализации АСУ ТП?

Евгений Генгринович

Неправильные настройки оборудования, искажения первичных сигналов, проблемы систем передачи данных, синхронизация времени, ошибки персонала.

Алексей Полетыкин

Риски нужно оценивать на всех этапах жизненного цикла, исходя из специфики объекта автоматизации и АСУ ТП.

Даниил Тамеев

Основной риск – нарушение работоспособности объекта защиты. Избежать этого можно, лишь выбрав в качестве исполнителя проекта грамотную команду специалистов, обладающих должными компетенциями и опытом. Единственным верным вариантом является проведение проекта строго в соответствии с отработанной методикой, согласованной с представителями предприятия и производителями промышленного оборудования.

– Какие основные угрозы безопасности информации и основные виды атак на предприятия КВО вы можете выделить?

Евгений Генгринович

Сама по себе передаваемая информация если и представляет какую-то ценность, то только косвенную, поэтому корректней говорить о безопасности инфраструктуры, а не о безопасности информации.

Угрозы безопасности инфраструктуры:

- нарушение технологического процесса;
- вывод из строя оборудования, задействованного в технологическом процессе;
- угроза жизни людей, участвующих в оперативном и оперативно-ремонтном обслуживании технологического процесса;
- нарушения договорных обязательств;
- техногенные и экологические катастрофы;
- влияние на процессы и людей, зависимых от данного технологического процесса.

Алексей Полетыкин

По частоте и массовости это угрозы, связанные с нецеленаправленными атаками на общепромышленное оборудование, применяемое в АСУ ТП. По тяжести ущерба – целенаправленные атаки.

Антон Шипулин

Основная и уже не такая экзотическая и маловероятная, как раньше, угроза – это угроза вмешательства террористических, экстремистских и враждебно настроенных государственных групп в управление автоматизированными системами критически важных объектов и вывод их из строя. В подтверждение этому можно назвать Указ Президента Российской Федерации от 31 декабря 2015 года № 683 "О Стратегии национальной безопасности Российской Федерации" где в п. 43 указывается, что основными угрозами государственной и общественной безопасности является в том числе деятельность террористических и экстремистских организаций, направленная на уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, а также устрашение населения, в том числе путем нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации. Также угроза кибертерроризма появляется в прогнозе чрезвычайной обстановки на территории Российской Федерации на 2016 г. от МЧС. В нем отмечается, что в настоящее время уровень информационной безопасности не соответствует уровню угроз в данной сфере, и в 2016 г. возможно повышение хакерских атак с целью создания условий для возникновения техногенных чрезвычайных ситуаций. Из промышленных объектов наиболее уязвимы при хакерских атаках энергетические и коммуникационные сети России.

И действительно, террористические организации повышают частоту атак на КВО. В частности, в 2015 г. ФБР США сообщило, что хакеры организации "Исламское государство" (запрещена в России) предпринимают попытки взлома сетей американских энергетических компаний. Пока террористы не применяли сложных инструментов, которые могли бы вызвать отказ в работе объектов, и, соответственно, их попытки атак были безуспешны. Что касается

России, то в 2015 г. российская компания Group-IB выпустила отчет, согласно которому за прошедший год более 600 российских интернет-ресурсов были атакованы хакерами террористической организации "Исламское государство Ирака и Леванта" (запрещена в России). Учитывая интерес подобных группировок к предприятиям КВО США, интерес к российским информационным ресурсам, их мотивированность и финансовые ресурсы, многие эксперты прогнозируют рост угрозы российским критически важным объектам, что находит место в государственных документах.

– С какими инцидентами ИБ вам приходилось сталкиваться на предприятиях КВО?

Евгений Генгринович

Информация является закрытой, компании обычно неохотно предоставляют такую информацию общественности и прессе.

На западе достаточно много публикаций о различных инцидентах, из последних можно упомянуть сталелитейный завод в Германии и Облэнерго Ивано-Франковской области Украины.

Даниил Тамеев

Инциденты ИБ на предприятиях КВО – как суслик в известном фильме: ты их не видишь, а они есть. По ряду причин не допускается публичная огласка мало-мальски значимых инцидентов. Хотя при этом "в кулуарах" зачастую можно услышать довольно курьезные случаи, большинство из которых, как правило, связано с нарушениями техники безопасности и разгильдяйством персонала.

– Как часто в реальности происходят проникновения в промышленные сети?

Дмитрий Даренский

Дело в том, что в России статистики как таковой не ведется. За рубежом с аналитикой немного получше. Например, ICS CERT раз в два–три месяца публикует отчеты с подобной информацией, но данные по российским предприятиям туда не попадают. Информация об инцидентах не публикуется намеренно. Также и результаты аудитов являются практически во всех организациях конфиденциальной информацией. Никто не хочет открыто заявлять о своих уязвимостях. А для крупных компаний это еще и репутационные риски.

Евгений Генгринович

По оценке международных экспертов, за последние два года 80% инцидентов, связанных с информационной безопасностью, имели место в промышленных сетях.

Егор Литвинов

К сожалению, если произошло проникновение в промышленные сети, владелец предприятия/завода старается об этом не распространяться. Другой вопрос – что считать проникновением в промышленную сеть. Как пример – Maroochy Water Breach (сброс сточных вод и загрязнение окружающей среды). Когда инцидент произошел, и о нем стало известно общественности, его не сочли проникновением в промышленную сеть, поскольку злоумышленник являлся сотрудником пострадавшей компании. Некоторые данные можно почерпнуть из базы статистики инцидентов в области АСУ ТП, представленной здесь: http://www.risidata.com/Database/event_date/desc.

Даниил Тамеев

Официально подтвержденных примеров в России, насколько мне известно, нет. Западная же статистика говорил о сотнях инцидентов за год, произошедших в компаниях различных отраслей – от нефтедобычи и металлургии до фармацевтики и пищевых производств.

– Как обеспечить безопасность промышленной сети?

Евгений Генгринович

Тянет на название книги. Однозначного ответа на этот вопрос нет. Гарантированной защиты на 100% не существует. Безопасность промышленной сети – это не результат, а процесс, который обеспечивается сочетанием организационных, методологических и технических мероприятий.

Егор Литвинов

Для обеспечения безопасности промышленной сети необходимо применять комплекс мер, начиная от физической безопасности различных датчиков и исполнительных механизмов. На сегодняшний день современные датчики становятся достаточно "умными", что может быть использовано как во благо, так и во вред. Не стоит также забывать тот момент, что различные протоколы обмена данных в АСУ ТП были разработаны в середине XX в. и не предполагают, что устройство может отвечать "неверными данными".

Алексей Полетыкин

Изоляция. Однонаправленная связь. Механическая защита помещений, кабельных каналов, приборных стоек. Шифрование следует применять, только когда элементы сети выходят за зону охраны.

Даниил Тамеев

Одна из фундаментальных основ ИБ технологической сети – соответствие ее архитектуры требованиям безопасности. В связи с этим большая часть проектов по созданию системы ИБ промышленного объекта базируется на сегментировании технологической сети и формировании выделенных контролируемых зон.

Антон Шипулин

Безопасность промышленной сети, как и безопасность всей АСУ ТП, элементом которой является сеть, обеспечивается применением комплексного последовательного подхода, учитывающего специфику и особенности промышленных систем и основанного на требованиях и рекомендациях как международных стандартов, так и российских нормативных документов по обеспечению информационной безопасности промышленных систем. В числе последних, в частности, приказ ФСТЭК России № 31, определяющий требования к обеспечению защиты информации в АСУ ТП.

Что касается комплексного подхода, то он включает в себя проведение регулярного аудита состояния защищенности АСУ ТП на основе интервьюирования специалистов заказчика, анализа документации, структуры и конфигурации систем, а также проведение инструментального анализа защищенности с целью поиска уязвимостей и с соблюдением предосторожностей, связанных с критичностью обследуемых систем. На основе полученных по итогам аудита данных производится анализ рисков, в результате которого определяются угрозы, представляющие опасность функционированию объекта. Для борьбы с данными угрозами разрабатываются

Groteck
Business Media

ИЗДАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ВСЕГДА НА РАБОЧЕМ СТОЛЕ

ПОДПИСКА НА ЖУРНАЛЫ:
ВО ВСЕХ ОТДЕЛЕНИЯХ ПОЧТЫ РОССИИ

ОФИСНАЯ ПОДПИСКА:
E-mail: monitor@groteck.ru
Тел.: (495) 647-0442, доб. 22-82

Информационное агентство
МОНИТОР

ПОДПИСКА

организационные и технические меры защиты АСУ ТП. Данный процесс не должен прерываться и повторяется периодически. Только так можно адекватно оценить состояние систем и соответствующие им угрозы, а также своевременное предотвращение данных угроз. Одним из важнейших инструментов такого подхода является процесс мониторинга состояния сети и происходящей сетевой активности, что позволяет вовремя реагировать на подозрительные инциденты.

– Насколько усложняет задачу защиты АСУ ТП тот факт, что многие из таких систем уникальны, создавались давно и с использованием устаревших языков?

Евгений Генгринович

Миф, распространяемый людьми, весьма далекими от АСУ ТП. Оборудование АСУ ТП всегда серийно. Автомобиль "Победа" давно не выпускается, но это не мешает действующим машинам ездить по современным дорогам. Запчасти давно не выпускаются, но документация и автомеханики есть. Аналогичная ситуация со старым оборудованием АСУ ТП, используемые протоколы известны, характеристики тоже.

Алексей Полетыкин

Это усложняет не столько защиту, сколько организацию атак. Вообще нужно подходить индивидуально.

Даниил Тамеев

Большинство средств защиты, применяемых в технологическом сегменте, являются наложенными, поэтому степень устаревания целевых систем зачастую может не иметь значения. Хотя, безусловно, это правило действует до определенного предела – когда, к примеру, речь не заходит об аналоговых и механических системах.

– Достаточно ли сейчас на рынке ресурсов, чтобы обеспечить полноценную защиту АСУ ТП, в том числе компетентных специалистов и технических средств защиты?

Алексей Полетыкин

Средств защиты много, но подавляющее большинство нельзя использовать в АСУ ТП по требованиям качества, которое должно обеспечиваться на всех этапах жизненного цикла (контролируется Ростехнадзором). Специалистов с опытом по защите АСУ ТП очень мало. Защиту от целенаправленных атак создавать практически не из чего и некому: крайне мало доверенных решений по компонентам и ПО, нет качественных нормативов и, как следствие, образования.

Евгений Генгринович

Рынок информационной безопасности АСУ ТП только формируется, основная проблема в отсутствии эсперанто ("единого языка общения") между специалистами ИТ, ИБ и АСУ ТП.

Даниил Тамеев

Тема ИБ АСУ ТП стала широко востребованной среди отечественных предприятий последние 1–2 года, и число компаний, заинтересованных в ее развитии, растет буквально с каждым днем: среди них и предприятия, и интеграторы, и производители средств защиты. Как известно, спрос рождает предложение, а значит, дефицит специалистов по ИБ АСУ ТП, который остро чувствуется до сих пор, со временем сократится.

– В каких случаях переход на бюджетные российские решения и оборудование вы считаете целесообразным?

Даниил Тамеев

Во-первых, необходимо разделять понятия "бюджетные" и "российские" решения, так как на сегодняшний день нельзя однозначно заявить, что приобретение отечественных решений всегда выгоднее, даже несмотря на текущую экономическую ситуацию.

Выбор в пользу отечественных решений определяется их большей (в сравнении с импортными) адаптированностью под российские реалии. Сегодня многие отечественные производители ИБ-решений обратили свой взгляд на безопасность промышленных объектов и разрабатывают свои продукты с четким пониманием специфики российского рынка ИБ, требований бизнеса и регуляторов. Поэтому их использование можно считать вполне целесообразным.

Евгений Генгринович

Нет понятия "бюджетные российские продукты", есть решения для различных классов задач (среди них уже достаточное число и российских).

Алексей Полетыкин

Для КВО должны применяться только доверенные российские решения с технической поддержкой на всем этапе жизненного цикла.

Для прочих АСУ российские элементы должны иметь приоритет на законодательном уровне.

– Какие из существующих методов обеспечения безопасности АСУ ТП можно использовать, какие требуют адаптации, а какие необходимо разработать?

Евгений Генгринович

Методы обеспечения безопасности АСУ ТП делятся на две категории. Первая – защита периметра, куда входят различные устройства типа Gateway, и вторая – контроль и анализ отклонений внутри сегмента АСУ ТП.

Разработки ведутся в обеих категориях, так как попытки использовать ИТ-наработки, к сожалению, дают только частичный результат. Уже есть специализированные решения, но развитие продолжается.

Алексей Полетыкин

Все можно использовать, но с адаптацией под специфику АСУ ТП.

– На основании каких характеристик АСУ ТП должны быть сформированы требования по его защите?

Евгений Генгринович

Требования по защите АСУ ТП формируются исходя из модели угроз для данного конкретного объекта или компании.

Алексей Полетыкин

Защита должна исключать неприемлемые риски, связанные со спецификой функций объекта. Например, для электростанции: "не допускается остановка производства электроэнергии из-за кибератак чаще 1 раза в 5 лет на срок более 2 часов".

– Как обеспечить контроль сотрудников предприятия?

Евгений Генгринович

С помощью программных и технических средств (в том числе систем видеонаблюдения).

Алексей Полетыкин

Это входит в сферу ответственности специальной безопасности. При оценке рисков необходимо рассматривать особенности этой защиты, которые служат барьерами проникновения опасного оборудования и злоумышленников для организации атак на АСУ ТП. В ИПУ РАН разработана методика расчета рисков нарушения информационной безопасности, учитывающая такого рода барьеры.

– Возможно ли защититься от инсайдерских инцидентов? Что для этого необходимо предпринять?

Евгений Генгринович

Да, возможно: установить специализированное ПО.

– Что должен включать в себя комплекс мер, предотвращающих появление мошенничества в компании?

Евгений Генгринович

Организационно-методический реинжиниринг существующих процессов и информационных потоков, а также использование специализированного ПО класса Predictable Analytics.

**– Учитывая стремительное распространение мобильных устройств, концепции BYOD, облачных вычислений и различных технологий для удаленной работы, все чаще приходится слышать об исчезновении периметра корпоративной сети.
Является ли концепция его защиты устаревшей или она нуждается в адаптации к современным условиям?**

Евгений Генгринович

Периметр корпоративной сети существует в любом случае, даже если мы говорим о транснациональной компании с выносом основной работы сотрудников в облако. Устарела концепция периметра как локализованного объекта, концепции его защиты не поменялись, просто часть функций обеспечивается внешней организацией.

Алексей Полетыкин

Адаптация к современным условиям необходима. По существу, контуры управления современными промышленными предприятиями вышли за пределы охраняемых зон. Этот феномен требует научного изучения и описания.

**– Согласно результатам исследований треть пользователей записывают пароли, а это означает, что любые носители информации о пароле могут быть доступны другим лицам.
Большинство экспертов приходит к выводу, что компаниям следует отойти от общепринятой системы авторизации, т.к. эта система слишком неустойчива к попыткам взлома, и использовать новые методы обеспечения безопасности. Основная рекомендация заключается в использовании биометрических технологий.
Как вы относитесь к внедрению биометрии на промышленных предприятиях?
Есть ли у вас опыт внедрения данной технологии?**

Евгений Генгринович

Никак, биометрия – один из способов аутентификации пользователей, при этом уже есть варианты ее обхода тоже. Для работы с паролями на рынке предлагаются системы менеджмента паролей с высоким уровнем защиты и шифрования данных. Треть пользователей записывают пароли, а 90% устройств АСУ ТП используются с заводскими паролями, но эта проблема не имеет отношения к способу аутентификации, а, скорее, к культуре организации эксплуатации того или иного объекта или системы.

Алексей Полетыкин

Я согласен, что пароли являются устаревшим и подчас опасным средством. В критических ситуациях они могут серьезно мешать работе.

Биометрия представляется лучшим решением. Но это нужно обосновать путем проведения специальных научных исследований, которые подтвердили бы надежность и безопасность для персонала и технологического процесса.

– Системы распознавания образов (СРО) на настоящий момент находят все больше применения в промышленности, торговле, бизнесе и повседневной жизни. Каковы основные этапы построения СРО на предприятиях КВО?

Евгений Генгринович

Странный вопрос: если сформулирована задача, например при работе с оперативно-ремонтным персоналом, то имеет место внедрение СРО. Этапы стандартные, ТЗ, проектирование, поставка оборудования и ПО, наладка, внедрение.

Алексей Полетыкин

К ним нужно применять требования по надежности, точности и т.п. и строить по ГОСТ 34.

– Система видеонаблюдения – одна из составляющих частей комплексной системы безопасности. Какими основными характеристиками должны обладать камеры видеонаблюдения на промышленных предприятиях?

Евгений Генгринович

Многое зависит от специфики производства. Базовые функции стандартные, а форм-фактор, питание, электромагнитная совместимость и каналы коммуникаций определяются требованиями заказчика и решаемой задачей.

Алексей Полетыкин

Мы проводили исследования, можно ли видеонаблюдение использовать для контроля доступа к элементам АСУ ТП. Вывод, скорее, отрицательный. Дело в том, что элементы АСУ ТП размещаются в помещениях сложной конфигурации, сами элементы часто очень сложные и включают маленькие детали, которые нетрудно подменить.

Видимо, для современных промышленных АСУ ТП видеонаблюдение не способно заменить надзор со стороны людей. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Новый взгляд на мошенничество в сфере компьютерной информации

Ильдар Бегишев, *институт экономики, управления и права (г. Казань)*

Вопрос хищения чужого имущества или приобретения на него права в сфере обращения компьютерной информации давно представляет научный и практический интерес. Совсем недавно данный вопрос был решен. Так, Федеральным законом Российской Федерации от 29 ноября 2012 г. № 207-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" законодатель включил ст. 1596 в Уголовный кодекс Российской Федерации (УК РФ).

Статья 1596 УК РФ устанавливает ответственность за "хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей".

Действия, являющиеся преступными, и предмет посягательства

В соответствии с диспозицией статьи 1596 УК РФ мошенничеством в сфере компьютерной информации признаются два общественно опасных действия: хищение чужого имущества и приобретение права на него. Причем оба действия должны обязательно осуществляться путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Предметом преступного посягательства рассматриваемой статьи являются:

- компьютерная информация, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи;
- имущество, т.е. совокупность вещей, которые находятся в собственности какого-либо физического или юридического лица, публично-правового образования (включая деньги и ценные бумаги), а также их имущественных прав на получение вещей или имущественного удовлетворения от других лиц, представляющие для собственника какую-либо полезность.

