Интернет-журнал «Науковедение» ISSN 2223-5167 http://naukovedenie.ru/
Том 7, №1 (2015) http://naukovedenie.ru/index.php?p=vol7-1
URL статьи: http://naukovedenie.ru/PDF/28PVN115.pdf
DOI: 10.15862/28PVN115 (http://dx.doi.org/10.15862/28PVN115)

УДК 378

Невский Александр Юрьевич
ФГБОУ ВПО «Национальный исследовательский университет «МЭИ»
Россия, Москва[1]
Профессор кафедры информационной и экономической безопасности
Кандидат технических наук, доцент
E-mail: NevskyAY@mpei.ru

Опыт использования возможностей DLP-системы в деловой игре при подготовке бакалавров по направлению «Информационная безопасность»

[1] 1112509, г. Москва, Красноказарменная ул., 14, ФГБОУ ВПО «Национальный исследовательский университет «МЭИ»

Аннотация. В данной статье рассматривается опыт проведения деловых игр с бакалаврами, получающими образование по направлению «Информационная безопасность» на кафедре информационной и экономической безопасности (ИЭБ) НИУ «МЭИ». В частности, рассматривается сценарий деловой игры, проводимой при изучении дисциплины «Управление инцидентами информационной безопасности», где в качестве программного обеспечения применяется одна из версий, так называемых DLP-систем, широко используемых в настоящее время для мониторинга поведения пользователей в автоматизированных информационных системах (АИС) организаций.

Проведение деловой игры призвано значительно повысить интерес обучаемых к практике внедрения DLP-систем и использования их ресурсов в процессе расследования инцидентов информационной безопасности в АИС организации.

Ключевые слова: автоматизированная информационная система; DLP-система; компетенция; мониторинг; инцидент информационной безопасности; деловая игра; утечка информации; снифер; «Контур информационной безопасности SearchInform»; политика безопасности; роль; трафик событий; критерий оценки.

Ссылка для цитирования этой статьи:

Невский А.Ю. Опыт использования возможностей DLP-системы в деловой игре при подготовке бакалавров по направлению «Информационная безопасность» // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 7, №1 (2015) http://naukovedenie.ru/PDF/28PVN115.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ. DOI: 10.15862/28PVN115

Введение

Современная АИС организации (компании) представляет собой сложную организационную и программно-аппаратную систему, эффективное использование ресурсов которой невозможно без всестороннего обеспечения их безопасности. Безопасность ресурсов АИС не может быть обеспечена, в том числе и без четкого контроля за выполнением правил поведения в системе каждым ее пользователем.

Нормативными документами, регламентирующими менеджмент информационной безопасности и возможных инцидентов информационной безопасности, предполагается применение средств мониторинга пользователей[2,3]. В частности, в разделе 13 «Менеджмент инцидентов в системе защиты информации» имеет место следующее требование: «Должны иметься (имеется ввиду в организации) обязанности и процедуры для того, чтобы результативно справляться с событиями и недостатками в системе защиты информации, как только о них будет сообщено. Процесс непрерывного улучшения должен применяться к реагированию на инциденты в системе защиты информации, постоянный контроль, оценивание и общий менеджмент инцидентов в системе защиты информации».

Кроме этого подобные требования можно отметить в законодательстве РФ, в частности в законах: «Об информации, информационных технологиях и защите информации», «О персональных данных», «О национальной платежной системе». Наиболее четкая регламентация менеджмента инцидентов информационной безопасности наблюдается в банковской сфере РФ.

Так, в 2012 году вышло Указание Банка России № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств», где в прямой постановке банковским организациям предписана подача отчетности по инцидентам, связанным с воздействием компьютерных вирусов, компрометацией электронной подписи и ключей шифрования, а также любых других воздействий.

Таким образом, в настоящее время, как в сфере информационных систем и технологий, так и в сфере обеспечения их безопасности сложились условия необходимости широкого внедрения и использования систем мониторинга, а в частности:

- существуют достаточно четко сформулированные требования и рекомендации законодательства РФ и т.н. регуляторов в области информационной безопасности;
- сформировался достаточно широкий «рынок» систем мониторинга, как зарубежных, так и отечественных;
- резко повысилась эффективность и гибкость систем;
- повысилась доступность систем.

---

[2] ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности, [Текст] – М. Стандартинформ, 2012.

[3] ГОСТ Р ИСО/МЭК ТО 18044-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности, [Текст] – М. Стандартинформ, 2007.

Следствием сказанного является растущая потребность организаций как государственного, так и частного сектора экономики в специалистах, подготовленных к внедрению и эксплуатации систем, позволяющих реализовать контроль и управление событиями в АИС для предотвращения утечки конфиденциальной и просто представляющей для компании ценность, информации.

DLP-система: понятие, назначение, возможности и особенности внедрения в АИС организации

DLP-система или система предотвращения утечек информации (от англ. Data Loss (Leak) Prevention) представляет собой совокупность технологий предотвращения утечек конфиденциальной информации из информационной системы по различным каналам передачи, а также технические, в том числе и программные (программно-аппаратные) средства предотвращения утечек.

