УДК 614.8 + 002.6:004.89

А.А. Азаров

ОСНОВЫ МОНИТОРИНГА ЗАЩИЩЕННОСТИ ПЕРСОНАЛА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОТЕХНИЧЕСКИХ АТАК

Азаров А.А. **Основы мониторинга защищенности персонала информационных систем от социотехнических атак.**

Аннотация. Активное привлечение информационных технологий при ведении современного бизнеса выдвигает ряд требований к обеспечению безопасности используемых при этом информационных ресурсов. В связи с этим большинство специалистов в информационной безопасности занимается разработкой различных методов защиты информационных систем от технических атак. В последнее время все больше сотрудников отделов информационной безопасности начинает обращать внимание на проблемы защищенности пользователей информационных систем (ИС). Про социотехнические (социо-инженерные) атаки говорят большинство авторов рассмотренных статей, но ни в одной из них нет сведений о решении задач автоматизированной оценки степени защищенности персонала информационных систем или задач оценки эффективности мероприятий, направленных на предотвращение таких атак. Целью данной статьи является краткий аналитический обзор научной литературы по тематике информационной безопасности, который позволит перечислить как существующие потребности в области анализа защищенности пользователей информационных систем, так и выявленные автором предпосылки к развитию новых подходов такого анализа.

Ключевые слова: социо-инженерная атака, социотехническая атака, информационная система, пользователь.

Azarov A.A. **Monitoring bases of informational system's personnel' security from sociotechnical attacks.**

Abstract. Active attraction of information technologies when conducting modern business puts forward a number of requirements to safety of information resources used thus. In this regard the majority of experts in information security is engaged in development of various methods of protection of information systems from technical attacks. Recently more and more the staff of departments of information security starts paying attention to problems of security of users of the information systems. About sociotechnical (socio-engineering) attacks tell the majority of authors of considered articles, but in one of them there are no data on the solution of problems of the automated assessment of degree of security of the personnel of information systems or problems of an assessment of efficiency of the actions directed on prevention of such attacks. The purpose of this article is the short state-of-the-art review of scientific literature on subject of information security which will allow to list as existing needs for the analysis of security of users of information systems, and the preconditions revealed by the author to development of new approaches of such analysis.

Keywords: socio-engineering attack, sociotechnical attack, informational system, user, user's vulnerabilities profile.

1. Введение. Активное привлечение информационных технологий при ведении современного бизнеса выдвигает ряд требований к обеспечению безопасности используемых при этом информационных ре-

сурсов. В связи с этим большинство специалистов в информационной безопасности занимается разработкой различных методов защиты информационных систем от технических атак [22, 23, 34, 39, 40, 55, 56, 57, 58, 59, 60] . В последнее время все больше сотрудников отделов информационной безопасности начинает обращать внимание на проблемы защищенности пользователей информационных систем (ИС). Про социотехнические (социо-инженерные) атаки говорят большинство авторов рассмотренных ниже статей, но ни в одной из них нет сведений о решении задач автоматизированной оценки степени защищенности персонала информационных систем или задач оценки эффективности мероприятий, направленных на предотвращение таких атак. Тем не менее, решение данных проблем крайне важно по двум причинам:

1) руководителю организации необходимо иметь средства для самостоятельного, в значительной степени независимого измерения степени защищенности персонала, задействованного в бизнес-процессах, протекающих в его организации, а не полностью полагаться на специалистов из служб безопасности и информационной безопасности;
2) руководителю организации необходимо оценивать затраты на проведение комплекса мер по обеспечению/актуализации защиты от социо-инженерных (социотехнических) атак с учетом его ожидаемой эффективности, а также обладать полной информацией о преимуществах внедрения данного комплекса.

Целью данной статьи является краткий аналитический обзор научной литературы по тематике информационной безопасности (ИБ), который позволит перечислить как существующие потребности в области анализа защищенности пользователей информационных систем, так и выявленные автором предпосылки к развитию новых подходов такого анализа.