Следует иметь в виду, что предметом компьютерного мошенничества, как и традиционного, является чужое имущество или право на него. Но в компьютерах и компьютерных сетях хранятся не деньги или имущество, а информация о них или об их движении. Информация – не имущество, она не обладает экономическим, социальным и юридическим признаками, характеризующими чужое имущество как предмет хищения, который выступает обязательным признаком состава мошенничества. Это всего лишь сведения, представленные в специфической форме. Законодателем акцент сделан на форму существования информации как сведений о лицах, явлениях и процессах, содержащихся в информационных системах (банках данных) именно в компилированном виде.[1]

Способы завладения имуществом

Законодательно выделилены следующие способы:

1. Ввод компьютерной информации, т.е. размещение сведений в цифровых устройствах для их последующей обработки и хранения.
2. Удаление компьютерной информации, т.е. совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации.
3. Блокирование компьютерной информации, т.е. совершение действий, приводящих к ограничению или полному запрету доступа к компьютерной информации, но не связанных с ее удалением.
4. Модификация компьютерной информации, т.е. совершение любых изменений компьютерной информации.

Помимо указанных действий законодателем отдельно выделены способы, связанные с иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Открытым и законодательно нерешенным остается вопрос о таком способе совершения рассматриваемого преступления, как копирование компьютерной информации, т.к. при помощи копирования с последующим ее изменением и перенаправлением в нужном векторе также может быть совершено хищение чужого имущества или приобретение права на него.

Мошенническое программное обеспечение

Мошенничество в сфере компьютерной информации может совершаться не только вышеописанными способами, но и с использованием вредоносных компьютерных программ. К этому классу можно отнести и мошенническое ПО.

На сегодняшний день мошенническим ПО выступают, например:

- программы-баннеры, всплывающие в окнах браузера;

[1] *Лопатина Т.М. Проблемы уголовно-правовой защиты сферы компьютерной информации: современный взгляд на мошенничество // Право и безопасность. – 2013. – № 3–4. – С. 93.*

- программы-блокираторы, блокирующие доступ в Интернет, возможности ОС Windows, действия с файлами и данными;
- программы-шифровальщики файлов и данных.

Общей особенностью для этого вида мошеннических программ является то, что устранение деструктивных действий указанных программ происходит путем отправки на известный номер телефона платного SMS-сообщения.

Однако уже сегодня можно с уверенностью констатировать, что мошенничество в сфере компьютерной информации будет только наращивать обороты и появляться в электронной коммерции, службах заказа билетов, на электронных площадках оплаты товаров и услуг, в секторе ДБО и т.д. Опасность распространения угрозы цифрового мошенничества налицо.

Рассуждая о мошенничестве в сфере цифровой информации, нельзя не сказать о мошенническом ПО, позволяющем нарушать системы защиты цифровой информации. Сегодня зачастую такое ПО находится в свободном доступе в сети Интернет или же нелегально приобретается на соответствующих виртуальных площадках у его разработчиков. Таким образом, ограничение в создании, использовании и распространении такого ПО существенно затруднило бы злоумышленникам совершение подобного рода мошенничеств. Это также касается вредоносных компьютерных программ и программных средств, предназначенных для нарушения систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей.

Поэтому предлагаем включить в единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено, сайты, содержащие или распространяющие вредоносные компьютерные программы, мошенническое ПО и программные средства, предназначенные для нарушения систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей.

Следует отметить, что правилами создания, формирования и ведения единой автоматизированной информационной системы единого реестра идентификации запрещенного на территории РФ контента в Интернете (№ 149-ФЗ от 27 июля 2006 г.), утвержденными постановлением Правительства Российской Федерации от 26 октября 2012 г. № 1101 "О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено"[2], за создание единого реестра отвечает Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Кроме того, ведение единого реестра осуществляется в электронной форме в ежедневном круглосуточном режиме.

Такой механизм предупреждения мошенничества в сфере компьютерной информации, по нашему мнению, является наиболее эффективным. Провайдеры хостинга и операторы связи используют указанный единый реестр и успешно ограничивают доступ к этим ресурсам. Необходимо отметить, что аналогичные схемы уже работают и успешно применяются на практике в отношении:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к его совершению;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 г. № 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" и Федерального закона от 11 ноября 2003 г. № 138-ФЗ "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи.[3]

Следует отметить, что многие современные антивирусные программы в своем составе имеют модули, позволяющие распознать и прекратить распространение мошеннического ПО. Однако некоторые пользователи сети Интернет не могут или не желают платить за антивирус и не устанавливают его на свои компьютеры, тем самым позволяя совершать в отношении них мошеннические действия в сфере компьютерной информации.

Выводы

В заключение сформулируем предложение по противодействию мошенничеству в сфере компьютерной информации.

Предлагается дополнить п. 1 ч. 5 ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ следующим пунктом:

е) вредоносных компьютерных программ и программных средств, предназначенных для нарушения систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей.

Согласно статье 273 УК РФ "Создание, использование и распространение вредоносных компьютерных программ" под вредоносными понимаются программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. В свою очередь, проанализировав диспозицию статьи 1596 УК РФ, можно сделать вывод о том, что мошенническое ПО – это программы, позволяющие вводить, удалять, блокировать, модифицировать компьютерную информацию либо осуществлять иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Таким образом, мошеннические программы по способу деструктивного воздействия на компьютерную информацию, результату воздействия, наличия целей и мотивов являются аналогичными с вредоносными программами.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

[2] *Собрание законодательства Российской Федерации от 29 октября 2012 г. – № 44. – Ст. 6044.*

[3] *Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // Собрание законодательства Российской Федерации от 31 июля 2006 г. – № 31 (часть I). – Ст. 3448.*

Предупрежден – значит вооружен

Дмитрий Фролов, *начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России*

Рост кибератак на кредитно-финансовые организации очевиден. Для эффективной борьбы с ними Банк России создал Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT), который осуществляет сбор и анализ информации от финансовых учреждений о кибератаках, а также предупреждает о возможных угрозах ИБ и взаимодействует с правоохранительными органами. Об основных принципах работы FinCERT и перспективах развития данного подразделения рассказывает его начальник Д.Б. Фролов.

– Дмитрий Борисович, напомните, пожалуйста, нашим читателям, каковы функции FinCERT?

– Основной стратегической целью деятельности FinCERT – Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере – является повышение организациями, поднадзорными Банку России, эффективности мер по борьбе с противоправными действиями, осуществляемых при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий. Центр также проводит работу по противодействию компьютерным атакам на информационные ресурсы организаций, поднадзорных Банку России.

Повышение уровня доверия к деятельности Центра должно произойти естественным путем после создания удобного и надежного интерфейса для информационного взаимодействия и обеспечения оперативного реагирования на выявленные угрозы нарушения информационной безопасности.

В качестве основных целей создания автоматизированной системы рассматриваются обеспечение двустороннего обмена данными как с Центром, так и с другими участниками информационного обмена и централизованное хранение данных о выявленных угрозах нарушения информационной безопасности.

Главной задачей в рамках обозначенной цели является организация непрерывного взаимного информирования об угрозах нарушения информационной безопасности организаций, поднадзорных Банку России, и минимизация наносимого при реализации угроз материального ущерба. Для этого Центр собирает технические данные об угрозах нарушения информационной безопасности из следующих источников:

- организации, поднадзорные Банку России;
- государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА);
- органы исполнительной власти;
- правоохранительные органы;
- иные организации, например, антивирусные компании, вендоры программного обеспечения, регистраторы доменных имен;
- средства массовой информации/Интернет;
- физические лица.

– С какими основными видами инцидентов приходится иметь дело?

– Среди наиболее актуальных угроз нарушения информационной безопасности организаций, поднадзорных Банку России, стоит отметить следующие:

- целевые атаки на платежные автоматизированные системы кредитных организаций;
- неправомерный доступ к конфиденциальной компьютерной информации;
- использование вредоносного программного обеспечения;
- распределенный отказ в обслуживании (DDoS-атаки);
- мошенничество с использованием электронной почты;
- мошенничество с использованием средств сотовой связи;
- мошенничество с использованием номеров в коде "8-800".

– На сегодняшний день основным принципом взаимодействия FinCERT с кредитными и финансовыми организациями является добровольность. Однако банки зачастую опасаются сообщать об инцидентах. Как можно решить эту проблему?

– Это, прежде всего, вопрос доверия как во взаимоотношениях банков друг с другом, так и с регулятором. Постепенно мы такое доверие рынка завоевываем. Причем среди банков, ставших участниками информационного обмена, есть и такие, которые не только делятся информацией, но и предлагают свои подходы к решению различных проблем. В то же время обмен техническими данными об угрозах позволяет существенно повысить эффективность мер по противодействию компьютерным атакам на информресурсы этих организаций. Понимание этого станет важным стимулом для расширения масштабов взаимного информирования.

Речь идет, например, об обмене следующими данными:

- IP-адреса, с которых осуществляются DDoS-атаки;
- IP-адреса, с которых осуществляется рассылка писем с вымогательством денежных средств за прекращение атак;
- маркеры заражения вредоносным программным обеспечением (например, временные папки, хеш-суммы файлов, создаваемые сетевые соединения и процессы);
- управляющие команды, которые могут быть использованы для удаленного несанкционированного управления программным обеспечением;
- IP-адреса и доменные имена сайтов, используемых для осуществления мошеннических действий;

● телефонные номера, с которых осуществляются мошеннические SMS-рассылки и телефонные звонки.

Повышение уровня доверия к деятельности Центра должно произойти естественным путем после создания удобного и надежного интерфейса для информационного взаимодействия и обеспечения оперативного реагирования на выявленные угрозы нарушения информационной безопасности.

На сегодняшний день одним из ключевых факторов, негативно влияющих на безопасность информационных ресурсов организаций, поднадзорных Банку России, является отсутствие оперативной координации таких организаций как между собой, так и с правоохранительными органами и органами исполнительной власти, а также с физическими лицами и иными организациями. На базе Центра организована возможность налаживания такого взаимодействия. С целью создания доверительной среды взаимодействия с поднадзорными организациями Центр проводит постоянную работу по освещению своей деятельности на профильных мероприятиях.

– Ранее в своем интервью нашему журналу* Артем Михайлович Сычев, заместитель начальника ГУБиЗИ Банка России говорил, что "должны появиться документы, формирующие процесс обмена информацией" между FinCERT и кредитными организациями. Когда можно ожидать подобные документы?

– Общие положения данного процесса предполагается закрепить в соглашении между участником информирования и Банком России.

Соглашение будет предусматривать разработку регламента взаимодействия, в котором среди прочего должно быть описание ответственных лиц, состава передаваемых технических данных, порядка действий участников непрерывного взаимного информирования.

На сегодняшний день проект соглашения прорабатывается в Банке России, результаты будут доведены до кредитных организаций.

– На одной из конференций прошлого года Вы говорили о планах по автоматизации Центра. Какие шаги уже предприняты и какие можно ожидать в ближайшее время и в долгосрочной перспективе?

– Мы прорабатываем вопросы, связанные с возможной архитектурой и сроками реализации проекта.

В качестве основных целей создания автоматизированной системы рассматриваются обеспечение двустороннего обмена данными как с Центром, так и с другими участниками информационного обмена и централизованное хранение данных о выявленных угрозах нарушения информационной безопасности.

В среднесрочной перспективе планируется создание полноценной системы аналитики, основанной на собранных данных об угрозах нарушения информационной безопасности.

– Осенью 2015 года благодаря Центру мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России была успешно предотвращена атака на ряд банков. Расскажите, пожалуйста, об этом подробнее.

– В рамках информационного обмена была получена информация о готовящихся DDoS-атаках на ряд кредитных организаций. Центр направил участникам информационного обмена уведомление о мощности и характеристиках ожидаемой атаки. В период с 28.09.2015 по 01.10.2015 злоумышленники осуществили ожидаемые DDoS-атаки. По информации Центра, характерная особенность атаки – использование публичных серверов точного времени для усиления мусорного трафика. Мощность атаки была выше средних значений, вместе с тем доступность систем кредитных организаций нарушена не была.

Дополнительно был выявлен факт вымогательства у организаций, на которые осуществлялись указанные DDoS-атаки. На электронную почту кредитных организаций рассылались электронные письма с требованием выплатить на Биткойн-кошелек 50 единиц криптовалюты.

– Удалось ли вычислить злоумышленников правоохранительным органам?

– В настоящее время оперативно-розыскные мероприятия продолжаются. Вся информация о характеристиках атак, собранная Центром в рамках информационного взаимодействия, передана в правоохранительные органы. По мере необходимости работники Центра в рамках своих полномочий принимают участие в совместной с правоохранительными органами работе по определению IP-адресов, с которых осуществлялись DDoS-атаки, привлекаются в качестве консультантов и специалистов в области безопасности банковских технологий.

– Какие рекомендации вы можете дать нашим читателям?

– Для повышения безопасности кредитным организациям необходимо соблюдать ряд правил:

1. Разделять сегменты локальной вычислительной сети кредитной организации, в которых обрабатывается платежная и иная информация, с обязательным контролем входящих и исходящих потоков данных.

2. Использовать эшелонированную и своевременно обновляемую защиту. При этом средства защиты информации должны быть не просто установлены в инфраструктуре, но и в обязательном порядке настроены с учетом особенностей бизнес-процессов кредитной организации.

3. Расчитывать риски нарушения информационной безопасности и включать их в состав операционных рисков кредитной организации.

4. Повышать квалификацию работников служб информационной безопасности.

5. Участие специалистов кредитной организации в непрерывном взаимном информировании об угрозах нарушения информационной безопасности, организованном Центром, и понимание на уровне руководства кредитной организации важности подобного обмена. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

По мере необходимости работники Центра в рамках своих полномочий принимают участие в совместной с правоохранительными органами работе по определению IP-адресов, с которых осуществлялись DDoS-атаки, привлекаются в качестве консультантов и специалистов в области безопасности банковских технологий.

Основной стратегической целью деятельности FinCERT – Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере – является повышение организациями, поднадзорными Банку России, эффективности мер по борьбе с противоправными действиями, осуществляемых при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий.

** Сычев А. Банк России среагировал на киберугрозы // Информационная безопасность/Information Security. — 2015. — №4. — С.10–11.*

SOC: кадры решают все

Андрей Янкин, *руководитель отдела консалтинга Центра информационной безопасности компании "Инфосистемы Джет"*

Обсуждение Security Operation Center (SOC) часто начинают с определения термина и, не придя к единому мнению, на нем же и заканчивают. Поэтому сразу обозначу: SOC – не столько технические средства, сколько команда, обнаруживающая, анализирующая, реагирующая, уведомляющая о возникновении и предотвращающая инциденты ИБ. Чтобы персонал, вооруженный техническими средствами, понимал свои задачи, имел четкие инструкции и KPI, мог эффективно взаимодействовать внутри SOC и со смежными подразделениями, необходимо выстроить целый ряд процессов в зоне ответственности SOC.

Состав персонала SOC разнообразен и определяется выполняемыми функциями и его местом в организации. Например, в данный момент мы принимаем участие в строительстве SOC в крупном банке и в промышленной компании. В первом случае в SOC также переданы задачи отслеживания фрода, а во втором – мониторинг технической и физической безопасности. Для решения таких задач дополнительно нужна целая команда узких специалистов. Но как обеспечить выполнение основных функций SOC: сбор и анализ данных от ИТ-систем и пользователей, расследование и реагирование на инциденты ИБ и оперативное информирование всех заинтересованных сторон? Как сформировать и поддерживать соответствующий штат?

Кого искать?

Ключевой принцип подбора персонала для SOC – "качество важнее количества". Главная задача в том, чтобы на ключевых позициях были профессионалы высочайшего уровня. Это тот случай, когда лучше нанять одну "звезду", чем двух рядовых аналитиков (особенно в начале создания SOC).

Помимо прочего SOC должен оперативно обрабатывать заявки и звонки пользователей, сообщения от различных подразделений компании, информацию из внешних источников и т.д. Для этого необходимы время и группа 1-й линии, которая обеспечит разбор входящей информации и выделение в общем потоке данных, свидетельствующих об инциденте ИБ. Специалисты 1-й линии не производят глубокий анализ инцидентов, их основная задача – оперативно обработать входящую информацию и принять решения по реагированию на типовые угрозы. Если обработка инцидента занимает более нескольких минут, инцидент передается на 2-ю линию SOC. Эскалации также подлежат все инциденты с высоким уровнем критичности.

Задержка между получением данных 1-й линией и эскалацией не должна превышать строго определенное время. Сотрудники 2-й линии должны обладать более глубокими экспертными компетенциями. Они могут расследовать инцидент от нескольких минут до недель, собирая детальные данные, привлекая экспертов, восстанавливая последовательность действий и готовя рекомендации по ликвидации последствий инцидента, внедрению контрмер и т.д. Формально относящиеся к делу сотрудники 2-й линии сделают неэффективным весь SOC. Здесь нужны настоящие энтузиасты своего дела (для которых ИБ больше, чем просто работа), обладающие практическим опытом в обеспечении ИБ.

Повышает качество работы SOC, мотивацию и профессиональный уровень персонала и кадровая ротация внутри SOC: специалисты 2-й линии должны

Создание SOC – дело не моментальное: если внедрение технических средств и процессов можно форсировать, то формирование крепкой команды SOC обычно требует длительного периода времени. Как совместить оба процесса с сохранением их максимальной эффективности? Один из наших проектов по созданию SOC выполнялся по следующему "календарю":
*** 0–4 месяц: SOC еще нет, но на этом этапе уже сформирована внутренняя команда "строителей", назначен руководитель. Формируется бюджет. Идет проектирование, в том числе и организационной модели.**
*** 5–12 месяц: активная стадия технического внедрения и вывод SOC в пилот. В это же время идет наем персонала, 1-я линия укомплектована на 80%, 2-я – на треть (частично за счет сотрудников компании). Сотрудники интенсивно обучаются.**
*** 12–18 месяц: SOC полноценно функционирует, готов к переводу на режим 24x7; окончено комплектование основного штата, перманентно идет поиск "звезд" для 2-й линии.**
*** После 18 месяцев: развитие SOC – формирование специализаций (особенно во 2-й линии), рост отдельных сотрудников из 1-й линии во 2-ю.**

часть времени работать в 1-й, а специалисты 1-й линии – привлекаться к расследованию части инцидентов. При этом специалисты 2-й линии (или отдельная команда) должны совершенствовать метрики, используемые специалистами 1-й линии при обработке и эскалации инцидентов, а также анализировать нетипичную и аномальную активность.