Назначение DLP-системы в комплексной системе обеспечения информационной безопасности организации вытекает из приведенного выше понятия и для целей данной статьи не нуждается в более полном раскрытии. Вместе с тем существует необходимость остановиться на различии во взглядах некоторых специалистов относительно «за» и «против» использования возможностей подобных систем в деятельности организации [5].

Основным доводом тех специалистов, кто поддерживает идею широкого использования возможностей DLP-системы, является то, что в современной АИС число и разнообразие каналов утечки информации достигло значительного количества. Несмотря на то, что под защитой от утечек информации в большинстве организаций по-прежнему подразумевают только контроль внешних устройств, принтеров и электронной почты, нельзя не учитывать весьма информативные каналы утечки, образованные интернет-сервисами, такими как: интернет-пейджеры, веб-почта, социальные сети, блоги, форумы, файлообменники, FTP, пиринговые сети, сервисы отправки SMS/MMS и это не полный их перечень.

Таким образом, совокупностью современных коммуникаций созданы условия постоянной и серьезной уязвимости корпоративной информации организации, в том числе и конфиденциальной, а если ситуация с обеспечением безопасности информационных активов организации выходит из под контроля, руководство имеет право принимать адекватные меры по противодействию этому, в том числе и с использованием программных средств с учетом законности, легальности и транспарентности процедуры внедрения.

В качестве основного довода противников использования DLP-систем приводятся соображения неэтичности, при раскрытии которых часто пользуются «конструкциями», главный смысл которых заключается в аморальности и противозаконности «шпионить» за сотрудниками, подслушивать (подглядывать) за их действиями, не доверять им и подобные.

Считаю, что данная статья отнюдь не призвана прекратить эти споры, но хочу кратко выразить свое собственное мнение. Любой гражданин, нанимаясь на работу, условно говоря, продает работодателю часть своего времени, получая взамен компенсацию в виде оплаты труда. За это он обязуется выполнять обязанности в полном объеме и в соответствии с принятыми в организации правилами, и, если данные правила не противоречат положениям законодательства, то их необходимо считать вполне правомочными и обязательными. Подтверждение этому можно найти в Гражданском и Трудовом кодексах РФ.

В материалах [1] рассматриваются два способа внедрения DLP-системы в организации: скрытый и открытый, а также делается предпочтение второму из них, как наиболее прозрачному и отвечающему целям внедрения.

В заключение этого раздела статьи приводится краткий материал о перечне инструментов DLP-системы. Дальнейший разговор мы будем вести о системе «**Контур информационной безопасности SearchInform**» [2].

Данная система выбрана в качестве программного обеспечения проведения деловой игры и выбор обусловлен установившимися тесными партнерскими отношениями между кафедрой ИЭБ и компанией **SearchInform** [3].

В настоящее время компания **SearchInform со своим комплексным программным решением выгодно отличается от других вендоров тем, что абсолютно бесплатно предоставляет свой продукт образовательным учреждениям для учебных целей, что, естественно, представляется для нас весьма важным фактором.**

Программное обеспечение «Контур информационной безопасности SearchInform» представляет собой совокупность отдельных инструментов – сниферов [7], сканирующих информацию, передаваемую в информационной системе организации по различным каналам: электронная почта; система мгновенных сообщений типа ICQ и подобных; интернет-сервисы типа FTP, Skype; внешние носители типа USB, CD, DVD; документы, переданные на печать; веб-браузеры; мобильные устройства типа планшетов, смартфонов, сотовых телефонов на различных платформах; ноутбуки; стационарные компьютеры, мониторы и файловые серверы (рис.1).