В современных исследованиях по ИБ выделяются следующие направления: исследование и классификация угроз ИБ, анализ и исследование социотехнических атак на ИС и различные методы защиты информационных систем от деструктивного поведения пользователей с помощью ограничения их прав доступа. Рассмотрим каждое из этих направления и достигнутые в них наработки в отдельности.

2. Угрозы информационной безопасности. Существует ряд различных классификаций угроз ИБ [16, 23, 30, 40, 55 - 59]. Как правило, авторы делят угрозы информационной безопасности по одному или нескольким признакам [40, 55 - 58]. В то же время, выделяются публи-

кации [19, 58], в которых приведены наиболее полные перечни угроз ИБ, построенные на основе более широкого набора базовых признаков. Поэтому такая классификация носит более общий характер и включает в себя ранее упомянутые классификации. Следуя данной классификации можно строго формализовать атрибуты угроз ИБ. Приведем доработанный в некоторой степени вариант подобной классификации (за основу взята классификация, приведенная в [58]). Выделяются следующие базовые признаки:

- По природе возникновения [58]
  - Естественные угрозы (связаны с протеканием физических процессов) [58]
  - Искусственные угрозы (связаны с деятельностью человека) [58]
- По степени преднамеренности проявления [58]
  - Преднамеренные действия
  - Непреднамеренные действия
- По непосредственному источнику угроз [58]
  - Не зависящие от человека (например, стихийные бедствия) [58]
  - Надежность аппаратно-технического обеспечения организации [58]
  - Угрозы, исходящие от пользователей ИС [58]
- По положению источника угроз [58]
  - Внутренние угрозы по отношению к ИС
    - Неквалифицированные организационные меры руководства компании, регламентирующие управление безопасностью и работу с информационными ресурсами; [56]
    - Не достаточная квалификация персонала, обеспечивающего управление объектом защиты; [56]
    - Преднамеренные и непреднамеренные действия персонала по нарушению безопасности; [56]
  - Внешние угрозы по отношению к ИС
    - Угрозы конкурентов компании, нацеленных на получение большей доли на рынке и вытеснение организации;
    - Вирусные угрозы, обеспечивающие утечку конфиденциальной информации по каналам связи. Утечка конфиденциальной информации на неправильно утилизированных носителях (как бумажных, так и электронных);
    - Несанкционированное проникновение на объект защиты; [56]

- Стихийные бедствия (пожары, наводнения ураганы и т.д.); [56]
- Преднамеренные и непреднамеренные действия поставщиков технических устройств, программного обеспечения и услуг по обеспечению информационной безопасности. [56]

- По степени зависимости от активности АС [58]
  - Независимые угрозы (например, хищение информации, подбор паролей и т.д.) [58]
  - Зависимые угрозы (например, распространение вирусов возможно только в работающей ИС) [58]
- По степени воздействия на АС [58]
  - Угрозы, изменяющие структуру ИС [58]
  - Угрозы, не изменяющие структуру ИС [58]
- По этапам доступа пользователей или программ к ресурсам АС [58]
  - Угрозы, связанные с несанкционированным доступом к ИС
  - Угрозы, связанные с некорректным использованием информационных ресурсов ИС
- По способу доступа к ресурсам АС [58]
  - Прямой доступ к ресурсам ИС (с помощью авторизированных записей пользователей) [58]
  - Скрытый, несанкционированный доступ к ресурсам ИС [58]
- По текущему месту расположения информации, хранимой и обрабатываемой в АС [58]
  - Угроза утечки информации с жестких дисков [58]
  - Угроза утечки информации из оперативной памяти [58]
  - Угроза утечки информации с визуализирующих устройств и печатных носителей [58]
  - Угроза утечки информации из сетевого трафика [58]

Также в [23, 30, 59] авторы рассматривают классификацию технических угроз безопасности ИС, приводятся различные варианты защиты ИС от тех или иных угроз ИБ. Таким образом, можно сделать вывод о больших наработках в области обеспечения ИБ ИС с технической точки зрения. Следует отметить, что во всех перечисленных статьях, а также в [16], авторы говорят о высокой доле влияния на обеспечение ИБ именно пользователей информационных систем. Тем не менее, в [16, 23, 30, 40, 55 - 59] авторы не предлагают никаких методов защиты ИС от деструктивного поведения пользователей и защиты самих пользователей от влияния извне, направленного на получение конфиденциальной информации. Подробнее данный тип атак рассматривается в следующих разделах.