Не каждый SOC может позволить себе две линии, но такое разделение позволяет наиболее эффективно использовать знания и таланты персонала. Помимо аналитиков 1-й и 2-й линии в состав SOC часто входят управленцы и администраторы используемых систем ИБ. Хотя администрирование может осуществляться и другим подразделением или частично самими специалистами SOC, имеющими достаточные компетенции.

Где искать?

Идеально – найти специалистов с опытом работы в SOC. Однако рынок предлагает исключительно малое число экспертов, уже работавших в российском, а тем более в западном или азиатском SOC. Хорошо, если такие профессионалы войдут в ядро команды, однако большую часть сотрудников, скорее всего, придется набирать из смежных областей.

Костяк команды лучше сформировать как можно раньше, чтобы он поучаствовал во внедрении систем и отладке процессов. Стоит привлечь к работе в SOC и часть сотрудников компании, знающих особенности ее ИТ-инфраструктуры, ИБ-систем и бизнес-процессов. Полезный для сотрудников SOC бэкграунд включает опыт администрирования ИТ- и ИБ-систем, навыки практической безопасности (особенно пентестов), умение программировать на одном или нескольких языках. Последний навык кажется избыточным, но на практике он крайне полезен при разборе инцидентов (глубокое понимание работы систем) и при автоматизации рутинных задач, которых в SOC хватает.

В 1-ю линию зачастую попадают молодые специалисты с начальным уровнем знаний. Не каждая компания может позволить себе обучать вчерашних студентов без опыта работы, однако даже небольшого опыта администрирования, как правило, хватает. Из-за разнообразия и интенсивности задач специалисты 1-й линии стремительно набирают опыт. Уже через пару лет многие профессионально готовы к переводу во 2-ю линию. И, учитывая сложности поиска хороших аналитиков для 2-й линии, этим источником не стоит пренебрегать.

Дополнительные скиллы

Иногда на SOC возлагаются задачи, требующие узкопрофильных специалистов. К примеру, опытный пентестер для SOC, в который передан процесс управлениями уязвимостями, – действительно ценное приобретение. Специалиста, осуществляющего периодическое сканирование сети на уязвимости и анализирующего результаты, найти сравнительно просто, а полноценного пентестера гораздо сложнее. Пентестер пригодится и в процессе расследования инцидента и имитации атак.

В ряде случаев в SOC выделяются специалисты по анализу вредоносного кода и анализу дампов памяти. Особенно это актуально для банков, традиционных жертв APT-атак. Или, скажем, при расследовании инцидента в системе ДБО крайне важно понимать логику ее работы. Но для этого проще привлечь сотрудника из другого подразделения. Однако согласовать это нужно заранее, т.к. процесс расследования должен быть максимально оперативным, и времени искать нужного специалиста не будет. Можно рассмотреть и вариант аутсорсинга для отдельных задач.

Режим работы

Важная тема – режим работы SOC. Идеальный вариант – работа 24x7 в полную мощность. Многие атаки осуществляются ночью. Поэтому при работе в режиме 8x5 полноценная реакция последует только к обеду следующего рабочего дня, когда аналитики разгребут завал данных за ночь (или выходные) и разберутся в ситуации.

Наш опыт показывает, что затраты на режим 24x7 могут оказаться неподъемными. В сменах работают живые люди, им необходимы выходные и отпуск. Работа в SOC требует внимания и быстрой реакции, поэтому превышение 8-часового порога нежелательно. Получается, что только на 1-ю линию необходимо минимум 5 человек на полную ставку (а ведь желательно, чтобы аналитики еще и страховали и перепроверяли друг друга, передавали дела между сменами – тут получаем все 8 человек). Поэтому зачастую формируют промежуточные варианты. Например, 12x5 с двумя пересекающимися сменами по 8 часов в будни и в выходные. Аналитики 2-й линии могут работать при этом в режиме 8x5. На ночь консоль SIEM можно выводить дежурной ИТ-смене, чтобы они отслеживали самые критичные ситуации. На практике очень сложно найти аналитиков 2-й линии, готовых работать в ночное время. С 1-й линией в этом вопросе обычно проще. Оценивая расходы на тот или иной режим работы SOC и актуальные ИБ-риски организации, можно выбрать наиболее оптимальную конфигурацию для каждого случая.

Учить или не учить?

Обучение сотрудников, посвященное техническим средствам, используемым в SOC, – неплохая идея. Оно не сделает из них экспертов, однако позволит быстро сориентироваться в сложных продуктах (типа SIEM или сканера безопасности). Обучение могут провести интегратор или консультанты, участвующие во внедрении системы. Оно может включать не только технические моменты, но и процедуры, индивидуальные для конкретного SOC. Все новые сотрудники SOC должны обязательно проходить тренинги, знакомящие их с обязанностями, регламентами и техникой. В противном случае есть риск однажды обнаружить, что 1-я линия, к примеру, уже 6 месяцев пропускает критичные инциденты. Сбор и распространение внутри команды информации о новых угрозах и трендах в ИБ должны быть непрерывным процессом. Важный компонент – обмен опытом внутри команды, в том числе в рамках ротаций.

В среднем команда SOC почти полностью обновляется за 6 лет. Это значит, что задача поиска новых специалистов и развития существующих будет стоять постоянно. К поиску и удержанию ключевых сотрудников стоит отнестись со всей серьезностью, так как профессиональная и сработавшаяся команда – главное слагаемое успеха корпоративного SOC.

Какой SOC выбрать?
Свой, аутсорсинговый или гибридный

Алексей Павлов, *ведущий аналитик Solar JSOC компании Solar Security*

За последнее время в прессе со скоростью грибов после дождя появляются статьи о SOC. Мысли про Security Operations Center плотно занимают умы многих сотрудников и руководителей служб информационной безопасности, которые рассматривают возможность строительства собственного SOC, но, столкнувшись с трудностями, часть из них отметает эту идею. В данной статье рассмотрим предпосылки и основные трудности строительства собственного Security Operations Center.

Каковы же главные критерии выбора в пользу использования локального Security Operations Center, для кого он актуален? Думаю, не открою тайну, если скажу, что основной SOCостроитель – компании и корпорации сегмента Enterprise. Именно в этом сегменте департамент информационной безопасности имеет значительный штатный состав, собственные бюджеты и четко очерченный круг решаемых задач. Высокая ценность защищаемой информации, большое количество различных средств ее защиты, территориально распределенная структура, количество работников в несколько тысяч человек – если эти критерии относятся к профилю компании, наверняка создание собственного SOC – вопрос времени.

Основой любого центра мониторинга и реагирования на инциденты информационной безопасности являются следующие компоненты:

- персонал – инженеры, аналитики, архитекторы, администраторы;
- контент – наборы корреляционных правил, регламенты анализа инцидентов, шаблоны оповещения, базы знаний по различным угрозам и векторам атак;
- процессы – процедуры разбора инцидента, реагирования, отчетности, эскалации и противодействия инцидентам;
- мощности и лицензии – размещение платформы SOC, SIEM-системы, средств мониторинга работоспособности, хранилища событий, инцидентов, лицензии SIEM-системы и дополнительных модулей.

Если вопрос с мощностями и лицензиями можно решить с помощью прямых финансовых вливаний, то первые три пункта требуют огромных временных и трудозатрат. Давайте рассмотрим подробнее именно эти пункты.

Персонал, контент, процессы

Про дефицит специалистов и инженеров ИБ на российском рынке написано немало статей. Поиск одного аналитика зачастую занимает несколько месяцев, в зависимости от предлагаемых условий. Далее необходимо еще до полугода, в зависимости от квалификации сотрудника, для полноценного включения его в работу. Если же у компании существуют требования к организации мониторинга 24x7, то ситуация усложняется еще больше.

Рассматривая второй и третий пункты, стоит сказать, что это краеугольный камень в задаче построения центра мониторинга и реагирования на инциденты ИБ.

Наполнение SIEM-системы контентом является важнейшей задачей, т.к. базовый набор правил "из коробки" не способен закрыть все потенциальные векторы угроз для компании, особенно класса Enterprise. Для решения данной задачи необходим архитектор SIEM-системы, который будет выстраивать контент в зависимости от поставленных перед SOC целей, адаптировать его под инфраструктуру, реализовывать сценарии выявления инцидентов в бизнес-приложениях. Также необходимы инженеры для подключения источников и написания коннекторов к приложениям, администратор, обеспечивающий работоспособность и занимающийся "железной" архитектурой.

Помимо персонала и контента, не менее важной задачей является строгое регламентирование процессов обнаружения, анализа инцидентов, оповещение ответственных лиц, выстраивание схем взаимодействия между подразделениями. Необходимо не только обеспечить процедуру уведомления и расследования каждого типа инцидента, но и предусмотреть SLA, эскалацию и отчетность. По инцидентам высокой критичности стоит заранее предусмотреть возможность вмешательства в бизнес-процессы вплоть до остановки последних, оценив риски последствий инцидента и сравнив их с потерями от временного простоя отдельных подразделений.

SOC as Service

Для крупной компании, желающей построить собственный SOC с нуля, попытка реализации может занять годы и не увенчаться успехом. Возникновение проблем в любом из пунктов, указанных в первой части статьи, может загубить благую идею SOC-строительства. Зачастую это может произойти не по вине ответственных за SOC департаментов, а по причине внутренних взаимодействий внутри структуры компании, конфликтов с бизнес-подразделениями.

Другим важным аспектом, который стоит учитывать при построении собственного центра мониторинга, является желание бизнеса выделять деньги

Для крупной компании, желающей построить собственный SOC с нуля, попытка реализации может занять годы и не увенчаться успехом. Возникновение проблем в любом из пунктов, указанных в первой части статьи, может загубить благую идею SOC-строительства. Зачастую это может произойти не по вине ответственных за SOC департаментов, а по причине внутренних взаимодействий внутри структуры компании, конфликтов с бизнес-подразделениями.

на обеспечение безопасности здесь и сейчас. Он часто не готов ждать 1–2 года, пока "взлетает" внутренний SOC.

Здесь и поможет сервис-провайдер, "закрыв" переходный период до запуска собственного Security Operations Center, встроив свои процессы в текущую модель информационной безопасности компании.

SOC as Service значительно снижает риски неудачи, позволяя запустить мониторинг в кратчайшие сроки, предоставляя экспертизу, команду и контент. При этом капитальные затраты отсутствуют, что позволяет "безболезненно" отключиться от облачного SOC в любой момент.

Если вы используете SOC as Service, то сразу решаете проблему персонала (как инженеров, так и аналитиков), наполнения контентом SIEM-системы, разработки регламентов и процессов взаимодействия при обнаружении, разборе и противодействии инцидентам – все задачи ложатся на плечи аутсорсера. При этом сервис-провайдер учитывает специфику компании и внутренние требования к организации процесса. В регламенте отражается четкое разделение ответственностей между заказчиком и подрядчиком.

Но если компания настроена на строительство собственного SOC, в рамках переходного периода наиболее интересным вариантом к рассмотрению является использование гибридной модели Security Operations Center, подразумевающей под собой использование собственной SIEM-системы, которую сервис-провайдер забирает на администрирование и "приземляет" на нее контент, оптимизируя под заказчика. Гибридный вариант также решает задачу быстрого поиска команды мониторинга, что дает дополнительное время компании на поиск собственной команды.

Гибридный SOC

Давайте остановимся подробнее на архитектуре данного решения.

В случае гибридной модели SIEM-система приобретается на средства компании и располагается в ее инфраструктуре. Выбор нужного решения является сложным вопросом, и при решении использовать гибридный SOC необходимо учитывать тенденции рынка и мнение компании, оказывающей аутсорсинговые услуги. Большинство отечественных сервис-провайдеров на данный момент используют HP ArcSight, хотя в последнее время поднимаются разговоры об использовании IBM QRadar, Splunk и даже российских SIEM-систем в качестве платформы оказания сервиса по мониторингу и реагированию на инциденты.

Первоначальная установка и настройка решения может реализовываться как интегратором, организующим поставку, так и сервис-провайдером, обеспечивающим мониторинг. Причем второй вариант предпочтительнее, так как при подключении компании к сервису по выявлению инцидентов подрядчик зачастую использует свои коннекторы, парсеры, настройки SIEM-системы, и его привлечение позволит исключить двойную работу.

На период оказания сервиса администрированием системы сбора событий и серверов коннекторов обычно занимается аутсорсер, а заказчику предоставляется ограниченный доступ к консоли SIEM-системы. Такой подход связан как с политикой конфиденциальности и защиты авторского контента, так и с разделением ответственностей – сервис-провайдер отвечает за работоспособность системы, в том числе и деньгами, поэтому старается минимизировать риски, связанные с человеческим фактором и нештатным вмешательством в работу ПО.

Параллельно с техническими работами на SIEM-системе происходит обследование инфраструктуры, общение с владельцами систем, службой ИБ, ИТ и выстраивание процедуры взаимодействия при разборе различных типов инцидентов. Документ, разрабатываемый в процессе обследования, представляет собой готовый регламент, который в дальнейшем может использоваться заказчиком при запуске собственного SOC.

Помимо регламента регистрации и оповещения по инцидентам ИБ, важным процессом является процедура взаимодействия с ключевыми подразделениями при разборе инцидентов и противодействия угрозам. Период оказания сервиса позволит создать представление о том, как выстраивать взаимодействие с ИТ-отделом, службой сервис-деска, бизнес-подразделениями к моменту запуска внутреннего SOC.

При использовании гибридного варианта решаются в том числе те немногие проблемы использования облачного SOC, которые тревожат некоторые компании:

1. События информационной безопасности с систем-источников компании остаются в ее инфраструктуре.
2. После отключения от услуги сервис-провайдера у компании остается система сбора событий, которую можно использовать далее.

3. Загрузка интернет-канала при гибридном варианте значительно ниже, чем при облачном варианте подключения.

Даже при отключении от услуг сервис-провайдера регламенты, процедуры, отработанные с сервис-провайдером, можно использовать в рамках внутреннего Security Operations Center, собрав собственную команду аналитиков, администраторов и инженеров мониторинга. Также большинство аутсорсеров позволяют "выкупить" контент и помогают в нем разобраться. Таким образом, когда команда будет готова, наберется опыта в разборе и расследовании инцидентов, необходимо будет лишь перевести SIEM-систему под свой контроль и бесшовно продолжить мониторинг инцидентов.

Данный способ нивелирует риски неудачного взлета, обеспечивает мониторинг и разбор инцидентов здесь и сейчас и позволяет собрать команду и ввести ее в процесс плавно, не нарушая процессы информационной безопасности компании. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

При решении использовать гибридный SOC необходимо учитывать тенденции рынка и мнение компании, оказывающей аутсорсинговые услуги.

Если вы используете SOC as Service, то сразу решаете проблему персонала (как инженеров, так и аналитиков), наполнения контентом SIEM-системы, разработки регламентов и процессов взаимодействия при обнаружении, разборе и противодействии инцидентам – все задачи ложатся на плечи аутсорсера. При этом сервис-провайдер учитывает специфику компании и внутренние требования к организации процесса.

Кибератаки поражают малый и средний бизнес чаще и сильнее

Михаил Орленко, *руководитель департамента корпоративных решений Dell в России, Казахстане и Центральной Азии*

Если вы хотя бы поверхностно следите за новостями, то, вероятно, сможете назвать несколько крупных организаций, пострадавших за последние несколько месяцев от инцидентов безопасности или хищения данных. Это, например, компания British Airways[1] и Управление по делам иммиграции Австралии[2].

Обычно атаки, направленные на крупные организации, привлекают к себе большое внимание мировой прессы и СМИ, но в действительности они составляют всего несколько процентов случаев хищения данных, регистрируемых в течение года. На самом деле 71% атак с целью хищения данных[3] поражает средний и малый бизнес.

По частоте атак лидируют целевой фишинг и атаки типа Watering Hole.

Хищения данных влекут за собой непоправимые последствия для большинства средних и малых компаний.

Самые частые атаки

В 91% случаев кибератак[4] первым этапом является целевой фишинг. Традиционная фишинговая атака действует по сетевому принципу и предполагает рассылку электронных сообщений сотням и тысячам потенциальных жертв. Целевой фишинг нацелен на небольшую группу пользователей (обычно сотрудников компании, выбранных в качестве потенциальной жертвы).

Организатор целевого фишинга может создать почтовый аккаунт фиктивного сотрудника и рассылать запросы корпоративной информации настоящим сотрудникам компании. А они могут без дополнительной проверки предоставить запрашиваемую информацию, думая, что общаются с настоящим коллегой.

Когда осуществляется атака типа Watering Hole, хакеры встраивают вредоносное ПО в код часто используемого Web-сайта. Если какой-нибудь сотрудник компании заходит на этот сайт с рабочего компьютера, вся корпоративная сеть становится доступной для вируса, осуществляющего хищение данных.

Почему средний и малый бизнес подвергаются атакам

Технологии атак, используемые хакерами, развиваются параллельно со средствами и технологиями ИТ-безопасности. Хотя на серверах крупных организаций размещено больше ценных файлов, представляющих интерес для злоумышленников, есть несколько причин увеличения количества атак на малый и средний бизнес:

- SMB обычно недостаточно защищен.

Например, более половины предприятий в Великобритании[5] не принимает никаких превентивных мер для своей защиты от кибератак. Более того, 85% предприятий не планируют увеличивать свой бюджет на ИТ-безопасность, несмотря на увеличение количества инцидентов. Все это делает сегмент среднего и малого бизнеса особенно привлекательным для злоумышленников, которые любят легкую добычу.

- Вредоносное ПО используется все чаще, а оно действует без разбора.

Согласно исследованию[6], за прошлый год было обнаружено 37 млн уникальных образцов вредоносного ПО, что почти вдвое больше результата за 2013 г. Когда атаки с использованием такого ПО осуществляются косвенно через "бреши" (watering holes), нет ограничений, которые бы направляли вирус исключительно на крупные компании. Добавьте к этому тот факт, что SMB обычно имеет меньше средств защиты, и становится понятно, почему малые организации принимают на себя главный удар таких атак.