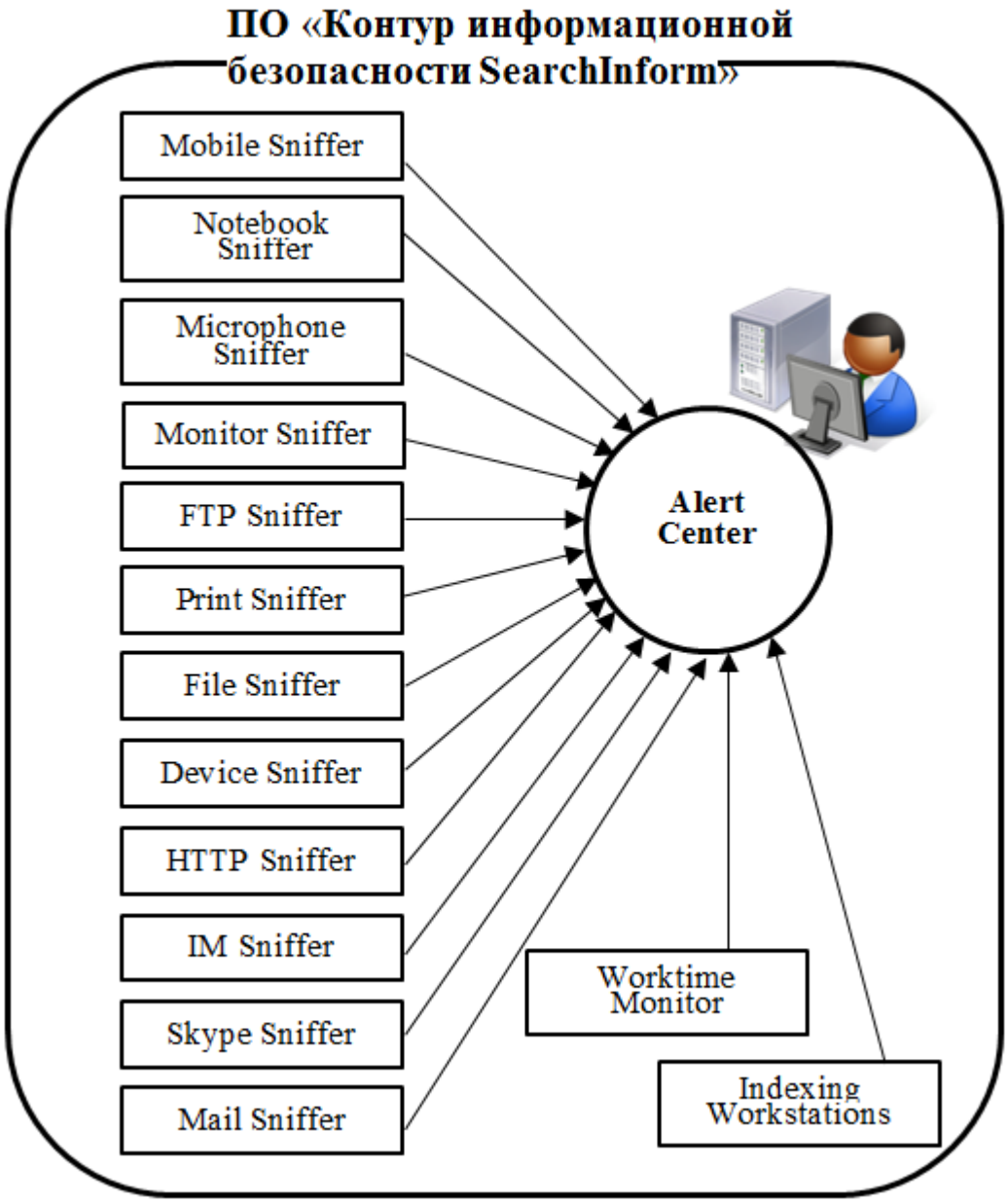

Рис. 1. *Структурная схема DLP-системы «**Контур информационной безопасности SearchInform**» [3]*

Эти многочисленные инструменты DLP-системы функционируют под управлением единой системы реагирования, называемой «Alert Center».

Интерес к приобретению и использованию в повседневной деятельности информационных систем различных предприятий достаточно высок, однако, правильная и эффективная эксплуатация подобных систем невозможна без персонала, или хотя бы одного сотрудника, имеющего соответствующую профессиональную подготовку.

Этим объясняется наш повышенный интерес, заключающийся во внедрении и совершенствовании практики использования DLP-системы в учебном процессе кафедры.

Более того, анализ содержания действующего образовательного стандарта по подготовке бакалавров по направлению «Информационная безопасность»[4] показывает, что изучение основных приемов использования подобных компьютерных систем способствует овладению некоторыми общекультурными (ОК-5,6,12) и большим перечнем профессиональных компетенций (ПК- 2-5, 8,10,11,15,16,18-21,26,27,29-32), что в свою очередь свидетельствует о важности использования программного продукта для образовательных целей.

Проведение деловой игры в процессе изучения дисциплины «Управление инцидентами информационной безопасности»

Деловая игра, как активный метод проведения учебного занятия, предназначена для повышения эффективности усвоения учебного материала за счет использования творческого мышления студентов, активизации их познавательной деятельности, возможности генерации ими новых идей, самостоятельного принятия управленческих решений, а также созданию необходимых условий для их реализации (обсуждения) [6].

Структура деловой игры.

Рассмотрим игровую модель как основную при разработке деловой игры. Игровая модель представляет собой совокупность следующих компонентов:

- цели игры;
- комплекс ролей и функций игроков;
- сценарий игры;
- правила игры.

Цель игры заключается в формировании профессиональных компетенций обучаемых, выражающихся в готовности к совершенствованию информационной безопасности организации посредством осуществления мониторинга поведения пользователей ее АИС в процессе выполнения служебных обязанностей с использованием ресурсов DLP-системы.