3. Социотехнические методы несанкционированного доступа к информации. В [22, 34, 39, 60] авторы приводят различные варианты анализа социотехнических атак и перечни социотехнических атак. Стоит особо отметить сильную корреляцию текстов разных статей с различными авторскими коллективами. Приведем ряд статей и рассмотрим выдвинутые авторами идеи.

В [22, 34, 39, 60] авторы рассматривают социотехнические методы доступа к информации. Для проведения атак злоумышленники, применяющие методы социотехники, эксплуатируют в своих целях доверчивость, лень, любезность и даже энтузиазм сотрудников организации. Злоумышленник пытается убедить сотрудников компании предоставить ему информацию, обеспечивающую доступ к корпоративным ИС или их ресурсам. Атаки, основанные на методах социотехники, в [22, 34, 39] разделены на пять основных направлений:

- сетевые атаки,
- телефонные атаки,
- поиск информации в мусоре, офисных отходах,
- персональные подходы,
- обратная социотехника.

Рассматриваются ситуации, когда пользователь полностью осознает неправомерность осуществляемых действий. В [22, 34, 39, 60] говорится о крайне высокой степени уязвимости пользователей сети Интернет, связанной в первую очередь с тем, что многие пользователи зачастую используют одну и ту же пару логин-пароль на различных интернет ресурсах, будь то электронная почта, социальная сеть или что-то еще. К сожалению, данные утверждения авторов статей [22, 34, 39] не подкреплены данными каких-либо проведенных исследований.

Следует отметить, что многие авторы указывают на такую распространенную уязвимость как использование сервисов, обеспечивающих мгновенный обмен сообщениями. Используя такие сервисы, злоумышленники могут налаживать отношения с сотрудниками компаний, оставаясь при этом анонимными, и обманным путем убеждать сотрудника компании предоставить им нужную информацию, приводя обоснованные правдоподобные доводы. Данные статьи позволяют эксплицировать на невысказанную им открыто мысль о том, что злоумышленник может использовать объединение технических и социотехнических атак. Так, например, в [34, 39] указывается на брешь в защите, связаную с несанкционированным анализом мусора. Злоумышленник может получить представление о структуре компании и,

затем, совершать социотехнические атаки, уже обладая некоторой информацией и, как следствие, вызывая меньше подозрения.

В работе [39] говорится о том, что злоумышленники пытаются создать совершенную психологическую среду для атаки. Основными методами убеждения, по мнению автора, являются: олицетворение, покорение, соответствие, разделение ответственности и простое дружелюбие. Также автор приводит широко распространенный пример хакерской атаки на информационную систему, заключающейся в следующем. Сначала хакер подрывает деятельность сети, создавая определенные программные ошибки. Затем он представляется тем специалистом, который может решить проблемы, а когда приходит выполнить эту работу, запрашивает у сотрудников требуемую ему информацию. Таким образом злоумышленник получает те данные, которые ему требовались. Аналогичные ситуации могут быть получены из-за деятельности инсайдеров, как описано в [66]. В этом случае пользователь, узнавший о своем скором увольнении, закладывает логическую бомбу в работу информационной системы и затем, после увольнения и запуска данной бомбы, возвращается как высокооплачиваемый сотрудник, способный решить проблемы компании. В заключении авторы отмечают, что для защиты от атак, основанных на методах социотехники, нужно изучить их разновидности, понять, что нужно злоумышленнику, и оценить ущерб, который может быть причинен организации. Кроме того, авторы указывают на методы, которые могут помочь в увеличении степени защиты корпоративных сетей организации. В частности предлагается доработка политик безопасности, так как большинство из подобных политик регламентируют лишь технические средства защиты. В то же время, ни в одной из статей [22, 34, 39] не учитывается квалификация персонала, в то время как данная характеристика является наиболее важной так как необученный персонал не сможет воспринимать доработанные политики безопасности. В статье [60] представлены практические рекомендации, нацеленные на увеличение степени защищенности пользователей информационных систем. Среди таких рекомендаций следующие: организация платформы, к которой пользователи и сотрудники могли бы обратиться в случае, если замечены подозрительные попытки собрать определенную информацию; повышение уровня подготовки пользователей. Тем не менее, ни в оной из статей [22, 34, 39, 60] не предлагаются подходы к оценке уровня защищенности персонала информационных систем, а также способы измерения эффективности результатов реализации предложенных мер.