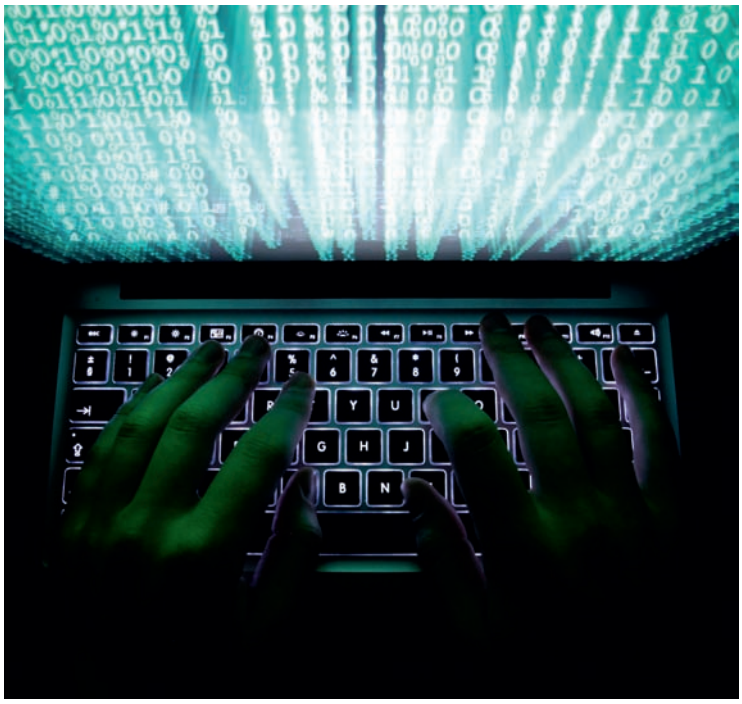
- SMB – трамплин для атак на крупные корпорации.

В конце 2013 г. хакеры получили номера банковских карт 40 млн клиентов из данных платежных терминалов сети супермаркетов Target, выкрав учетные данные у компании, поставлявшей холодильники и кондиционеры[7]. Этот инцидент не только стал крупнейшим случаем хищения данных в истории американской розничной тор-

[1] *http://www.csoonline.com/article/2903937/data-breach/british-airways-frequent-flyer-program-grounded.html.*
[2] *http://www.theguardian.com/world/2015/mar/30/personal-details-of-world-leaders-accidentally-revealed-by-g20-organisers.*
[3] *https://aerissecure.com/blog/smb-data-breach-fallout/.*
[4] *http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/.*
[5] *http://www.itproportal.com/2015/07/07/smbs-still-not-prepared-for-a-serious-data-breach/.*
[6] *http://www.sonicwall.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf.*
[7] *http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.*


КОМПЛЕКСНАЯ
НЕПРЕРЫВНАЯ
ЗАЩИТА ДАННЫХ
СЕГОДНЯ НА СЛУЖБЕ У ВАШЕГО БИЗНЕСА.
Уязвимость от кибер-атак растёт. Объем данных увеличивается.
Угрозы становятся все более изощренными и непредсказуемыми.
У компании Fortinet есть ответ - единое
интегрированное решение защиты сетевой инфраструктуры,
способное предотвращать существующие
и будущие атаки в реальном времени.
FORTINET®
Защита без компромиссов.
Copyright © 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet.

В конце 2013 г. хакеры получили номера банковских карт 40 млн клиентов из данных платежных терминалов сети супермаркетов Target, выкрав учетные данные у компании, поставлявшей холодильники и кондиционеры[7]. Этот инцидент не только стал крупнейшим случаем хищения данных в истории американской розничной торговли, но и напомнил всему миру, как злоумышленники могут использовать средние и малые компании с недостаточным уровнем ИТ-безопасности для доступа к данным крупных корпораций, которые эти последние обслуживают.



говли, но и напомнил всему миру, как злоумышленники могут использовать средние и малые компании с недостаточным уровнем ИТ-безопасности для доступа к данным крупных корпораций, которые эти последние обслуживают.

Непоправимые последствия

Большинство средних и малых предприятий просто не сможет пережить хищение данных. Подобные атаки сопряжены с большими расходами, а в случае невозможности восстановления данных средние и малые компании сталкиваются не только с репутационными, но и с операционными проблемами: 68% представителей SMB в Великобритании[8] не имеют плана обеспечения непрерывности бизнеса на случай хищения данных. В этом случае ставки исключительно велики, т.к. 60% средних и малых компаний вынуждены прекратить деятельность и закрыться в течение полугода после произошедшего хищения данных.

Добавьте к этим проблемам, что большая часть случаев хищения связана с кражей или потерей устройств[9], и станет ясно, что для средних и малых предприятий настало время серьезнее относиться к вопросам защиты данных.

Защита данных без снижения производительности работы

Средние и малые компании должны использовать свое важное преимущество – оперативность и мобильность. Специалисты средних и малых компаний часто озабочены тем, что усиление безопасности приведет к снижению производительности, т.к. пользователи будут вынуждены проходить сложные процедуры аутентификации.

Однако существуют способы, позволяющие обеспечить защиту от атак хакеров и хищения данных без наложения существенных ограничений на деятельность пользователей.

- Бесперебойное шифрование.

Сейчас можно обеспечить защиту данных независимо от места их хранения (на мобильных или настольных устройствах, внешних носителях или даже в публичном облаке) без затруднения доступа к ним пользователей. Благодаря бесперебойному шифрованию сотрудники компании могут использовать данные и совместно работать с ними, не испытывая неудобств из-за чрезмерных проверок безопасности или медленной загрузки данных.

- Расширенная аутентификация.

Расширенная аутентификация объединяет несколько форм аутентификации, чтобы обеспечить достоверность идентификации сотрудников для доступа к корпоративным данным. Компании могут комбинировать аппаратную аутентификацию, аутентификацию на базе учетных данных, централизованное удаленное управление и безопасный единый вход, чтобы сотрудники имели доступ только к той информации, которая им действительно необходима.

- Контейнеризация.

Современные системы предотвращения вредоносного ПО позволяют автоматически распознавать и блокировать вредоносные программы в корпоративной сети до их проникновения в сеть. Программы контейнеризации дают браузерам команду выполнять наиболее подверженные атакам приложения в виртуализированной среде. В этом случае даже при посещении сотрудником Web-страницы, пораженной вредоносной программой, эта программа не сможет атаковать ОС хоста. Кроме того, такие системы могут автоматически выявлять атаки, совершаемые на базе вредоносного ПО, используя для этого не сигнатуры вредоносных программ, а закономерности поведения, таким образом предотвращая распространение даже атак "нулевого дня".

Никогда еще в истории ИТ-отрасли средние и малые предприятия не подвергались столь высокому риску стать мишенью кибератак, а ставки сейчас высоки как никогда. Урок, которые многие средние и малые компании усваивают слишком поздно, заключается в том, что ценность превентивных систем обеспечения безопасности равна разнице между прочным будущим и стремительным уходом из бизнеса.

Возможно, такое заявление звучит излишне категорично, но статистика показывает, что поводов для беспокойства более чем достаточно. Оценивайте риски, информируйте своих сотрудников и вкладывайте средства в безопасность данных, чтобы ваша компания не стала еще одним назидательным примером для других средних и малых компаний. ●

Никогда еще в истории ИТ-отрасли средние и малые предприятия не подвергались столь высокому риску стать мишенью кибератак, а ставки сейчас высоки как никогда. Урок, которые многие средние и малые компании усваивают слишком поздно, заключается в том, что ценность превентивных систем обеспечения безопасности равна разнице между прочным будущим и стремительным уходом из бизнеса.

[8] *https://aerissecure.com/blog/smb-data-breach-fallout/.*
[9] *http://www.foxbusiness.com/features/2015/03/11/cyber-hacks-against-smbs-on-rise-what-can-do.html.*

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Управление корпоративной мобильностью: взгляд из России. Часть 2

Сергей Симонов, *главный специалист НИИ СОКБ*

В первой части данной статьи была рассмотрена концепция использования мобильных средств коммуникации, а также представлена характеристика продуктов группы "BrendName" – вендоров известных решений, выпустивших EMM-продукт, обеспечивающий возможность использования мобильных средств коммуникации (МСК) в информационных системах, основанных на их решениях.

Во второй части речь пойдет о еще двух группах игроков данного рынка управления корпоративной мобильностью: "Универсалах" и "Нишевых игроках". Будут рассмотрены тенденции зарубежного и особенности российского рынка EMM.

Ключевые игроки рынка EMM-решений 2015 года

"Универсалы"

Компании данной категории предлагают решения, которые можно использовать для управления МСК различных производителей, имеющих функционал, подходящий для решения типичных задач пользователей, обеспечивающих интеграцию с распространенными программными продуктами.

AirWatch

Основанная в 2003 г., быстро заняла лидирующее положение на рынке в своем сегменте благодаря решению для управления беспроводными устройствами. Его установка вариативна: на локальном сервере либо как облачный сервис.

Основной функционал решения включает средства управления e-mail, приложениями, контентом, браузерами.

Возможна интеграция с партнерскими продуктами, реализующими:

- Directory Services;
- Business Intelligence;
- PKI;
- Unified Communications;
- Network Access Control.

Реализованы сервисы самообслуживания пользователей, инструментарий для администрирования включает черные и белые списки, настройку профилей доступа и т.д.

Имеются клиентские модули для всех основных мобильных платформ, включая Android, iOS, BlackBerry, Symbian, Windows.

Особенности реализации функционала безопасности

Концепция обеспечения безопасности данного продукта – обеспечение безопасности взаимодействующих объектов на разных уровнях, включая оборудование, пользователей, контент, данные, e-mail, сетевую инфраструктуру. Решение интегрировано с AD или LDAP, реализует правила доступа в соответствии с политикой безопасности. Возможно использование дополнительных средств: усиленной криптографии, удаленное уничтожение контента и обеспечение его безопасности – AirWatch Content Locker.

Good Technology

Компания специализируется на безопасных мобильных решениях для бизнеса, финансового и правительственного секторов. Декларируются цели обеспечения защиты информационных ресурсов предприятия, мобильных устройств и хранимых данных.

Good Technology ввело контейнеризацию приложений. Криптографическая защита и логическое разделение приложений и данных позволяют надежно разделить корпоративные и личные данные и приложения.

Приложение интегрирует функционал MDM, MAM, MCM и ориентировано на использование банка приложений App Store.

Особенности реализации функционала безопасности

Обеспечивается End-to-End Security для приложений, данных.

Функционал:

- App Authorization;
- App-Level Encryption;
- App Authentication;
- Single Sign-on;
- Strong Password Enforcement;
- Remote Lock/Wipe;
- Data Loss Prevention;
- Secure Corporate Access Behind Firewalls.

MobileIron

EMM-решение представлено на рынке с 2007 г. Возможны варианты реализации архитектуры как облачного сервиса или с использованием серверного оборудования заказчика. Данное решение предоставляет сервисы управления приложениями, контентом, МСК различных типов. Имеются средства автоматизации конфигурирования клиентского ПО, интеграции в различные системы безопасности.

MobileIron – устройства разных производителей, но основной фокус сделан на iOS, Android, Windows.

Приложение предоставляет функционал MDM, MAM, MCM.

MAM обеспечивает управление доступом к App Store (Apps@Work) и контейнеризацией приложений и данных.

MCM (Docs@Work) предоставляет защищенные e-mail и браузер для доступа к корпоративным ресурсам.

Особенности реализации функционала безопасности

Представлены средства для криптографической защиты данных, паролей, использования строгой аутентификации, DLP уровня приложений, оценка их репутации и безопасного

EMM (Enterprise Mobility Management) – управление корпоративной мобильностью.

МСК – мобильных средств коммуникации.

EMM предполагает рассмотрение комплекса вопросов интеграции МСК в корпоративные бизнес-процессы, обеспечения ИБ, поддержки пользователей этих устройств (ПО, инфраструктура, технологии, обеспечивающие возможность интеграции МСК в корпоративные информационные бизнес-процессы).

"Магический квадрант для EMM-решений" от Garner, динамика игроков рынка за 2 года

В соответствии с периодически проводимыми исследованиями аналитической компании Garner рынок EMM-решений характеризуется ростом более 20% в год, в абсолютных цифрах – продажи в 2014 г. составили $1,4 млрд (оценка компании IDC). На рынке наблюдается значительная фрагментация, происходит активный передел данного сегмента рынка (рис. 1).

взаимодействия без использования VPN с использованием Web@Work.

"Нишевые" игроки

В исследовании Gartner (2015 г.) присутствуют 3 игрока данной категории: BlackBerry, LANDesk, Globo.

BlackBerry

Типичным "нишевым" игроком можно назвать компанию BlackBerry, известного производителя одноименных МСК и EMM-решений для МСК этого типа.

MDM-система использует BlackBerry Enterprise Service (BES), поддерживает управление устройствами на BlackBerry® OS и BlackBerry® 10, Android™ и iOS (смартфоны и планшеты).

Корпоративная служба ИБ (администратор) может устанавливать ограничения (задавать бизнес-профиль МСК), контролировать работу приложений, удаленно стирать данные и ПО, осуществлять целый ряд административных действий.

Особенности реализации функционала безопасности

На МСК реализовано разделение рабочего и личного пространства.

Реализован широкий функционал, позволяющий реализовать различные требования: от базового уровня до повышенного уровня безопасности и контроля, требуемого правительством и регламентами отраслей промышленности.

Данная EMM может быть использована для реализации концепций COPE и BYOD.

Существенной особенностью является то, что система управления размещена на серверах компании BlackBerry.

LANDesk Software

В 2012 г. компания LANDesk приобрела поставщика специализированного ПО для МСК и систем устройств – компанию Wavelink, – позже, в 2014 г., – компанию LetMobile, специализирующуюся на решениях по безопасности для мобильных устройств.

LANDesk Mobility Manager – Wavelink Avalanche – ПО для управления телефонами, планшетами, штрих-сканерами и другими системами, имеющими свои ОС. Включает центр мобильности, консоль управления для контроля и настройки МСК и систему дистанционного управления в интегрированной системе. Кроме того, компания предлагает продукты класса MAM – ПО управления операциями на складе (продукт Wavelink) и решение по обеспечению безопасности почтовой корреспонденции и ее разделения на корпоративную и личную LANDesk Secure Mobile E-mail (продукт разработки LetMobile).

Особенности реализации функционала безопасности

Wavelink Avalanche включает в себя агент безопасности для Windows CE и обеспечивает возможность установки усиленного режима безопасности в целях постоянной защиты МСК и данных от несанкционированного доступа.

Тенденции зарубежного рынка EMM

Тенденция EMM со стороны зарубежных потребителей – смягчение жестких правил в направлении большего удобства для пользователя. Изменения происходят в правилах ИБ (политика ИБ для МСК), системе управления устройствами, приложениями. Больше внимания уделяется безопасности в интересах как пользователя, так и компании. Как следствие – большинство продуктов подходит для реализации концепции BYOD.

Из представленных в обзоре продуктов только для двух явно указано, что они применимы для реализации обеих концепций, COPE и BYOD: это решения Symantec и BlackBerry.

Особенности российского рынка EMM

Требования, предъявляемые корпоративными потребителями EMM-решений на российском рынке, отличаются от требований зарубежных потребителей.

С позиции службы ИБ российских крупных корпоративных потребителей при использовании мобильных устройств в бизнес-процессах необходимо учитывать, что:

- МСК не являются доверенными устройствами: ОС и прикладное ПО могут иметь недекларированные возможности (НДВ);
- встроенные средства защиты должны соответствовать отечественным требованиям и быть сертифицированными;
- на мобильных устройствах разных производителей могут быть установлены различные ОС (Android, iOS, BlackBerry OS…), к тому же и разных версий; встроенные механизмы безопасности МСК имеют разную функциональность;
- серверная часть EMM-решений не должна включать в свой состав серверы-посредники сторонних вендоров.

С учетом этих факторов, а также ряда требуемых нормативных документов в части защиты информации:

1) предпочтительно использовать отечественные EMM-решения, учитывающие особенности требований российской нормативной базы;

2) при использовании МСК в корпоративных бизнес-процессах целесообразно использовать концепцию COPE.

Эти тезисы подтверждает статистика внедрений EMM-решений в России: более половины внедрений приходится именно на отечественные продукты. Все отечественные EMM-решения относятся к категории "нишевых" и учитывают специфику требований определенных групп заказчиков.

В следующей статье рассматривается пример российского EMM-решения – SafePhone PLUS. ●

Литература

1. Колесов А. Управление корпоративной мобильностью. Взгляд Gartner (14.07.2015) [online]. Доступ через http://www.pcweek.ru/mobile/article/detail.php?ID=175881.

2. Mobile Device Management (MDM). Enterprise Mobility Management (EMM). Управление мобильными устройствами [online]. Доступ через http://www.tadviser.ru/index.php/Статья:Mobile_Device_Management_(MDM)_Управление_мобильными_устройствами_Enterprise_Mobility_Management_(EMM).

3. Hess K. 10 Enterprise Mobility Management Solutions: Beyond MDM [online]. Доступ через http://mobile.datamation.com/mobile-wireless/10-enterprise-mobility-management-solutions-beyond-mdm-1.html Posted 2015. – April, 22.

SafePhone PLUS на страже коммуникаций

Сергей Симонов, *главный специалист НИИ СОКБ*

SafePhone PLUS – решение, разработанное для защиты корпоративной системы коммуникаций. В число его задач входят:
- защита мобильного устройства и информации, хранящейся на нем, от несанкционированного доступа;
- обеспечение защищенного доступа с МСК к корпоративным ресурсам;
- конфиденциальный обмен данными;
- обеспечение безопасности телефонных переговоров и безопасной видеоконференцсвязи на мобильных устройствах;
- реализация возможностей интеграции с другими корпоративными системами (СКУД, SIEM, УАТС и др.).

Решение построено на базе системы SafePhone от компании "НИИ СОКБ" для защиты информации на корпоративных мобильных устройствах и каналов связи передачи информации ViPNet от компании "ИнфоТеКС". На мобильном устройстве функционируют клиентские программы SafePhone, ViPNet и SIP-клиент, а на контролируемой территории предприятия – серверные компоненты этих систем: SafePhone Server, ViPNet Coordinator Server SIP.

В состав SafePhone PLUS входят 2 компонента:

1. SafePhone – система защиты информации на корпоративных мобильных устройствах с централизованным управлением.

Функции SafePhone

- Защита от несанкционированного доступа к конфиденциальной информации.
- Предотвращение несанкционированной установки стороннего ПО.
- Ведение банка доверенного программного обеспечения.
- Контроль использования служебных мобильных устройств.
- Применение различных политик безопасности на территории предприятия и за ее пределами.
- Мониторинг событий и подготовка отчетов.