Комплекс ролей и функций участников игры (рис.2):

- *руководитель* – преподаватель, ведущий курс, осуществляет общее руководство проведением игры, готовит разбор и подведение итогов игры;
- *помощники руководителя* – (1-2 человека) ассистенты, лаборанты, которые контролируют действия всех категорий игроков, готовят исходные данные для разбора и подведения итогов;
- *пользователи (обычные)* АИС компании (1-2 человека) - выполняют операции, характерные для нормальной служебной деятельности сотрудников организации;
- *нарушители* политик и правил работы в АИС компании (1-2 человека), выполняющие действия или работы, представляющие собой факты нарушения режима и правил безопасности в АИС;

[4] Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «Бакалавр»), федеральный портал «Российское образование», [Электронный ресурс], http://www.edu.ru/db/portal/spe/fgos/pr_fgos_2009_pv_64b.pdf.

- *удаленные пользователи* (1-2 человека), выполняют операции, характерные для деятельности клиента компании;
- *внешние злоумышленники (хакеры)* (1 человек), выполняют действия злоумышленного характера по отношению к безопасности ресурсов АИС;
- *администраторы* DLP-системы - (2 - 3 человека), осуществляющие операции по настройке компонентов системы, а также по сбору и обработке информации о событиях в АИС компании. В сущности это, так называемые, по сложившейся в последнее десятилетие терминологии в области информационной безопасности *офицеры безопасности* [4];
- *руководство компании* - (1 - 2 человека), выполняющие работы по управлению режимом информационной безопасности компании на основе информации о событиях в АИС, предоставляемых администраторами DLP-системы.

Сценарий игры:

В информационной системе коммерческого предприятия ООО «Х», занимающегося оптовой продажей продуктов питания сетевым магазинам, развернута DLP-система с целью мониторинга поведения пользователей при использовании его информационных активов.

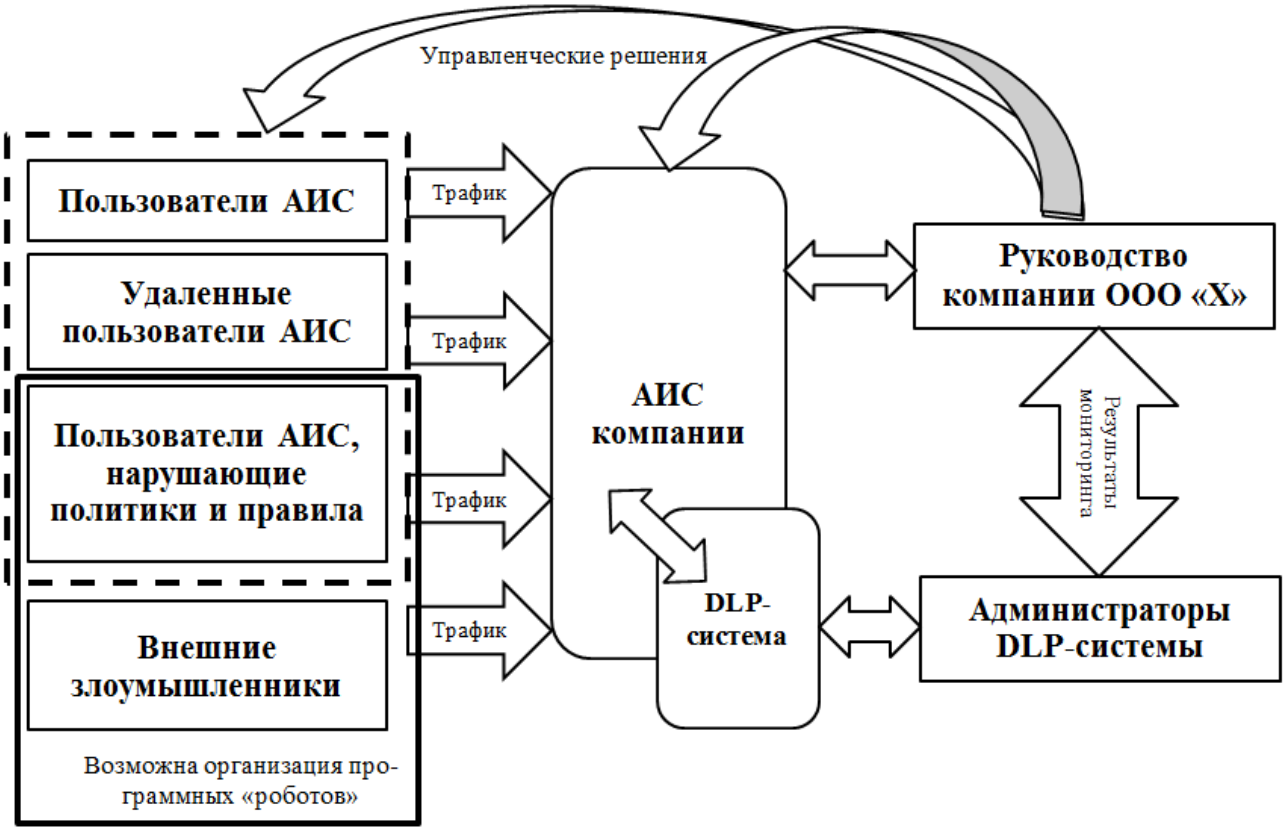

Рис. 2. *Распределение ролей участников игры и организация взаимодействия между ними (разработано автором)*

DLP-система «Контур информационной безопасности SearchInform» развернута в связи с имеющимися фактами нарушений порядка и правил использования информационных активов предприятия, описанных в политиках безопасности.