Авторы [21] представляют организацию «Учебный центр «Информзащита», к одной из основных услуг которой относится внедрение комплексной программы повышения осведомленности персонала информационных систем об угрозах информационной безопасности. Данный курс рассчитан на повышение компьютерной грамотности пользователей, что влечет за собой повышение уровня защиты таких пользователей информационных систем от социо-инженерных атак, а также значительно снижает вероятности инсайдерских атак. В статье [42] авторским коллективом были рассмотрены возможные варианты оправдания правовой борьбы против инсайдеров в информационной системе. К сожалению, данная борьба возможна только в двух случаях: в случае совершения инсайдерами противоправных действий, а также в случае обнаружения этих действий и наличия достаточной доказательной базы. Авторы отмечают, что необходимо заранее прогнозировать возможное деструктивное поведение пользователей на основании их психологических характеристик. Данная мера позволит не только обеспечить безопасность информационной системы, но также уменьшить затраты на выявление инсайдеров, так как данный подход позволяет строить вероятностные оценки того, в какой степени пользователь подвержен тем или иным видам атак. Кроме того, авторы описывают личный опыт столкновения с социо-инженерными атаками, например такими, как описано в [33], и предлагают стандартный перечень мер для противодействия таким атакам (стать менее доверчивыми и не лениться обращаться в компетентные органы). Однако причины восприимчивости пользователя к тому или иному типу социо-инженерных атак не анализируются. Кроме того, вопросы эффективности перечисленных мер и количественной оценки их влияния на защищенность пользователей остаются не решенными. Также, в статье [26] авторы говорят о необходимости контроля пользователей с помощью «четких и продуманных правил и регламентов». В частности они рекомендуют «проводить мониторинг электронной почты сотрудников, блокировать доступ к определенным сайтам и запрещать использование некоторых портов». Такие меры могут, по мнению авторов, помешать злоумышленнику влиять на пользователей. Тем не менее, они не устраняют первопричины восприимчивости пользователей к влияниям извне. По нашему мнению, такой контроль не является препятствием для атак инсайдеров на информационные системы. Кроме того, тотальный контроль может существенно замедлить или вообще прекратить нормальное функционирование бизнес-процессов в организации.

Диссертация [32] посвящена разработке методики оценки информационной защищенности социотехнических систем с использованием функций чувствительности. Автор вводит понятие социотехнических информационных систем (СТИС). Отмечено, что функционирование таких систем характеризуется многообразием и сложностью влияния на СТИС социальных, экономических, политических, природных, технических и других факторов, приводящих к поступлению в систему новой для нее информации. Также автор говорит о том, что новая информация, поступающая извне, и возмущения, происходящие внутри системы, приводят к модификации исходных данных, необходимых для функционирования системы и ее защиты. При этом могут меняться цели, решаемые задачи и ресурсы социотехнической системы, поэтому ее защита также должна постоянно модифицироваться. В связи с этим необходима разработка эффективной модели, устанавливающей связь процессов обработки и накопления информации с проявлениями различного рода дестабилизирующих факторов. Утверждается, что наиболее точную оценку степени защищенности СТИС возможно получить только на основе исследования движения характеристик системы при воздействии дестабилизирующих факторов. Таким образом, автор данной диссертации фактически проводит анализ изменения информационной системы под действием различных внешних факторов и, как следствие, анализ соответствующих изменений доступности данных в данной системе. Отметим, однако, что автор уделяет недостаточно внимания пользователям информационной системы, в то время как в любой момент времени жизнедеятельности СТИС пользователи могут несанкционированно модифицировать и/или удалять данные из этой информационной системы как самостоятельно, так и под действием злоумышленника.