Система SafePhone сертифицирована ФСТЭК России и позволяет построить систему защиты информации на корпоративных мобильных устройствах, обеспечивает централизованное управление парком мобильных устройств и защиту от утечки информации с них. Решение соответствует требованиям безопасности.

2. Mobile VoIP: обеспечивает корпоративную голосовую связь по каналам Интернета или локальным сетям.

Функциональное назначение

- Обеспечение возможности ведения конфиденциальных переговоров по мобильному устройству с мобильными и стационарными абонентами.
- Снижение затрат на оплату трафика.
- Предоставление корпоративным абонентам доп. услуг.
- Переадресация звонков.
- Конференц-связь, видеоконференция.
- Обмен текстовыми и медийными сообщениями по защищенному каналу.
- Единый номер в корпорации (в рамках интеграции с УПАТС).

Программный комплекс ViPNet Client, входящий в Mobile VoIP, имеет сертификат соответствия ФСБ России, удостоверяет соответствие требованиям к СКЗИ класса КС1.

Наличие "сертификатов соответствия" позволяет использовать SafePhone PLUS не только для защиты коммерческих секретов, но и в государственных ИС, а также в информационных системах ПДн.

NM
АДРЕСА И ТЕЛЕФОНЫ ООО "НИИ СОКБ" см. стр. 56

Анализ рисков ИБ в корпоративной среде

Денис Макрушин, *антивирусный эксперт "Лаборатории Касперского"*

Любая компания, вне зависимости от уровня своей зрелости, обладает какой-либо чувствительной информацией, нелегитимная манипуляция которой может привести к прямым или косвенным финансовым потерям. Внедрение ИТ в фундамент бизнес-процессов ведет к "оцифровке" практически всех активов организации, и словосочетание "информационная безопасность" начинает плотнее входить в повседневную жизнь ее сотрудников.

Бизнес понимает последствия проблем защищенности своих информационных ресурсов и готов осуществлять внушительные инвестиции в продукты обеспечения ИБ и соответствующие квалифицированные кадры. Регулярные оповещения об очередной утечке, вызванной уязвимостью в инфраструктуре Web-приложения или инсайдером компании, периодически отрезвляют топ-менеджмент, и он, в свою очередь, выделяет бюджет для соответствующих мер. Однако ИБ это довольно абстрактное для руководящего персонала состояние информационных активов, и в связи с этим индустрии ИБ приходится вводить определенные метрики этого состояния и впоследствии на них опираться. И вот именно такой метрикой выступают риски: компраментации, потери репутации и денег.

Если взглянуть на процедуру реализации политики ИБ с "высоты птичьего полета", то рождается мысль об унификации ПО, предназначенного для защиты информации.

Системный менеджмент – технология централизованного управления комплексной системой ИБ.

Attributes / Methods	Risk identification	Risk Analysis	Risk Evaluation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only) (information assessed in June 2006)	Size of organization	Skills needed*	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	••	•	•	•••	•••	•••	•••	DE	Free	All	**	N	N	Prototype (free of charge)
Cramm	•••	•••	•••					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	•••	•••	•••					NL	Free	All	*	N	N	
Ebios	•••	•••	•••	•••	•••	•••	•••	EN, FR, DE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	•••	•••	•••	•••	•••	•••	•••	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	••	••	••	••	•••	•••	•••	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	•				•			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001					•	•		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	•••	•••	•••	•••	•••	•••	•••	EN, DE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	•••	•••	•••					EN, FR	Not free	Large	*	N	N	
Mehari	•••	•••	•••					EN, FR	€100-500	All	**	N	N	RISICARE
Octave	••	••	••	••	••	••	••	EN	Free	SME	**	N	N	
SP800-30 (NIST)	•••	•••		•••	•••	•••		EN	Free	All	**	N	N	

Таблица методик оценки рисков информационной безопасности

Методики анализа рисков

Анализ рисков ИБ – это, прежде всего, процесс, входящий в непрерывную процедуру защиты информации. Комплекс мероприятий по оценке состояния защищенности инфраструктуры, в которой осуществляется манипуляция чувствительной для бизнеса информацией. Организация данного процесса описывается в нормативных документах, а также документах, носящих рекомендательный характер. Здесь все зависит от конкретного вида деятельности компании.

Стандарты ИБ, в нормативном или рекомендательном характере описывающие защиту информации для различных отраслей бизнеса, практически всегда ссылаются на авторитетные методики анализа рисков (ISO/IEC IS 27001, NIST и т.п.). Европейская организация ENISA* составила интересный материал, в котором содержится таблица методик оценки рисков и оценивается полнота описания процедур для различных аспектов риск-менеджмента (см. рис.).

Политика ИБ

Документом, резюмирующим весь комплекс процедуры управления ИБ-рисками, является… Нет, не формальный отчет о ее проведении, а фактически политика ИБ, в которую внесут соответствующие поправки, учтут всевозможные недостатки в технических и организационных составляющих бизнес-процессов целевой организации. На основе отчетности анализа рисков строится картина "непаханного поля" всевозможных угроз, подавляющее большинство которых ложится на ИТ. Ознакомившись с подобным отчетом, руководящий состав делает выводы об объемах инвестиций, направленных на построение или модернизацию автоматизированной системы защиты информации. Для этого команда экспертов определяет то множество рисков, которые можно минимизировать программно-аппаратными средствами.

Эксплуатация уязвимостей в корпоративном Web-приложении, перехват конфиденциальных данных, передающихся по каналам связи в открытом виде, внедрение сторонних аппаратных средств в информационную среду с последующим копированием чего-либо, не предназначенного для ознакомления третьими лицами, – все это заставляет администраторов ИБ разворачивать корпоративные версии разноплановых продуктов, тратить временные ресурсы на их конфигурирование и, что самое трудоемкое, проводить аудит получившийся системы.

Вывод

Процесс "Анализ рисков ИБ – Подготовка отчета – Создание/модернизация политики ИБ – Развертывание программно-аппаратных средств" является непрерывным и значительным образом опирается на системный менеджмент. Интегрированная платформа, на которой будет разворачиваться совокупность программных решений, позволит существенно ускорить процедуру минимизации рисков при косвенных плюсах, которые она за собой тянет. Унификация интерфейсов управления приведет к сокращению человеческих и временных ресурсов на аудит ИБ постоянно растущей инфраструктуры, при этом свойство интегрированности средств защиты поможет компании минимизировать риски в кратчайшие сроки за счет широкого спектра компонентов, отвечающих за устранение источников различных угроз, характерных для ИТ-инфраструктур практически любых масштабов. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

* *http://www.enisa.europa.eu*

Современные технологии контроля привилегированных пользователей

Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*
Михаил Романов, *директор по развитию бизнеса ООО "Новые технологии"*

На сегодняшний день вопросы обеспечения информационной безопасности являются актуальными для организаций любых масштабов и видов деятельности. Необходимо отметить, что большинство современных компаний достаточно хорошо защищены от внешних атак из сети Интернет за счет использования межсетевых экранов, антивирусов, систем IPS/IDS и др. Защита же от внутренних угроз направлена, как правило, на обычных пользователей информационных систем, а администраторы и привилегированные пользователи сторонних организаций, как правило, остаются без надлежащего контроля.

Это создает особую категорию угроз безопасности, связанных с умышленными или неумышленными действиями этой категории пользователей. Высокий уровень опасности подобного рода угроз обусловлен тем, что привилегированные пользователи зачастую имеют максимальный уровень доступа. Кроме этого, необходимо отметить, что 100% привилегированных пользователей – технически грамотные и хорошо подготовленные специалисты, обладающие максимумом возможностей, что потенциально может поставить под угрозу конфиденциальность, целостность и доступность информационных ресурсов компании. Именно поэтому необходимо контролировать и ограничивать доступ суперпользователей, а также иметь возможность ретроспективного анализа их действий для выявления и расследования инцидентов.

В настоящее время на рынке информационной безопасности существуют специализированные программные и программно-аппаратные решения для постоянного контроля учетных данных привилегированных пользователей в сети и достоверного учета их использования. В использовании такого рода решений могут быть заинтересованы не только подразделения ИБ, но и ИТ. Это связано с сокращением трудозатрат сотрудников ИТ-служб, поскольку появляется возможность оперативно предоставлять пароли пользователям по первому требованию и отпадает необходимость в трудоемком ручном поиске, изменении и учете записей. Кроме того, они позволяют полностью контролировать выполнение всех правил и политик ИБ привилегированными пользователями, упрощают расследование инцидентов, предоставляют неопровержимые доказательства, обеспечивают полный контроль рабочих процессов пользователей, а также исключают скрытую активность.

Контроль суперпользователей

В прошлом году в России появилась первая отечественная система контроля привилегированных пользователей – SafeInspect, которая представляет собой полнофункциональную платформу для эффективного контроля за суперпользователями, административными учетными записями и сессиями в информационных системах.

Решение дает возможность контролировать каналы SSH, RDP, HTTP/HTTPs, Telnet и др., которые используются для администрирования серверов и сетевых устройств. Весь трафик (включая изменения конфигурации, выполненные команды) записывается в журнал и архивируется. При возникновении проблем (ошибок в конфигурации сервера, манипулирования с базой данных или аварийного отключения) информация о них сразу же отображается в отчетах. Таким образом, можно легко определить причину данных инцидентов и предпринять соответствующие действия.

Любые действия привилегированных пользователей аудитор получает в виде видеозаписи, воспроизводящей работу конкретного привилегированного пользователя, что позволяет намного быстрее и точнее найти причину инцидента.

С помощью системы SafeInspect можно контролировать не только внутренние соединения, но и внешние подключения к своим ресурсам со стороны подрядчиков, а также доступ к облачным ресурсам. При помощи системы можно сохранить все действия несанкционированных пользователей, а также проанализировать методы, используемые при таких видах доступа, чтобы потом можно было усовершенствовать систему безопасности.

Система в своем основном режиме работает без агентов, что позволяет очень быстро ее развернуть и настроить (10–20 мин. – и можно контролировать все подключения). Для использования не требуется каких-либо существенных изменений в ИТ-инфраструктуре и сетевой среде.

В заключение необходимо отметить, что использование специализированных решений для контроля привилегированных пользователей позволяет существенно повысить уровень информационной безопасности организации за счет снижения рисков внутренних угроз.

На российском рынке ИБ можно выделить три наиболее популярных западных системы контроля привилегированных пользователей – Balabit, CyberArk и Wallix.

NM
АДРЕСА И ТЕЛЕФОНЫ АО "ДИАЛОГНАУКА" см. стр. 56

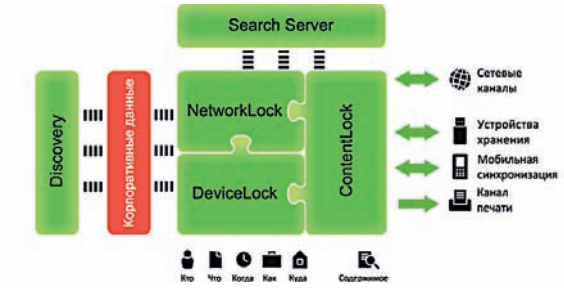
DeviceLock DLP

как инструмент выполнения некоторых требований стандарта СТО БР

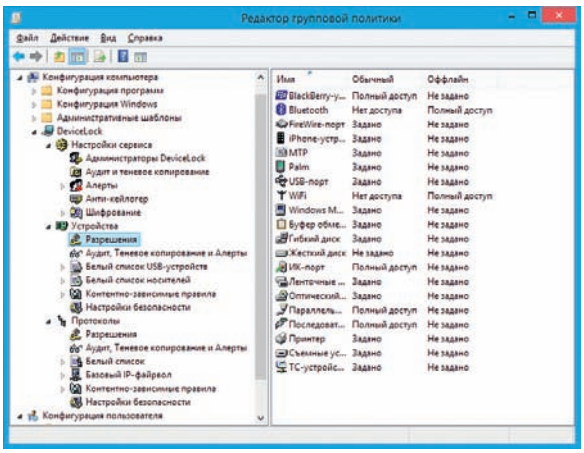
Информация сейчас является основным активом, особенно в финансовой сфере. Это подчеркивают и регуляторы, которые все чаще начинают требовать от организаций и банков соблюдения требований информационной безопасности, то есть обеспечения защиты банковской информационной системы. Среди этих требований есть и контроль за утечками информации, и контроль действий сотрудников, и протоколирование происходящих в информационной системе событий. Эти функции вполне могут выполнить современные DLP-продукты, такие как DeviceLock.

НСД – это несанкционированные действия, а НРД – нерегламентированные действия в рамках предоставленных полномочий, то есть НСД – это внешние нападения, а НРД – внутренние.

Например, в готовящемся стандарте Банка России по информационной безопасности некредитных финансовых организаций СТО БР ИБНФО есть такое требование – обеспечить "защиту от НСД и НРД, управление доступом и регистрацией всех действий в АС НФО РФ". Кроме того, это требование предполагает не только управление доступом, что обеспечивает, как правило, сама автоматизированная система, но и регистрацию всех действий пользователей, что сложно сделать в рамках прикладной системы или приложения. Для этого нужно использовать специальное дополнительное средство мониторинга всех действий пользователя, его обращений к файловой системе и использование сетевого взаимодействия.



Программный комплекс DeviceLock DLP Suite



DeviceLock DLP Suite. Контроль доступа к устройствам и интерфейсам

Теневое копирование позволяет максимально подробно регистрировать действия сотрудников в автоматизированной системе для дальнейшего анализа и проведения расследования. NetworkLock позволяет максимально подробно контролировать действия пользователей в том числе и в экзотических системах типа Lotus Notes, а также в различных облачных сервисах, причем с поддержкой локальных сервисов типа Яндекс.Диск или web.de.

Мониторинг

Именно этим занимается решение компании SmartLine с названием DeviceLock DLP Suite. Это модульное решение, которое состоит из следующих компонентов:

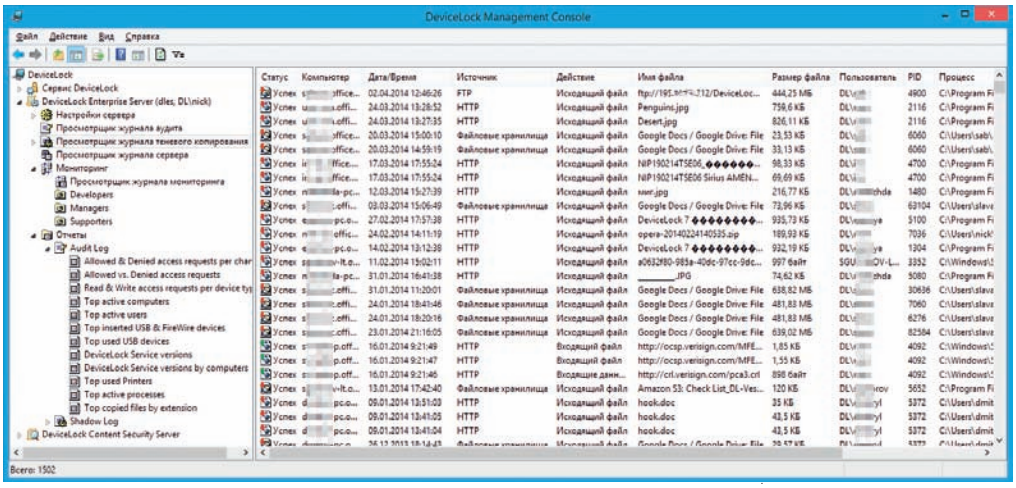
- DeviceLock Base. Это базовый компонент, который реализует все функции централизованного управления и администрирования другими компонентами комплекса, а также сбор данных в центральное хранилище. Этот компонент является базовым и требует установки на каждое рабочее место собственного агента. Центральный сервер обеспечивает сбор данных с агентов, событийное протоколирование (аудит) и теневое копирование данных для всех локальных каналов ввода-вывода на защищаемых компьютерах, включая периферийные устройства и интерфейсы, системный буфер обмена, локально подсоединенные смартфоны и другие мобильные устройства, а также канал печати документов на локальные и сетевые принтеры. При этом ядро сохраняет сведения о контексте взаимодействия и имеет необходимый набор механизмов контекстного контроля доступа пользователей, который минимизирует ложные срабатывания.
- NetworkLock. Этот компонент обеспечивает контекстный контроль каналов сетевых коммуникаций на рабочих компьютерах, включая распознавание сетевых протоколов независимо от используемых портов, детектирование коммуникационных приложений и их выборочную блокировку, реконструкцию сообщений и сессий с восстановлением файлов, данных и параметров, а также событийное протоколирование и теневое копирование передаваемых данных.
- ContentLock. Модуль реализует механизмы контентного

анализа, циркулирует в компании информации и фильтрации файлов и данных, передаваемых с/на сменные носители, и в каналах сетевых коммуникаций – Web-почте и социальных сетях, службах мгновенных сообщений, файловом обмене по протоколам FTP и FTP-SSL и др. Кроме того, технологии контентной фильтрации в модуле ContentLock позволяют задать фильтрацию для данных теневого копирования, чтобы снизить количество ложных срабатываний для эффективного решения задач аудита информационной безопасности, расследований нештатных ситуаций и их криминалистического анализа.

- DeviceLock Discovery. Компонент проводит сканирование рабочих станций и корпоративных сетевых ресурсов и на основании заданных политик обнаруживает документы и файлы с критическим содержимым, осуществляет различные опциональные действия с обнаруженными документами, а также может инициировать процедуры управления инцидентами, направляя тревожные оповещения в реальном режиме времени, если конфиденциальная информация обнаружилась в неположенном месте.
- DeviceLock Search Server (DLSS). Он обеспечивает полнотекстовый поиск по централизованным базам данных теневого копирования и событийного протоколирования DeviceLock. Сервер DLSS позволяет значительно снизить трудозатратность и повысить эффективность процессов аудита и расследования инцидентов информационной безопасности, связанных с утечками информации, их криминалистического анализа и сбора доказательной базы.

В целом же DeviceLock DLP Suite сильно расширяет возможности контроля администратора за действиями пользователей. Если встроенные правила доступа для приложений и платформ ограничены только ими, то средства контроля модуля ContentLock позволяют устанавливать сложные правила контроля доступа и регистрации событий.