Частной политикой мониторинга действий пользователей в АИС организации администратору DLP-системы предписано предоставлять руководству результаты анализа сведений о событиях в системе не реже 1 раза в неделю, а при возникновении инцидентов ИБ или грубых нарушений – немедленно. При этом руководством вырабатываются управленческие решения, направленные на:

- АИС организации с целью совершенствования механизмов контроля и защиты ее информационных активов;
- сотрудников организации различных категорий по привитию им культуры поведения при работе в АИС и культуры информационной безопасности;
- управлению инцидентами информационной безопасности и проведению служебных расследований, связанных с ними.

Правила игры:

Руководителем игры является преподаватель, ведущий курс по дисциплине «Управление инцидентами информационной безопасности».

Руководитель игры обладает следующими полномочиями:

- осуществляет распределение группы (подгруппы) обучаемых по ролям;
- выдает обучаемым общие материалы, групповые или индивидуальные задания и контролирует их подготовку;
- осуществляет контроль за действиями обучаемых в процессе игры;
- оценивает действия обучаемых в соответствии с принятыми критериями, т.е. является экспертом;
- подводит итоги игры.

Технология деловой игры состоит из следующих этапов [8]**.**

Этап подготовки. Условно говоря, основу этапа подготовки составляет разработка игровой модели, которая была раскрыта в ранее изложенном материале.

Этап ввода в игру. Данный этап заключается в ориентации всех категорий участников. Определяется режим работы, осуществляется постановка проблемы. Обучаемым выдаются материалы для подготовки. Осуществляется (при необходимости) сбор дополнительной информации. При необходимости обучаемые обращаются к руководителю игры за консультацией.

В процессе данного этапа допускаются предварительные контакты между участниками игры. Однако правилами игры запрещается следующее:

- отказываться от полученной, по решению руководителя, роли;
- самостоятельно выходить из игры;
- пассивно относиться к игре, подавлять активность, нарушать этику поведения.

К последнему положению необходимо сделать некоторые пояснения. Мнения коллег на кафедре разошлись относительно этичности существования в игре таких ролей, как нарушитель политики безопасности компании, а, проще говоря, ее сотрудник, допускающий по каким-либо мотивам нарушения, а также внешний злоумышленник (хакер) и необходимости их активной работы в ходе игры.

Одни считают, что это является недопустимым, так как, якобы предполагает обучение студентов неэтичным приемам работы в АИС организации. Другие стоят на позиции, что в этом нет ничего предосудительного, так как:

- во-первых, студенты старших курсов, а данный курс читается им на 4-ом курсе, прекрасно знают обо всех угрозах безопасности информации, в условиях актуальности которых осуществляется функционирование АИС любой организации;
- во-вторых, постановка задачи на подобные действия и их выполнение осуществляется преподавателем, или под его контролем и проводится полностью открыто;
- в-третьих, подобными действиями осуществляется подтверждение тенденции, неоднократно показанной в статистиках нарушений и заключающейся в существовании постоянной угрозы средствам и активам АИС организаций от неподготовленности (некомпетентности) персонала.

Можно и дальше продолжить перечень доводов. Наконец, в дальнейшем, при проработке всех механизмов игры, нами планируется разработка программных «роботов», которые с заданной руководителем последовательностью будут генерировать трафик событий, являющихся фактами нарушения политики безопасности (рис.2).

Этап проведения – это непосредственно сам процесс игры, который должен сопровождаться обязательным выполнением некоторых правил:

- с началом игры никто не имеет права вмешиваться в нее и изменять ее ход;
- право корректировки действия участников игры имеет только руководитель и только в тех случаях, когда участники уходят от главной цели игры.

Реализация сценария игры осуществляется следующим образом.

Все участники занимают места в двух учебных аудиториях. Участники игры, которые выполняют роли нарушителей, располагаются в отдельной аудитории, так как им предстоит выполнять специфические действия, имитирующие действия нарушителей (злоумышленников) под непосредственным контролем руководителя игры.

Участники игры, выполняющие роли сотрудников организации и удаленных пользователей АИС, выполняют задания в соответствии с их ролями. Результатом выполнения является трафик событий в АИС ООО «Х», параметры которого поступают на вход DLP-системы (рис.3). При этом участники выполняют свои задания с таким расчетом, чтобы с учебными и познавательными целями задействовать как можно больше ресурсов DLP-системы:

- редактируют документы;
- отправляют документы на печать и по электронной почте;
- пользуются ресурсами и сервисами интернет (http, ftp);
- подключают и используют в работе мобильные устройства типа съемных дисков, смартфонов, планшетов и др.;
- организуют между собой и с руководством компании общение с использованием службы немедленных сообщений, skype и подобных.