Документ [38] является политикой информационной безопасности «Газпромбанк». В [38] при построении модели нарушителя происходит деление на внешних и внутренних нарушителей. В качестве потенциальных внутренних нарушителей банком рассматриваются зарегистрированные пользователи информационных систем банка; сотрудники банка, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем банка, но имеющие доступ в здания и помещения; персонал, обслуживающий технические средства корпоративной информационной системы банка; сотрудники самостоятельных структурных подразделений банка, задействованные в разработке и сопровождении программного обеспечения; сотрудники самостоятельных структурных подразделений,

обеспечивающие безопасность банка; руководители различных уровней. Потенциальными внешними нарушителями являются бывшие сотрудники банка; представители организаций, взаимодействующих по вопросам технического обеспечения банка; клиенты банка; посетители зданий и помещений банка; конкурирующие с банком кредитные организации; члены преступных организаций; сотрудники спецслужб или лица, действующие по их заданию; лица, случайно или умышленно проникшие в корпоративную информационную систему банка из внешних телекоммуникационных сетей (хакеры). В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других сотрудников банка;
- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности потенциальный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

Таким образом, современная политика обеспечения безопасности в банках, подобных [38], предполагает анализ защищенности пользователей информационных систем от социо-инженерных и социотехнических атак, но подходы к защите не до конца формализованы. В то же время, из политики информационной безопасности следует, что никаких мер, предупреждающих противоправные действия сотрудников, не предусмотрено, предполагается активное вмешательство службы безопасности уже после совершения противоправного действия.

Подводя итог, хочется отметить общее понимание исследователями того факта, что необходимо защищать пользователей информационных систем и что именно от них исходят многие угрозы ИБ ИС. В то же время нет общего понимания и проработанных, эффективных методик повышения уровня защищенности пользователей информационных систем. Также не разработаны метрики, показывающие текущий уровень защищенности пользователей информационных систем.

4. Краткий обзор предлагаемых методов выявления достаточных для работы с критичной информацией прав пользователя. Данный раздел посвящен обнаруженным в результате данного обзора методам выявления достаточных для работы с критичной информацией прав пользователя. На сегодняшний день данный подход является наиболее распространенным среди специалистов в информационной безопасности методом противодействия инсайдерским атакам и социо-инженерным атакам на пользователей информационных систем.

Во всех статьях [24, 25, 27, 28, 29, 64] указывается на избыточность прав пользователей, работающих с критичной информацией. Данная избыточность является основным источником злоупотребления пользователями ИС своими правами с целью получения конфиденциальной информации компании и передачи ее злоумышленнику. Все предложенные авторами подходы связаны с анализом текущей деятельности пользователя и выявлением аномального поведения пользователя относительно его предшествующего поведения в информационной системе. Таким образом, предлагаемые подходы позволяют выявить совершаемое деструктивное поведение пользователя в информационной системе и прекратить его. Процедуры выявления деструктивного поведения пользователя и прекращения подобных действий требуют больших информационных и организационных ресурсов. В то же время, можно уменьшить количество затрачиваемых ресурсов, если проводить профилактику подобных действий. Никаких методов профилактики деструктивного поведения пользователей авторы статей [24, 25, 27, 28, 29, 64] не предлагают. Рассмотрим подробнее предложенные подходы.