Обычно операционные системы и базы данных не контролируют контент действий пользователя, в то время как правила DeviceLock позволяют сотрудникам отдела ИБ пользоваться не только стационарными правами доступа, но и так называемыми контентно-зависимыми правилами. Это позволяет добиться с помощью DeviceLock высочайшего уровня детализации в контроле устройств и сетевых протоколов, которого невозможно достигнуть стандартными средствами групповых политик Windows. Причем обеспечивается он с помощью интерфейса, прозрачно интегрируемого в редактор групповых политик Windows Group Policy Editor, что позволяет легко управлять контролем доступа в больших корпоративных сетях.

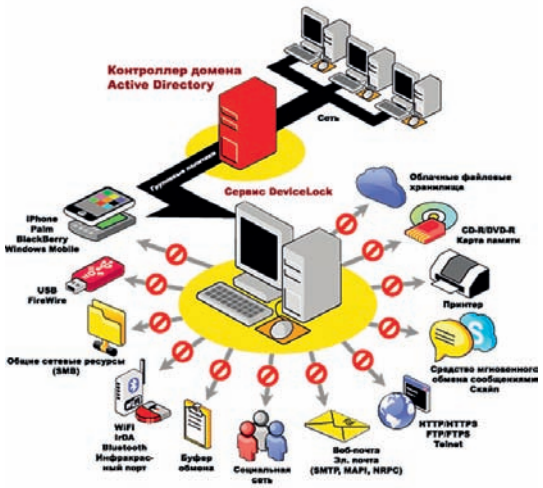


Теневое копирование

Теневое копирование

Отдельно стоит упомянуть о такой функции DeviceLock, как теневое копирование с возможностью анализа накопленных данных с помощью DLSS. Этот функционал позволяет не просто фиксировать действия пользователей в системе, что может делать и система Syslog, но также передавать на центральный сервер информацию, с которой работал пользователь и которую он попытался вынести из компании с помощью накопителя или в виде бумажной копии. Эти данные также собираются в хранилище и могут быть в дальнейшем проанализированы с помощью DLSS.

Таким образом, DeviceLock является уникальным инструментом для удовлетворения требований Центрального банка РФ и других регуляторов. При этом он является модульным продуктом, что позволяет постепенно наращивать функциональность защиты по мере необходимости.



Компонент DeviceLock Search Server (DLSS)

Обязательным компонентом является только само ядро DeviceLock Base, к которому в любой момент можно добавить модули сетевого мониторинга NetworkLock, контент-анализа ContentLock, поиска мест хранения конфиденциальной информации DeviceLock Discovery и сервера анализа теневых копий и системных записей DeviceLock Search Server. Модульный подход позволяет постепенно наращивать функциональные возможности DLP-системы DeviceLock DLP Suite. ●

DDoS-атака как метод конкурентной борьбы

Евгений Горбачев, *начальник управления информационной безопасности, Департамент по обеспечению безопасности, Банк Москвы.*

DDoS-атака – это ничем не регламентированное, ограниченное только фантазией злоумышленников, вредоносное воздействие на сетевой ресурс. Атака может быть простой (маломощной), сверхмощной (превышающей пределы мощностей Центров фильтрации) или комбинированной ("интеллектуальной").

Для начала можно привести ряд общих фактов для понимания масштабов того, чему мы пытаемся противостоять. Если не брать определение DDoS-атаки в классическом ее варианте, то можно сказать так: DDoS-атака – это ничем не регламентированное, ограниченное только фантазией злоумышленников, вредоносное воздействие на сетевой ресурс. Атака может быть простой, сверхмощной или комбинированной.

Последние используются атакующими чаще, являются наиболее эффективными и полностью выводят из строя атакуемый ресурс. При таких атаках нелегитимные запросы маскируются под легитимные, и отделить их от настоящих запросов пользователей в Центре фильтрации крайне затруднительно.

Понятно, что эволюция атак менялась со временем, но разные по типу и мощности атаки приводят к одним и тем же последствиям – вывод из строя важного бизнес-сервиса.

При регулярных атаках, как правило, происходит постоянное "соперничество" между атакующими и защищающимися, а защитная система должна уметь подстраиваться так, чтобы фильтровать трафик в постоянно меняющихся условиях.

При этом нужно понимать, что злоумышленники могут:

- Изменять (усовершенствовать, усложнять) алгоритмы атаки таким образом, чтобы сделанные ранее настройки фильтрации оказались неэффективными.
- Применять минимальные мощности атак, необходимые для вывода ресурса из строя. Когда, например, у злоумышленников есть возможность проведения атаки мощностью 60 Гбит, они используют только часть своих мощностей, т.к. для успешной атаки достаточно и 3 Гбит. Но после усиления защиты организации, например с 3 до 6 Гбит, злоумышленники просто поднимут мощность и продолжат выводить ресурсы из строя.
- Использовать комбинированные методы атак, подстраиваясь под легитимный трафик. При этом атака необязательно может быть мощной.

Не существует средства защиты, способного единожды подстроиться под атаку, натренироваться и в дальнейшем избегать последствий путем "быстрого переключения в режим фильтрации".

Если атаки разнятся по своим характеристикам, то в каждом случае инженерам придется находить новые пути защиты. Защита от DDoS требует постоянной работы и обучения со стороны защищаемого.

Объекты атаки

Ими становятся ресурсы, использующие Интернет. Как правило, это внешняя почта, сайт организации, банкоматы, IP-телефония, и т.д. При этом основной непосредственный ущерб – отказ в обслуживании конкретного сервиса, а косвенный – недополученная прибыль от простоя этого сервиса либо мошеннические действия "под прикрытием".

Интернет-магазины

Особенно остро проблемы от DDoS-атак на себе будут ощущать те организации, чья деятельность непосредственно связана с продажей тех или иных товаров или услуг через Интернет, а минимальные простои, даже самые незначительные, могут привести к оттоку клиентов на другие, работающие сайты в этой сфере. Это зачастую идет на руку их конкурентам.

По данным "Лаборатории Касперского", каждая шестая российская компания в 2015 г. подвергалась DDoS-атаке, а сама страна оказалась в первой пятерке государств, чьи интернет-ресурсы вызывали наибольший интерес у киберзлоумышленников. Об этом свидетельствуют не только результаты исследования*, проведенного "Лабораторией Касперского", но и внутренняя статистика компании. В общей сложности в прошлом году эксперты "Лаборатории Касперского" зарегистрировали более 120 тыс. атак, которые были направлены на интернет-ресурсы в 96 странах мира.

В России киберпреступники чаще всего атаковали компании среднего и крупного бизнеса – от DDoS-инцидентов пострадало соответственно 20% и 17% организаций. Однако микробизнес также не остался без внимания: 12% компаний, принявших участие в опросе*, с численностью персонала до 25 человек испытали на себе последствия DDoS-атак.

Атакующие старались вывести из строя не только лишь общедоступный сайт организации, хотя эта цель, безусловно, была в приоритете – 55% DDoS-атак были направлены именно на официальный Web-портал компании. Тем не менее, треть инцидентов затронула коммуникационные сервисы

**Исследование "Информационная безопасность бизнеса", "Лаборатория Касперского" и B2B International, Россия, 2015.*

Эволюция атак менялась со временем, но разные по типу и мощности атаки приводят к одним и тем же последствиям – к выводу из строя важного бизнес-сервиса.

(прежде всего почтовые), в 23% случаев пострадали страницы, предназначенные для клиентов компании, 18% атак были нацелены на файловые серверы, а еще 12% – на сервисы для совершения финансовых операций.

При этом довольно часто DDoS-атака осуществлялась одновременно с другой кибератакой, в которой использовалось вредоносное ПО, или же она служила прикрытием для кражи ценных данных. О подобных двойных инцидентах заявили 59% российских компаний, участвовавших в опросе "Лаборатории Касперского".

В результате DDoS-атак скорость загрузки Web-страниц значительно замедлялась у половины пострадавших организаций. Однако четверть компаний, столкнувшихся с этой угрозой, имела дело с более неприятными последствиями: DDoS-атаки полностью нарушили работоспособность сервисов или же стали причиной сбоя финансовых транзакций.

Банки и кредитные организации

Что касается финансовой сферы, то по имеющейся у нас информации, ежегодно DDoS-атакам подвергается каждый второй банк в России, а крупные банки – по нескольку раз в год. Таким образом, в среднем на долю банков приходится по 0,7 атак в год на каждый банк в России. Что касается Банка Москвы, то за 2015 г. нами зафиксировано 6 DDoS-атак, которые были успешно отражены и не привели к нарушению работоспособности ресурсов банка.

В последнее время можно констатировать факт увеличения числа и мощности атак на банки в целом, что в очередной раз подтверждает острую необходимость использования эффективных и профессиональных систем противодействия.

Защита от DDoS

Стоимость зарубежных систем фильтрации может достигать значений, многократно превышающих прибыль организаций от предоставления услуг, связанных с сетью Интернет. Поэтому очень важно подходить с умом к выбору методов защиты от угроз подобного типа. Сегодня, например, на российском рынке много компаний и провайдеров, предлагающих средства защиты от DDoS-атак, ничем не уступающие западным аналогам.

Понятно, что крупные организации всегда защищаются от подобных угроз. Кто-то покупает и настраивает собственное оборудование, держит в штате специалистов, кто-то идет по пути заключения договора на поставку услуг очистки трафика со специализированной компанией, а кто-то использует комбинированные методы защиты.

Более сложно дела обстоят с небольшими компаниями – малым бизнесом. Как это по-русски: "Нас не трогали, и зачем нам защищаться…". Но все когда-то случается в первый раз, и здесь важно оценить все "за" и "против". В любом случае, защищаться или нет – выбор конкретной организации. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Не существует средства защиты, способного единожды подстроиться под атаку, натренироваться и в дальнейшем избегать последствий путем "быстрого переключения в режим фильтрации".

В России киберпреступники чаще всего атаковали компании среднего и крупного бизнеса – от DDoS-инцидентов пострадало соответственно 20% и 17% организаций. Однако микробизнес также не остался без внимания: 12% компаний, принявших участие в опросе*, с численностью персонала до 25 человек испытали на себе последствия DDoS-атак.

Комментарий эксперта

Константин Коротнев,
руководитель информационной безопасности, CISSP, CISA, "Эльдорадо"

"Эльдорадо" занимает лидирующие позиции по обороту интернет-магазина среди крупных федеральных ритейлеров бытовой техники и электроники. Оборот интернет-площадки занимает значительную долю в общем обороте компании. В связи с этим интернет-магазин становится не только онлайн-каталогом для поддержки продаж традиционных розничных магазинов, но и отдельным критичным направлением деятельности компании, которое, кроме этого, еще и демонстрирует наиболее динамичный рост. Все это повышает рискообразующий потенциал интернет-магазина и делает его привлекательным для злоумышленников, которые осуществляют различные виды атак.

В процессе управления рисками ИБ мы регулярно оцениваем в деньгах риски ИБ для бизнеса. С ростом актуальности атак на интернет-магазин и ростом его ценности для бизнеса риски ИБ для этого ценного актива растут пропорционально. При этом DDoS-атаки можно выделить в отдельный тип атак, при успешной реализации которых фактически останавливается функционирование интернет-канала продаж компании "Эльдорадо". Таким образом, DDoS-атаки могут нанести прямой ущерб бизнесу, делая невозможным для компании зарабатывать деньги на продажах через интернет-магазин.

Предотвратить возникновение атак мы не можем, так как не имеем возможности влиять на злоумышленников, реализующих их. Но для снижения влияния атак на интернет-магазин мы используем специализированные средства защиты. Если говорить о статистике атак, то за прошедший год общая продолжительность успешно отраженных DDoS-атак составила около 10 суток, и в случае отсутствия средств защиты в такой период времени наши покупатели не смогли бы пользоваться услугами интернет-магазина "Эльдорадо" и осуществлять покупки через него. Именно поэтому мы уделяем особое внимание защите интернет-магазина "Эльдорадо" от DDoS-атак. ●

ГОСТ Р 34.11–2012: три года в строю

Александр Бондаренко, *эксперт технического комитета по стандартизации ТК 26*
Григорий Маршалко, *эксперт технического комитета по стандартизации ТК 26, эксперт ISO/IEC JTC1/SC 27*
Василий Шишкин, *к.ф-м.н., эксперт технического комитета по стандартизации ТК 26, эксперт ISO/IEC JTC1/SC 27*

Хеш-функция, без сомнения, – уникальный объект в криптографии: сама по себе она не реализует никакой криптографической функции безопасности (конфиденциальности, аутентификации, подтверждения подлинности и др.), но в то же время без нее невозможно представить функционирования подавляющего большинства современных алгоритмов и протоколов: выработки случайных чисел, вычисления кода аутентификации сообщения, формирования и проверки электронной подписи. Недаром многие специалисты называют хеш-функцию "рабочей лошадкой современной криптографии".

С первого января 2013 г. в России действует национальный стандарт ГОСТ Р 34.11–2012 г. [1], определяющий алгоритм и процедуру вычисления двух функций хеширования (с различными длинами хеш-кодов) семейства "Стрибог", первоначально представленных на конференции Рускрипто в 2010 г. Три года – это уже значительный срок, по прошествии которого можно подвести некоторые промежуточные итоги.

Принципы синтеза

В наиболее общем понимании функция хеширования предназначена для преобразования входных строк произвольной длины в выходной хеш-код фиксированной длины (при этом различные входные сообщения могут иметь, вообще говоря, один и тот же хеш-код). При использовании в криптографических механизмах функция хеширования должна удовлетворять ряду дополнительных условий. Каждое из этих условий позволяет обеспечивать требуемые криптографические характеристики алгоритма или протокола, который использует данную функцию хеширования. В конкретном протоколе или алгоритме может и не потребоваться выполнения одновременно всех условий сразу, но с прикладной точки зрения удобно, чтобы всем им удовлетворял один алгоритм выработки хеш-кода.

Дополнительные условия для криптографических хеш-функций

Должно быть вычислительно сложно:

- Найти два различных входных сообщения, которые бы давали один и тот же хеш-код – т.н. стойкость к нахождению коллизии. Для стойкой функции с длиной хеш-кода, равной n битам, для нахождения коллизии требуется порядка $2^{n/2}$ операций вычисления хеш-кода. Эта характеристика важна, например, при использовании хеш-функции в алгоритмах электронной подписи.
- По значению хеш-кода найти исходное сообщение – т.н. стойкость к нахождению прообраза. Для стойкой функции с длиной хеш-кода, равной n битам, для нахождения прообраза требуется порядка 2^n операций вычисления хеш-кода. Эта характеристика важна, например, при использовании хеш-функции в алгоритмах хеширования паролей.
- По сообщению, соответствующему значению хеш-кода, найти какое-либо другое сообщение, дающее такой же хеш-код, – т.н. стойкость к нахождению прообраза. Для стойкой функции с длиной хеш-кода, равной n битам, для нахождения прообраза требуется порядка $2^n/m$ операций вычисления хеш-кода, где m – длина первого сообщения. Эта характеристика также важна при использовании хеш-функции в алгоритмах хеширования паролей.
- По значению хеш-кода, значению длины исходного сообщения дополнить исходное сообщение так, чтобы найти хеш-код нового (дополненного) сообщения, – т.н. стойкость к дополнению сообщения. Для стойкой функции с длиной хеш-кода, равной n битам, для решения задачи дополнения сообщения требуется порядка 2^n операций вычисления хеш-кода. Эта характеристика важна при использовании хеш-функции в алгоритмах вычисления кодов аутентификации сообщений (MAC).

Функция хеширования должна максимально сильно перемешивать биты исходного сообщения так, чтобы в результате невозможно было получить никакой информации об исходном сообщении.

Иными словами, функция хеширования должна максимально сильно перемешивать биты исходного сообщения так, чтобы в результате невозможно было получить никакой информации об исходном сообщении. Такое свойство, кстати, и натолкнуло на мысль дать ей имя древнего славянского бога ветра – Стрибога (рис. 1).

При разработке нового алгоритма использовались только хорошо изученные конструкции и преобразования, которые обеспечивают отсутствие свойств, позволяющих эффек-

тивно применять известные методы криптографического анализа. В результате появилась конструкция, не имеющая ничего лишнего, в которой каждый элемент решает определенную криптографическую задачу. Это, в свою очередь, позволило повысить быстродействие при заданных криптографических характеристиках.

Основой алгоритма является т.н. функция сжатия, представляющая собой блочный шифр, функционирующий в режиме Миягучи-Принеля (рис. 2), для которого обоснованы хорошие криптографические качества [2].

При хешировании исходное сообщение дополняется последовательностью битов специального вида, разбивается на блоки, которые последовательно подаются на вход функции сжатия. После того, как все блоки обработаны, происходит процедура финализации: дополнительно хешируется длина сообщения и его контрольная сумма. С учетом реализованных параметров общая конструкция хеш-функции "Стрибог" является дальнейшим развитием хорошо исследованной конструкции Меркля-Дамгорда [3, 4] с усилением и сходна с наиболее современной на настоящее время конструкцией HAIFA (Hash Iterative FrAmework) [5].

В целом все опубликованные результаты можно разделить на два основных направления: исследование свойств функции сжатия и исследование свойств конструкции хеш-функции в целом. Отдельно следует упомянуть большое количество работ по исследованию вопросов реализации функции хеширования на различных вычислительных платформах. В этой статье мы кратко охарактеризуем полученные результаты, более полную информацию можно найти в оригинальных работах или в обзоре [7].

Исследования функции сжатия

К настоящему моменту исследована возможность применения большинства наиболее эффективных методов анализа к функции сжатия хеш-функции "Стрибог": метода встречи посередине [8], метода столкновений [9], метода, использующего супер S-блоки [10, 11], интегрального криптоанализа [12]. Во всех этих работах показана возможность эффективного применения методов только к редуцированным версиям функции сжатия (с уменьшенным числом итераций). Уже начиная с 8 итераций (из полных 12) ни один известный метод эффективно не применим.

За прошедшие 5 лет хеш-функции семейства "Стрибог" стали объектом пристального внимания специалистов в области криптографии. Немалую роль в активизации этих исследований сыграл открытый конкурс научно-исследовательских работ по анализу разработанных хеш-функций.
В целом все опубликованные результаты можно разделить на два основных направления: исследование свойств функции сжатия и исследование свойств конструкции хеш-функции в целом.

Результаты анализа

За прошедшие 5 лет хеш-функции семейства "Стрибог" стали объектом пристального внимания специалистов в области криптографии. Немалую роль в активизации этих исследований сыграл проведенный Российским техническим комитетом по стандартизации "Криптографическая защита информации" (ТК 26) при участии Академии криптографии Российской Федерации и при организационной и финансовой поддержке ОАО "ИнфоТеКС" открытый конкурс научно-исследовательских работ по анализу разработанных хеш-функций [6].