К этому трафику «подмешивается» информация о событиях, которые по своему содержанию представляют факты нарушений политики безопасности. Это может быть:

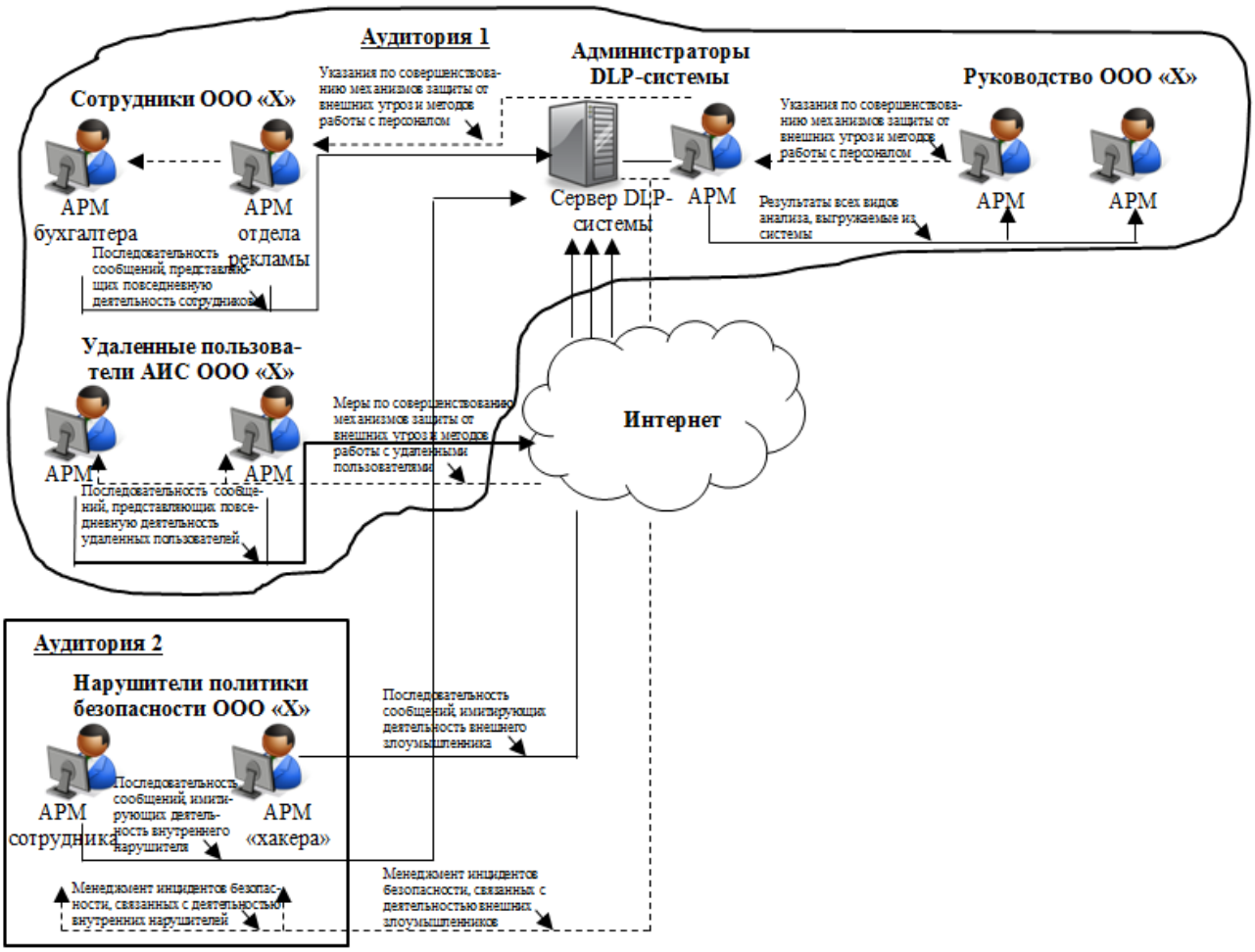

Рис. 3. *Реализация сценария деловой игры (разработано автором)*

- посещение интернет-сайтов, содержание которых не связано с исполняемыми сотрудниками должностными обязанностями;
- пересылка по электронной почте сообщений, содержащих «контролируемые» выражения;
- отправка на печать документов с грифом «Коммерческая тайна»;
- копирование документов с грифом «Коммерческая тайна» на мобильные носители;
- использование в процессе общения с применением служб мгновенных сообщений, skype и подобных «контролируемых» выражений, и другие.

В период, когда вышеперечисленные игроки занимаются «нагоном» трафика, администраторы DLP-системы выполняют следующие виды работ:

- проверяют работоспособность серверной и клиентских частей DLP-системы «**Контур информационной безопасности SearchInform**»;

- контролируют перечень активных компонентов системы и соответствие их параметров и настроенных реакций требованиям политики безопасности организации;
- администрируют серверную часть системы;
- контролируют работу модуля управления «Alert Center»;
- обрабатывают результаты мониторинга событий и выделяют из них те, которые имеют признаки относящихся к инцидентам безопасности;
- представляют выделенные события группе руководителей с заданной руководителем игры периодичностью (15-20 минут) исходя из продолжительности занятия.

В этот же период времени игроки группы руководителей выполняют следующие работы:

- руководят деятельностью администраторов;
- получают с заданной периодичностью результаты мониторинга;
- оценивают характер выделенных событий, заслуживающих немедленного реагирования;
- совместно с администраторами системы проводят анализ событий с целью определения признаков инцидентов;
- по выделенным инцидентам, а также в случае подозрения на таковые проводят работу с подчиненными из групп игроков: с сотрудниками организации, находящимися в аудитории 1 - непосредственным общением; с удаленными сотрудниками – по электронной почте и с использованием других средств. Если установлено, что выявленные инциденты или их признаки связаны с деятельностью внешних злоумышленников, то руководители вместе с администраторами (офицерами безопасности) вырабатывают контрмеры по минимизации последствий злоумышленных воздействий на функционирование АИС организации.

Подведение итогов деловой игры.

Подведение итогов проводится руководителем игры.

Каждая группа игроков к подведению итогов готовит отчет об участии в игре и достигнутых результатах, и самостоятельно (в случае недостаточной самостоятельности студентов – с помощью руководителя или помощника) выбирает одного из участников для выступления.

В процессе подведения итогов проводится заслушивание одного студента из каждой группы игроков. В процессе заслушивания студент докладывает результаты своего участия в игре по следующим позициям:

- характер выполняемой роли;
- общий объем выполненной работы, при этом должны быть применены единицы измерения для четкой квалиметрии результатов и последующего выставления оценки за занятие. Примерами таковых единиц измерения могут быть: количество затраченного времени в мин., час.; количество созданных (отправленных) сообщений в ед.; параметры созданного потока событий (трафика) в ед/час., количество событий, выделенных модулями DLP-системы в

соответствии с правилами мониторинга по категориям, в ед.; относительная частота срабатывания модулей DLP-системы, в % от общего, и другие;

- отдельно объем работы, который должен повлиять на показатели работы другой группы, например «злоумышленник - администратор», или «администратор - руководитель».

Оценку каждому студенту выставляет руководитель. При выставлении оценки руководитель занятия учитывает, как формальные, так и неформальные критерии.

К студентам, играющим роли сотрудников, удаленных пользователей и нарушителей более применимы формальные критерии в виде оценок результатов их работы, показанных выше; а к оцениванию студентов, играющих роли администраторов и руководителей, более применимы неформальные критерии, оценивающие логичность, целесообразность и корректность выработанных рекомендаций и решений.

Заключение

Опыт проведения деловых игр в процессе изучения дисциплины «Управление инцидентами информационной безопасности» позволяет сделать некоторые выводы:

- правильно разработанная, активно и эффектно проведенная деловая игра, безусловно, является эффективным способом формирования профессиональных компетенций студентов, а, кроме этого, это еще и очень яркое событие в их «учебной» жизни, о котором студенты помнят очень долго;
- перед проведением учебного занятия с реализацией подобной формы необходимо реально оценить профессиональную, деловую, моральную готовность обучаемых к этому, в противном случае из-за пассивности студентов есть риск превращения деловой игры в «тягомотину». Кстати, мы проводили занятия по данной теме и в традиционных (лекция – семинар – практическое занятие) формах;
- реализация игрового метода в учебном процессе является весьма трудоемким и затратным делом, которое нельзя проводить как другие формы занятий «с колес», поэтому обилие деловых игр в учебном процессе должно вызывать, в первую очередь не восторг, а сомнение в их качестве;
- проведению игры со студентами должен предшествовать ряд репетиций с полным «прогоном» всех ее элементов и проверкой готовности всех видов обеспечения: методического, материально-технического, программного и др. Сбои в работе техники, программных средств в процессе игры могут только дискредитировать этот прогрессивный метод.

Кроме этого, необходимо обозначить и некоторые проблемы, которые, на наш взгляд необходимо решать в дальнейшем.

Первая проблема заключается в тяготении значительной части преподавателей к традиционным формам проведения занятий. Здесь нельзя однозначно сказать к какой возрастной категории относятся последние, так как наши наблюдения свидетельствуют о том, что некоторые возрастные преподаватели весьма активно используют их, а более молодые – наоборот, сторонятся.

Вторая проблема тесно связана с первой и выражается в необходимости больших временных и материальных затрат на внедрение игровых форм в учебный процесс, а

реальный эффект от их реализации появится, начиная со 2-й и далее реализации одной и той же учебной программы дисциплины, что в современных условиях проблематично.