Отдельно следует отметить работу [13], в которой была произведена модификация функции сжатия посредством замены структурных элементов – итерационных констант (различных фиксированных векторов, используемых в вычислениях на каждой итерации) таким образом, что авторы смогли в явном виде построить коллизию.

В целом это направление исследований появилось на волне разоблачений Эдварда Сноудена и было связано с вопросом, можно ли выбирать значения структурных элементов криптографического алгоритма так, чтобы в каком-то смысле ослабить его. Первой

Рис. 1. Изображение славянского бога Стрибога с сайта mythology.info

работой в данном направлении была публикация известного криптографа Жана-Филиппа Омассона и др. [14] которые показали, как указанным выше способом можно строить коллизию для хеш-функции SHA-1. Следует отметить, что подобные результаты носят чисто теоретический интерес, поскольку для построения очередной коллизии злоумышленнику необходимо подбирать каждый раз новый набор кон-

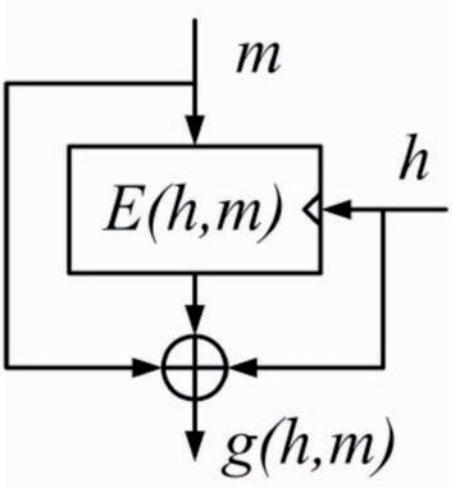


Рис. 2. Блочный шифр E( ) в режиме Миягучи–Принеля. Здесь m – очередной блок хешируемого сообщения, h – значение предыдущей функции сжатия

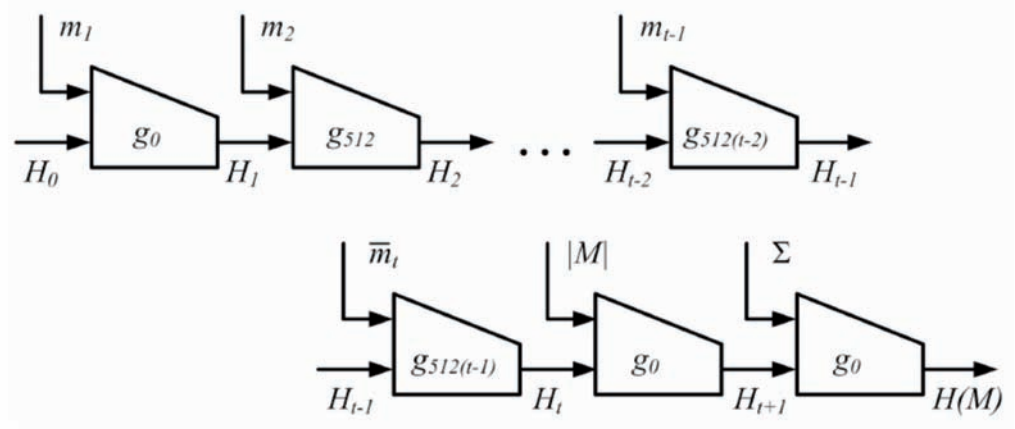


Рис. 3. Общая конструкция хеш-функции "Стрибог"

стант. В то же время, в работе [15] показано, что константы в хеш-функциях "Стрибог" выбраны доказуемо псевдослучайным способом, поэтому указанный подход даже теоретически не может быть использован.

Исследования конструкции в целом

Несомненным достоинством хеш-функций "Стрибог" является наличие теоретического доказательства стойкости использованной конструкции к атакам поиска коллизии и прообраза [16], выполненного выпускником МГУ им. М.В. Ломоносова Георгием Седовым. Следует отметить, что далеко не для всех используемых в настоящее время функций хеширования такое доказательство было получено.

В работе [17], победившей на упомянутом ранее конкурсе научно-исследовательских работ, получено существенное продвижение в развитии методов построения второго прообраза для конструкций типа Меркля-Дамгорда, но и в этом случае для хеш-функций "Стрибог" авторам публикации не удалось предложить методов эффективнее общих методов анализа, что также является подтверждением правильности выбранных синтезных решений.

Вопросы реализации

Вопросам эффективной реализации хеш-функций "Стрибог" к настоящему моменту посвящено большое количество публикаций конференций Рускрипто и CTCrypt [18–21]. В частности, в работе [20] показано, что на процессорах общего пользования "Стрибог" оказывается быстрее своего предшественника, хеш-функции ГОСТ Р 34.11–94, и сопоставим со скоростью реализации нового американского стандарта SHA-3.

Можно отметить также последние результаты специалистов университета Люксембурга [22], которые нашли компактное представление для нелинейного преобразования, используемого в функции сжатия. Такое представление позволяет существенно оптимизировать аппаратные реализации отечественной хеш-функции.

Отметим, что в настоящее время в сети Интернет доступны реализации алгоритмов, описанных в ГОСТ Р 34.11–2012, на различных языках программирования (таких, например, как C++, JavaScript, Java, Python, PHP, Verilog).

Потомки

Интересно, что к настоящему моменту на основе конструкций, использованных при синтезе "Стрибога", начинают разрабатывать и другие алгоритмы. Так, в 2014 г. финский специалист Маркку-Юхани Олави Сааринен на основе функции сжатия отечественного стандарта разработал алгоритм аутентифицированного шифрования STRIBOBr1 [23] для участия в организованном американским Национальным институтом стандартов (NIST) конкурсе. К настоящему моменту этот алгоритм успешно вышел во второй этап состязания.

В 2015 г. индийскими специалистами предложена новая функция MGR (Modified Gost R) [24], которая наследует общую структуру хеш-функции "Стрибог", но имеет другую функцию сжатия.

Выводы

За прошедшие 3 года хеш-функции "Стрибог", определяемые стандартом ГОСТ Р 34.11–2012, зарекомендовали себя как стойкие и эффективно реа-

Рис. 4. Заглавная страница конкурса по анализу хеш-функций "Стрибог"

Вопросы реализации

На процессорах общего пользования "Стрибог" оказывается быстрее своего предшественника хеш-функции ГОСТ Р 34.11--94, и сопоставим со скоростью реализации нового американского стандарта SHA-3.

Специалистами университета Люксембурга найдено компактное представление для нелинейного преобразования, используемого в функции сжатия. Оно позволяет существенно оптимизировать аппаратные реализации отечественной хеш-функции.

лизуемые синтезные решения, которые отвечают современным требованиям по безопасности, а многочисленные независимые исследования подтвердили правильный выбор подходов к их проектированию.

Литература

1. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хеширования.
2. Preneel B., Govaerts R. and Vandewalle J. Hash functions based on block ciphers: A synthetic approach. In: CRYPTO 1993, LNCS. – Vol. 773. – P. 368–378, Springer, London, 1994.
3. Damgård I. A Design Principle for Hash Functions. In: Brassard, G. (ed.) CRYPTO 1989, LNCS. – Vol. 435. – P. 416–427, Springer, Heidelberg, 1989.
4. Merkle R.C. Secrecy, authentication, and public key systems. Stanford Ph.D. thesis 1979.
5. Biham E., Dunkelman O. A framework for iterative hash functions – HAIFA [online]. Доступ через https://eprint.iacr.org/2007/278.pdf.
6. Открытый конкурс научно-исследовательских работ, посвященных анализу криптографических качеств хеш-функции ГОСТ Р 34.11–2012 [online]. Доступ через http://www.streebog.info.
7. Лавриков И.В. Обзор результатов анализа хеш-функций ГОСТ Р 34.11–2012. Проблемы информационной безопасности / И.В. Лавриков, Г.Б. Маршалко, В.И. Рудской, С.В. Смышляев, В.А. Шишкин // Компьютерные системы. – 2015. – № 4. (презентация: http://www.ruscrypto.ru/resource/summary/rc2015/02_rudskoy.pdf).
8. AlTawy R., Youssef A.M. Preimage Attacks on reduced-round Stribog, Preimage Attacks on Reduced-Round Stribog. In: Pointcheval, D., Vergnaud, D. (eds.) AFRICACRYPT 2014. LNCS. – Vol. 8469. – P. 109–125. – Springer International Publishing, 2014.
9. AlTawy R., Kircanski A., Youssef A.M. Rebound attacks on Stribog, In: Lee, H.S., Han, D.G. (eds.) ICISC 2013. LNCS. – Vol. 8565. – P. 175–188. – Springer International Publishing, 2014.
10. Ma B., Li B., Hao R., Li X. Improved cryptanalysis of reduced-round GOST and Whirlpool hash function, n: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) ACNS 2014. LNCS. – Vol. 8479. – P. 289–307. – Springer International Publishing, 2014.
11. Zou J., Wu W., Wu S. Cryptanalysis of the round-reduced GOST hash function, In: Lin, D., Xu, S., Yung, M. (eds.) Inscrypt 2013. LNCS. – Vol. 8567. – P. 309–322. Springer International Publishing, 2014.
12. AlTawy R., Youssef A.M. Integral distinguishers for reduced-round Stribog. Information Processing Letters 114, 8 (2014), P. 426–431.
13. AlTawy R., Youssef A.M. Watch your Constants: Malicious Streebog [online]. Доступ через http://eprint.iacr.org/2014/879.pdf.
14. Albertini A. Malicious Hashing: Eve's Variant of SHA-1 / A. Albertini, J.-P. Aumasson, M. Eichlseder, F. Mendel, M. Schlaffer / In SAC (2014), A. Joux and A. Youssef, Eds. – Vol. 8781 of Lecture Notes in Computer Science, Springer.
15. Рудской В.И. Об алгоритме выработки констант хеш-функции "Стрибог" [online]. Доступ через https://www.tc26.ru/ISO_IEC/Streebog/streebog_constants_rus.pdf.
16. Седов Г. Стойкость ГОСТ Р 34.11–2012 к атаке на прообраз и атаке поиска коллизий // Матем. вопр. криптогр. – 2015. –№ 6:2. – С. 79–98.
17. Guo J., The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function / J. Guo, J. Jean, G. Leuren, T. Peyrin, L. Wang / In: Joux, A., Youssef, A. (eds.) SAC 2014, LNCS. – Vol. 8781. – P. 195–211. Springer International Publishing, 2014.
18. Borodin M., Rybkin A., Urivskiy A. High-Speed Software Implementation of the Prospective 128-bit Block Cipher and Streebog Hash-Function. – CTCrypt, 2014.
19. Lebedev P. A. Comparison of old and new cryptographic hash function standards of the Russian Federation on CPUs and NVIDIA GPUs // Математические вопросы криптографии. – 2013. – № 4:2. – С. 73–80.
20. Казимиров А., Смышляев С. О создании эффективных программных реализаций отечественных криптографических стандартов. – Рускрипто, 2013 [online]. Доступ через http://www.ruscrypto.ru/resource/summary/rc2013/ruscrypto_2013_028.zip.

21. Бородин М., Рыбкин А. Эффективная реализация базовых криптографических конструкций: перспективного алгоритма блочного шифрования с длиной блока 128 бит, функции хеширования ГОСТ Р 34.11–2012 и ЭЦП ГОСТ Р 34.10–2012. – Рускрипто, 2014 [online]. Доступ через http://www.ruscrypto.ru/resource/summary/rc2014/03_borodin_rybkin.pdf.
22. Biryukov A., Perrin L., Udovenko A. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 [online]. Доступ через http://eprint.iacr.org/2015/812.
23. Saarinen M.-J. O. StriBob: authenticated encryption from GOST R 34.11–2012 LPS permutation // Математические вопросы криптографии. – 2015. – № 6:2. – С. 67–78.
24. Bussi K., MGR hash function / K. Bussi, D. Dey, P.R. Mishra, B.K. Bass / [online]. Доступ через http://eprint.iacr.org/2015/856.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

В условиях цейтнота

Марк Соломон (Marc Solomon), *вице-президент компании Cisco по маркетингу средств информационной безопасности*

В то время как злоумышленники активно расширяют арсеналы средств нападения, пользователи невольно помогают им осуществлять атаки. Вследствие этого инциденты ИБ перешли в разряд обыденных явлений. При этом современные атаки зачастую очень трудно остановить. Их особенностью стала повышенная скрытность. Нередко они остаются необнаруженными в течение длительного времени. И в течение всего этого времени критичная информация и интеллектуальная собственность находятся под прямой угрозой компрометации, что создает огромные риски для активов, ресурсов и репутации компании.

От того, насколько быстро сотрудники служб ИБ обнаружат и устранят угрозу, зависит, ограничится ли дело еще одной проблемой или закончится катастрофой. Попытки не отставать от постоянной эволюции ландшафта угроз привели к тому, что в последние годы наметился определенный сдвиг от традиционных средств ИБ, основанных на концепции реагирования на события, к упреждающему аналитическому подходу.

Ситуация напоминает то, как общество защищается от обычных преступников. Налицо тенденция смещения от трудоемких, экстенсивных мер локального характера к высокотехнологичным, масштабным методам обеспечения безопасности. Раньше правоохранительные органы США получали сведения о преступлениях в основном в результате работы полицейских патрулей или посредством звонков от частных граждан. Такое положение вещей до сих пор обеспечивает надежный уровень базовой безопасности. Вместе с тем для того чтобы обеспечить адекватный уровень защиты от наиболее мобильных, скрытных, хорошо организованных (и потому наиболее опасных) преступников, правоохранительные органы вынуждены были дополнить традиционные методы современными комплексными технологиями сбора и обработки информации.

Такая же ситуация сложилась в сфере ИБ. Для того чтобы успешно противодействовать современным атакам, уже недостаточно обычных средств, рассчитанных на то, чтобы обнаруживать вредоносную активность угроз уже известного типа. Необходима расширенная аналитическая информация, включающая, помимо прочего, оперативные данные о самых новых, еще только набирающих обороты угрозах. Реализация систем такого рода, однако, крайне сложна. Основная проблема заключается в том, чтобы обеспечить непрерывный и тщательный сбор нужной информации. Кроме того, очень важно правильно управлять полученными данными, проверять их, выявлять закономерности и взаимосвязи. Только так можно получить полноценную информацию о современных атаках, позволяющую успешно противодействовать им.

В современном мире ситуация обстоит таким образом, что в результате успешной атаки злоумышленники могут похитить важные данные за считанные минуты, тогда как обнаружение и изучение атаки может занять месяцы и даже годы. Таким образом, очевидно, что главными факторами эффективности систем ИБ становятся, во-первых, сокращение времени, затрачиваемого на обнаружение инцидента (TTD), а во-вторых, времени, затрачиваемого на реагирование на обнаруженный инцидент (TTR). Аналитическая информация об угрозах ИБ жизненно важна для эффективной работы систем защиты и реагирования. Вместе с тем такая информация должна иметь определенные особенности:

- Тактический характер. Непрерывный и тщательный сбор важной информации из доверенных источников, управление полученными данными, выяснение взаимосвязей, изучение действий злоумышленников и принятие соответствующих мер – все это должно осуществляться в рамках риск-ориентированного подхода, точно определяющего, как использовать эту информацию. Объемы информации могут быть огромными, поэтому очень важно использовать подходящий формат хранения, обработки и предоставления данных – это значительно облегчит их использование.
- Наличие контекста. Данные об угрозах нельзя изучать как автономные элементы. Они рассматриваются в рамках той или иной совокупности, а для адекватной интерпретации такой совокупности необходимо знание общего контекста. Этот контекст может включать в себя сведения о расположении, масштабе или специфике деятельности предприятия. Он может функционировать в тесной связи с индикаторами компрометации (IoCs), информационными лентами и другими средствами. Например, для организаций сферы финансовых услуг прежде всего важна информация об угрозах, характерных для этой отрасли, тогда как, к примеру, аналитика угроз, касающихся сферы розничной торговли, будет представлять существенно меньшую ценность.

В современном мире ситуация обстоит таким образом, что в результате успешной атаки злоумышленники могут похитить важные данные за считанные минуты, тогда как обнаружение и изучение атаки может занять месяцы и даже годы.

● Высокая степень автоматизации. Автоматизация определяется тем, насколько легко и согласованно реализуются процессы получения и обработки данных, а также эффективностью создания итоговой оперативной аналитики, специализированной для конкретных нужд предприятия. Такая система не должна включать никаких трудоемких ручных операций (они лишь ограничат ее эффективность). Информация об угрозах должна непрерывно поступать, обрабатываться и преобразовываться в форму, необходимую для обеспечения эффективной защиты предприятия. Кроме того, понятие автоматизации включает в себя методики обмена информацией между доверенными структурами для ускорения процессов взаимодействия и принятия решений.

Важным дополнением к глобальной аналитике угроз следует назвать аналитику локального характера. Она предоставляет данные об особенностях и функционировании внутренней вычислительной инфраструктуры организации. Такая информация предоставляет дополнительный уровень контекста и является необходимой основой для принятия конкретных решений в области ИБ предприятия. Чтобы получать такую информацию в полном объеме, необходимо осуществлять всеобъемлющий мониторинг вычислительной сети, что сопряжено с определенными сложностями.

Современные сетевые инфраструктуры вышли далеко за пределы традиционных периметров ЛВС. Теперь они включают в себя не только серверы и конечные точки, но и ЦОДы, мобильные устройства, разнообразные виртуальные и облачные платформы. Современные сети и их компоненты постоянно развиваются, что зачастую порождает новые векторы атак. В качестве примера можно назвать специфические атаки, направленные на гипервизоры, домашние компьютеры, мобильные устройства и приложения, на интернет-приложения, браузеры, социальные сети и даже на автомобили. Только всесторонний контроль за устройствами, приложениями, пользователями и другими системами, являющимися частью расширенной сети предприятия, позволит правильно интерпретировать все внутрисетевые события и взаимосвязи между ними, а это важная предпосылка для правильного применения глобальной аналитики угроз.