Третья проблема связана со значительным количеством обучаемых по направлению «Информационная безопасность» на кафедре ИЭБ и назревшей необходимостью частичной виртуализации учебного процесса. Однако данная необходимость находится в противоречии с описанной выше методикой проведения деловой игры, потому что применение дистанционных технологий в обучении предполагает возможность участия игроков в произвольные моменты времени, что не позволит создать динамичную информационную обстановку игры.

Перечень проблем можно продолжить, однако в качестве основного вывода скажем, что на примере описанной деловой игры нами осознана важность подобных учебных мероприятий для реализации компетентностного подхода в образовательной деятельности.

ЛИТЕРАТУРА

1. Ковалёв А. Как выбрать DLP-систему? [Текст] - М. PC Week/RE «Компьютерная неделя») №42 (744) 9 - 15 ноября 2010 г.
2. Дрозд А.В. SearchInform усовершенствовала свои продукты обеспечения безопасности информации, материалы официального сайта компании SearchInform, [Электронный ресурс], http://searchinform.ru/news/products/3390/.
3. Невский А.Ю. Пресс-релиз «SearchInform наладила сотрудничество с Институтом безопасности бизнеса Национального Исследовательского университета МЭИ», материалы сайта электронного журнала «Директор по безопасности», [Электронный ресурс], http://www.s-director.ru/news/view/1326.html.
4. Невский А.Ю. Без погон, но офицеры, [Текст] – М., Журнал BIS-Journal - Информационная безопасность банков, №4, 2013.
5. Подопригора М.Г. Деловая этика, Учебное пособие, [Текст] - Таганрог: Изд-во ТТИ ЮФУ, 2012.
6. Басова Н.В. Педагогика и практическая психология, [Текст] - Ростов н/Д: Изд-во «Феникс», 2000.
7. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей, Учебник [Текст] - М: Изд-во «Academia», 2006.
8. Панфилова А.П. Инновационные педагогические технологии, Учебное пособие, [Текст] - М: Изд-во «Академия», 2009.

Рецензент: Писаренко Игорь Викторович, заместитель начальника отдела информационной безопасности Управления обеспечения безопасности, кандидат технических наук, доцент, Коммерческий банк ВТБ24 (ЗАО).

Nevsky Aleksander Jurjevich
National Research University "Moscow Power Engineering Institute"
Russia, Moscow
E-mail: NevskyAY@mpei.ru

Experience opportunities DLP-systems in a business game in preparation of bachelors in information security

Abstract. This article discusses the experience of conducting business games with a bachelors in education, in the direction of Information security at the Department of information and economic security National Research University "Moscow Power Engineering Institute". In particular, consider the scenario of business games played while studying the discipline "Management of information security incidents", where the software is used one of the versions, the so-called DLP-systems, widely used at present for monitoring user behavior in automated information systems (AIS) organizations.

Conducting business game designed to significantly increase the interest of students to the practice of implementation of DLP systems, and use their resources in the process of investigation of information security incidents in the AIS organization.

Keywords: futomated information system; DLP-system; competence; monitoring; information security incident; business game; information leakage; sniffer; SearchInform information security system; security policy; role; event traffic; the evaluation criteria.

REFERENCES

1. Kovalev A. Kak vybrat' DLP-sistemu? [Text] - M. PC Week/RE «Komp'yuternaya nedelya») №42 (744) 9 - 15 noyabrya 2010.
2. Drozd A.V. SearchInform usovershenstvovala svoi produkty obespecheniya bezopasnosti informacii, materialy oficial'nogo sajta kompanii SearchInform, [Elektronnyj resurs], http://searchinform.ru/news/products/3390/.
3. Nevskij A.YU. Press-reliz «SearchInform naladila sotrudnichestvo s Institutom bezopasnosti biznesa Nacional'nogo Issledovatel'skogo universiteta MEHI», materialy sajta ehlektronnogo zhurnala «Direktor po bezopasnosti», [Elektronnyj resurs], http://www.s-director.ru/news/view/1326.html.
4. Nevskij A.YU. Bez pogon, no oficery, [Tekst] – M., ZHurnal BIS-Journal - Informacionnaya bezopasnost' bankov, №4, 2013.
5. Podoprigora M.G. Delovaya ehtika, Uchebnoe posobie, [Tekst] - Taganrog: Izd-vo TTI YUFU, 2012.
6. Basova N.V. Pedagogika i prakticheskaya psihologiya, [Tekst] - Rostov n/D: Izd-vo «Feniks», 2000.
7. Platonov V.V. Programmno-apparatnye sredstva obespecheniya informacionnoj bezopasnosti vychislitel'nyh setej, Uchebnik [Tekst] - M: Izd-vo «Academia», 2006.
8. Panfilova A.P. Innovacionnye pedagogicheskie tekhnologii, Uchebnoe posobie, [Tekst] - M: Izd-vo «Akademiya», 2009.