Итак, для того чтобы уменьшить затраты времени на обнаружение (TTD) и реагирование (TTR) на инциденты ИБ, аналитическая информация об угрозах должна иметь выраженный тактический и контекстуальный характер, быть автоматизированной и хорошо приспособленной к обмену и совместной работе. Кроме того, она должна охватывать все пространство расширенной сети и включать в себя полные данные обо всех подключенных устройствах. Аналитическая информация об угрозах, обладающая всеми этими свойствами, способна обогатить арсенал средств защиты и обеспечить специалистам все преимущества аналитического подхода к обеспечению информационной безопасности. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Современные сетевые инфраструктуры вышли далеко за пределы традиционных периметров ЛВС. Теперь они включают в себя не только серверы и конечные точки, но и ЦОДы, мобильные устройства, разнообразные виртуальные и облачные платформы. Современные сети и их компоненты постоянно развиваются, что зачастую порождает новые векторы атак.

Бизнес-аналитика
для сети магазинов "Детский мир"

Группа компаний "Детский мир" и компания "Инфосистемы Джет" построили систему бизнес-анализа и отчетности на платформе QlikView в виртуальном ЦОДе (ВЦОД) компании "Инфосистемы Джет". Система развернута на отказоустойчивом кластере (текущая конфигурация – 12 серверов). Система обрабатывает In-Memory большие объемы данных, поступающих от более чем 380 торговых точек, склада, бэк-офиса. Специально разработанный набор отчетов позволяет анализировать показатели продаж и товарных остатков в различных разрезах, эффективнее планировать ассортимент и объемы закупок, упростить процесс получения информации для переговоров с поставщиками.

Поддержка эксплуатации системы осуществляется в режиме 24x7. Время реакции на сбой наиболее критичных сервисов не превышает 15 минут, а время восстановления – двух часов.

"За время эксплуатации QlikView количество формируемых отчетов и пользователей существенно возросло, повысились требования к мощности вычислительной платформы. Кластерная конфигурация позволила быстро нарастить вычислительный ресурс и обеспечить оперативное построение отчетов для множества пользователей. С системой могут работать до 60 человек одновременно, при этом сохраняется высокая производительность за счет динамической балансировки нагрузки между серверами кластера", – рассказывает Сергей Кондарев, директор Департамента информационных технологий Группы компаний "Детский мир".

В это же время "Детский мир" перевел автоматизацию основных бизнес-процессов на новую учетную систему – SAP ERP for Retail. Основным источником данных для системы анализа и отчетности QlikView стало корпоративное хранилище SAP BW. Специалисты компании "Инфосистемы Джет" мигрировали данные из прежнего хранилища и адаптировали модели существующих отчетов к логике хранения и обработки данных в SAP, принципам учетной политики. Кроме того, были настроены механизмы получения системой QlikView данных из ряда дополнительных источников, таких как база данных Oracle, работающая в зарубежном филиале, кассовый сервер, пользовательские Excel-файлы. Благодаря этому система получает более полные данные для бизнес-анализа. ●

Новые продукты

Программный комплекс автоматизированного контроля и мониторинга за состоянием информационной безопасности организации и поддержки специалистов в принятии решений по комплексной защите информации организации от компьютерных угроз R-Vision S-GRC

Производитель: компания R-Vision ("Ай-Эс-Эм Системс")
Сертификат: 000327, выдан ООО "Центр стандартизации ИСО"
Назначение: автоматизированный контроль и мониторинг за состоянием ИБ и поддержка руководства в принятии решений по комплексной защите организации от компьютерных угроз
Особенности:
- SGRC – это центр контроля ИБ, состоящий из объединенных и интегрированных в единое решение модулей системы R-Vision
- предназначен для сбора и обработки информации из различных процессов информационной безопасности с целью поддержки руководителя в принятии решений по дальнейшему стратегическому и тактическому управлению ИБ в компании

Возможности:
- контроль и управление информационными и физическими активами
- управление рисками информационной безопасности
- управление инцидентами информационной безопасности
- соответствие законодательным и отраслевым требованиям

Время появления на российском рынке: 2011 г.
Подробная информация: http://dialognauka.ru/press-center/news/16393/; https://rvision.pro/modules/security-grc/
Фирма, предоставившая информацию: ДИАЛОГНАУКА, АО

См. 3-ю обл. и стр. 43

Программный комплекс DeviceLock DLP, версия 8.1 DeviceLock DLP

DeviceLock
Proactive Endpoint Security

Производитель:
АО "Смарт Лайн Инк"
Назначение: выявление нарушений корпоративной политики безопасного хранения файлов, документов и данных, в том числе данных ограниченного доступа, на рабочих станциях, серверах и в сетевых хранилищах организации
Особенности:
- осуществляет централизованный контроль и протоколирование доступа пользователей к устройствам, портам ввода-вывода, сетевым протоколам и приложениям
- обеспечивает проактивную защиту от утечки данных и проникновения вредоносных программ на рабочих компьютерах сотрудников, что существенно снижает риски бизнеса и финансовые потери от злоумышленных действий, ошибок и халатности инсайдеров или других лиц, имеющих физический доступ к рабочим станциям

Возможности:
- комплекс DeviceLock DLP предназначен для организаций, заинтересованных в простом, доступном и высокоэффективном подходе к решению задачи предотвращения утечки корпоративных данных с Windows- и Mac-компьютеров, а также виртуализованных Windows-сред
- обеспечивает координированное применение полного набора механизмов контекстного контроля и контентной фильтрации для защиты от утечек данных при их использовании, передаче и хранении на корпоративных компьютерах, при этом не прерывая штатные производственные процессы
- позволяет службам информационной безопасности централизованно и оперативно управлять DLP-политиками в масштабах всей организации независимо от размера ИТ-инфраструктуры. Это достигается благодаря нативной интеграции управления в групповые политики домена Microsoft Active Directory и встраиванию консоли DeviceLock в оснастку управления Microsoft Group Policy Management Console (GPMC)
- поддерживает любые LDAP-каталоги, рабочие группы и может использоваться на отделенных от общей сети рабочих станциях под управлением ОС Windows
- предоставляет службам ИБ высочайший уровень функциональных возможностей для DLP-защиты рабочих станций при гибкой ценовой политике

Характеристики:
- описаны на Web-сайте разработчика www.devicelock.com/ru
- среди новых возможностей DeviceLock DLP, появившихся в версии 8.1 – контроль IBM (Lotus) Notes, протокола Torrent, поддержка OCR в сервере полнотекстового поиска DeviceLock Search Server и др.

Время появления на российском рынке: III квартал 2015 г.
Подробная информация: www.devicelock.com/ru
Фирма, предоставившая информацию: СМАРТ ЛАЙН ИНК, АО

См. стр. 44, 45

Межсетевой экран нового поколения FortiGate-3810D

Производитель: Fortinet
Сертификат: изделие подлежит сертификации
Назначение: для крупных распределенных сетей
Особенности: порты 100GbE и сверхвысокая проходимость 300+ Гбит/с
Возможности:
- интегрированная безопасность сети с высокой производительностью для крупных предприятий и провайдеров, предоставляющих услуги по управлению сервисами
- высокая пропускная способность за счет процессоров ускоренной обработки FortiASIC, высокая плотность портов и гибкость при развертывании
- каждое устройство FortiGate имеет следующие функции: межсетевой экран, IPS, контроль приложений, фильтрацию Web-контента, VPN, противодействие шпионскому ПО, оптимизацию WAN, антиспам и т.д.

Характеристики: пропускная способность МСЭ до 320 Гбит/с, IPS до 25 Гбит/с, AV до 7,7 Гбит/с, IPSec VPN до 135 Гбит/с
Время появления на российском рынке: декабрь 2014 г.
Подробная информация: http://www.fortinet.com/press_releases/2014/fortigate-3810D-world-first-data-center-firewall-appliance.html
Фирма, предоставившая информацию: FORTINET

См. стр. 37

Решение по борьбе с изощренными вредоносными программами и целенаправленными устойчивыми угрозами FortiSandbox 3000D

Производитель: Fortinet
Сертификат: изделие подлежит сертификации
Назначение: ключевое решение в борьбе с изощренными вредоносными программами и целенаправленными устойчивыми угрозами в рамках более широкой, комплексной системы безопасности
Особенности:
- динамическая защита от вредоносных программ, на основе облачного сервиса обновлений
- эмуляция кода
- полная виртуальная среда

- расширенная наблюдаемость
- обнаружение обратных сетевых обращений
- анализ вручную
- дополнительный доступ к услугам FortiGuard

Возможности:

- мощное средство по борьбе с целенаправленными устойчивыми угрозами (APTs)
- функционирует вместе с межсетевыми экранами нового поколения Fortinet FortiGate (NGFW) и шлюзом для защиты электронной почты FortiMail и сочетает в одном устройстве уникальный сервис двухуровневой песочницы, динамический анализ угроз, приборный интерфейс в реальном времени и подробную отчетность
- межсетевые экраны нового поколения Fortinet выступают в качестве первой линии обороны, сканируя и снижая уровень угроз. При их использовании вместе с FortiSandbox они способны выявлять и проверять подозрительные файлы, а затем устанавливать обновленный уровень защиты на основе полного жизненного цикла угрозы
- в 2014 г. решение получило статус "рекомендовано" по результатам тестирования NSS Labs и прошло 100 процентов тестов, которые позволили оценить степень надежности и стабильности работы устройства
- анализ NSS Labs подтвердил, что FortiSandbox-3000D в реальной среде тестирования (более 1800 реальных уязвимостей и образцов вредоносных программ) показывает уровень обнаружения угроз до 99 процентов. Тесты NSS Labs также подтвердили, что большинство обнаружений происходило в течение трех или менее минут

Время появления на российском рынке: январь 2014 г.
Подробная информация: http://www.fortinet.com/press_releases/2014/fortinet-earns-recommended-rating-fortisandbox-nss-labs.html
Фирма, предоставившая информацию: FORTINET

См. стр. 37

Высокоэффективный межсетевой экран для защиты Web-приложений FortiWeb 4000E

Производитель: Fortinet
Сертификат: изделие подлежит сертификации
Назначение: обеспечивает современную многоуровневую защиту приложений в сетях средних и крупных организаций, поставщиков служб приложений и поставщиков SaaS
Особенности: предоставляет пропускную способность до 10 Гбит/с, полный объем хранения

Возможности:

- обеспечивает беспрецедентную пропускную способность 20 Гбит/с
- первое решение на рынке брандмауэров, оснащенное встроенными современными функциями защиты от вредоносных программ
- дополнено передовыми функциями сканирования на наличие уязвимостей от Acunetix
- производительность, эффективность и функционал средств Fortinet FortiWeb превосходят аналогичные показатели решений конкурентов
- брандмауэры серии FortiWeb включают FortiSandbox и инфраструктуру защиты от продвинутых угроз, что обеспечивает всестороннюю защиту корпоративных сетей от наиболее изощренных киберугроз

Характеристики: порты 4 x GE RJ45, RJ45 4 x GE, обходные порты, порты SFP GE 4 x, порты 4 x 10G SFP +, два блока питания переменного тока, 2 x 2 ТБ для хранения
Время появления на российском рынке: сентябрь 2015 г.
Подробная информация: http://www.fortinet.com/products/fortiweb/index.html
Фирма, предоставившая информацию: FORTINET

См. стр. 37

Система управления инцидентами кибербезопасности Positive Technologies Industrial Security Incident Manager (PT ISIM)

Производитель: Positive Technologies
Назначение: обнаруживает хакерские атаки и помогает в расследовании инцидентов на критически важных объектах без остановки основного технологического процесса
Особенности:

- цепочки атак против распределенных во времени угроз
- визуализация атак на бизнес-логику

Возможности:

- визуализация атак на бизнес-логику позволяет корректно интерпретировать события системы
- цепочки атак – мощное средство против распределенных во времени угроз
- исключительно пассивный режим работы
- оперативная информация для принятия решений на всех уровнях
- расследование инцидентов без остановки системы
- каждая отрасль получает свой продукт
- помогает обнаружить и предотвратить действия злоумышленников
- соответствует требованиям промышленной среды

Ориентировочная цена: от 800 000 руб.
Время появления на российском рынке: февраль 2016 г.
Подробная информация: http://www.ptsecurity.ru/
Фирма, предоставившая информацию: POSITIVE TECHNOLOGIES

См. стр. 17

Самообучающийся защитный экран уровня приложений PT Application Firewall

Производитель: Positive Technologies
Сертификат: 3455, выдан ФСТЭК
Назначение: выявление и блокирование современных атак
Особенности: может применяться в государственных информационных системах до первого класса защищенности

Возможности:

- продукт сертифицирован ФСТЭК, а значит, повторная сертификация защищаемых приложений в случае их модификации не требуется
- выполнение рекомендаций и требований приказов ФСТЭК № 17 и 21 и стандарта PCI DSS
- контроль доступа к конфиденциальным документам
- моментальная реакция на угрозы с помощью установки виртуальных патчей до устранения уязвимости
- защита от всех распространенных уязвимостей по классификации OWASP и WASC, включая SQLi, XSS и XXE
- гибкие модели развертывания, легкость настройки, валидация и профилирование SOA-вызовов и XML-сообщений, защита от DDoS-атак и др.

Ориентировочная цена: от 750 000 руб.
Время появления на российском рынке: май 2015 г.
Подробная информация: http://www.ptsecurity.ru/products/mp8/
Фирма, предоставившая информацию: POSITIVE TECHNOLOGIES

См. стр. 17

Система контроля защищенности и соответствия стандартам MaxPatrol 8

Производитель: Positive Technologies
Сертификат: 2922, выдан ФСТЭК
Назначение: автоматизирует процесс поиска уязвимостей и контроля соответствия стандартам в IT-инфраструктуре любого масштаба с учетом специфики каждой отрасли

Особенности:
- единый автоматизированный инструмент контроля
- база знаний уязвимостей – одна из крупнейших в мире
- не требует установки программ-агентов
- стандартные и собственные настройки
- гибкая система отчетности
- оценка эффективности защиты всей IT-инфраструктуры, а также отдельных узлов

Возможности: механизмы тестирования на проникновение, системных проверок и контроля соответствия стандартам в сочетании с поддержкой анализа различных операционных систем, СУБД и Web-приложений обеспечивают непрерывный мониторинг безопасности на всех уровнях информационной системы
Время появления на российском рынке: май 2008 г.
Подробная информация: http://www.ptsecurity.ru/products/mp8/
Фирма, предоставившая информацию: POSITIVE TECHNOLOGIES
См. стр. 17

Услуги

Обеспечение защиты информации в автоматизированных системах управления производственными и технологическими процессами (защита АСУ ТП)

Отрасль: нефтегазовая, электроэнергетика, ЖКХ
Регион: РФ
Описание:
- анализ текущего уровня защищенности АСУ ТП
- тест на проникновение в АСУ ТП
- разработка комплексной системы защиты АСУ ТП
- формирование требований по обеспечению ИБ к техническим решениям в процессе проектирования АСУ ТП сторонними разработчиками
- подготовка и сертификация компонентов АСУ ТП по требованиям ФСТЭК
- аттестация АСУ ТП

Фирма, предоставившая информацию: ИНФОРМЗАЩИТА, НИП, ЗАО
См. стр. 21

НЬЮСМЕЙКЕРЫ

ДИАЛОГНАУКА, АО
117105 Москва,
ул. Нагатинская, 1
Тел.: (495) 980-6776
Факс: (495) 980-6775
E-mail: info@dialognauka.ru,
marketing@dialognauka.ru
www.dialognauka.ru
См. ст. "Современные технологии контроля привилегированных пользователей" на стр. 43
См. 3-ю обл.

ИНФОРМЗАЩИТА, НИП, ЗАО (КОМПАНИЯ "ИНФОРМЗАЩИТА")
Почтовый адрес:
127018 Москва, а/я 55
Фактический адрес:
127018 Москва,
ул. Образцова, 38
(вход с улицы Образцова)
Тел/факс: (495) 980-2345 (многоканальный)
E-mail: market@infosec.ru
www.infosec.ru,
www.20.infosec.ru
См. ст. "Защита АСУ ТП. Прежде чем что-то внедрять" на стр. 21

ИНФОСИСТЕМЫ ДЖЕТ, КОМПАНИЯ
127015 Москва,
ул. Большая Новодмитровская, 14, стр. 1
Тел.: (495) 411-7601, 411-7603
Факс: (495) 411-7602
E-mail: info@jet.msk.su
www.jet.msk.su
См. ст. "SOC: кадры решают все" на стр. 32, 33

НАУЧНО-ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ СИСТЕМ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ, ООО
117246 Москва,
Научный пр., 17, этаж 8
Тел.: (495) 646-7563
E-mail: info@niisokb.ru
www.niisokb.ru
См. ст. "SafePhone PLUS на страже коммуникаций" на стр. 41

СМАРТ ЛАЙН ИНК, АО
107140 Москва,
1-й Красносельский пер., 3, пом. 1, ком. 17
Тел.: (495) 647-9937
Факс: (495) 647-9938
E-mail:
ru.sales@devicelock.com
devicelock.com/ru
www.smartline.ru
См. ст. "DeviceLock DLP как инструмент выполнения некоторых требований стандарта СТО БР" на стр. 44, 45

FORTINET
121099 Москва, Смоленская пл., 3, Регус, офис 610
Тел/факс: (499) 955-2499
E-mail: russia@fortinet.com
www.fortinet.com
См. стр. 37

POSITIVE TECHNOLOGIES
107061 Москва,
Преображенская пл., 8
Тел.: (495) 744-0144
E-mail: pt@ptsecurity.com
www.ptsecurity.ru
См. ст. "Эволюция индустриальной кибербезопасности. Построение интеллектуальных систем обеспечения защиты АСУ ТП промышленных предприятий" на стр. 17

KASPERSKY lab

ЗАЩИТА СЕГОДНЯ — ШАГ В БЕЗОПАСНОЕ ЗАВТРА

Стратегические решения в сфере IT-безопасности

ДиалОгНаука
системная интеграция в области информационной безопасности

www.dialognauka.ru

kaspersky.ru/corporate

ГЛАВНОЕ СОБЫТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

itsec by Groteck

infosecurity RUSSIA

InfoSecurity Russia

БЕЗОПАСНОСТЬ. ИННОВАЦИИ. СООБЩЕСТВО

27–29 Сентября 2016

6015 профессиональных посетителей

4155 участников деловой программы

более **15 000** предварительно назначенных встреч

более **300** продуктов и решений, представленных в экспозиции

163 мероприятия на стендах экспонентов и в конференц-залах

146 спикеров из числа ведущих мировых и российских экспертов, выступающих в четырех параллельных конференционных потоках.

Выставка обеспечивает максимальную полезность визита для заказчика и наивысший в России ROI для экспонента

Прием заявок на участие открыт:

www.infosecurityrussia.ru

Groteck Business Media