В диссертации [64] автор указывает на необходимость разработки функционально-ролевой модели разграничения доступа в социотехнических информационных системах на основе среды радикалов. В данной диссертации разработана модель злоумышленника, названная автором «активатором монитора безопасности». Следует отметить, что автор выработал методы оценивания безопасного выполнения коллективных информационных задач, другими словами, не рассматривается индивидуальность каждого отдельного пользователя, а исследуется коллектив пользователей как единый организм. Таким образом, не могут быть рассмотрены социо-инженерные атакующие воздействия злоумышленника на пользователей информационной системы. Данный подход применим для экспресс-оценки защищенности пользователей информационных систем, основанный на общем уровне подготовки и осведомленности пользователей. В то же время, данный подход с тру-

дом масштабируется на задачи анализа защищенности каждого отдельно взятого пользователя.

В [27, 28, 29] авторы рассматривают проблему моделирования атак в больших информационных системах, отмечая, что данное моделирование затруднено из-за неполноты и неопределенности информации, доступной для использования средствами моделирования, а также большой вычислительной сложностью алгоритмов построения и анализа моделей атак. Авторы отмечают несколько вариантов моделирования атак в сложных информационных системах. В качестве дальнейших планов развития авторы указывают на AMSEC компоненту SIEM-систем и выдвигаю ряд предложений по ее развитию. Основной функцией SIEM-систем является обработка большого количества событий безопасности, порождаемых различными системами, и генерация на их основе инцидентов информационной безопасности (то есть нарушений конфиденциальности, целостности или доступности информации). От миллионов сообщений и log-записей осуществляется переход к небольшому количеству настоящих инцидентов ИБ. Авторы статьи совместно со своими европейскими коллегами выполняют проект по построению компонентов SIEM-систем нового поколения. Данный проект должен предоставить инновационные методы для обнаружения возникающих угроз безопасности и инициирования действий, направленных на восстановление безопасности до непосредственного возникновения возможных инцидентов. Такой результат предполагается достичь за счет формирования уведомлений в режиме, близком к реальному времени, а также за счет применения проактивного управления инцидентами и событиями. Таким образом, авторский коллектив занимается разработкой подхода, позволяющего выявить или уже свершившееся правонарушение, или остановить неправомерные действия пользователя.

В [24, 25] затронута проблема внутренних нарушителей в критически важных инфраструктур (КВИ), обладающих высокими требованиями к непрерывности функционирования и защищенности обрабатываемой информации. В самом начале статьи авторы говорят о том, что «опасность данных угроз определяется их непредсказуемостью, наличием у пользователя полномочий по доступу к защищаемым ресурсам». Авторы указывают, что проблемы предотвращения несанкционированного использования защищаемых ресурсов КВИ и предотвращения использования ресурсов неполномочным способом решается двумя основными путями: разграничением доступа и организационными мерами. Предложено динамическое управление доступом, раз-

работанное на основе учета информационных профилей пользователей. Авторы, ссылаясь на то, что действия пользователя в КВИ носят типовой характер, вводят понятие типичных действий, как действий, отклоняющихся от типовой схемы. Авторы говорят об априорной и контекстной избыточностях прав пользователя, которые ведут к избыточности прав пользователя при выполнении возложенных на них задач. Предлагаемый авторами подход заключается в формировании иерархического информационного профиля пользователя, который строится по ходу выполнения пользователем различных задач. В дальнейшем такой профиль используется при оценке степени атипичности поведения пользователей. Таким образом, применение такого подхода, по утверждению авторов, приводит к снижению возможностей пользователя по совершению атипичных действий. Полученный авторами подход позволяет выявить уже существующее нарушение информационной безопасности, при этом выявить готовящееся нарушение и провести ряд контрмер предложенный подход не позволяет.

Предлагаемые подходы, несмотря на очевидное преимущество, которое заключается в серьезном усложнении проведения инсайдерских атак, не устраняет угрозу таких атак. Кроме того, данные подходы позволяют сравнительно легко выявить пользователей, замешанных в утечке информации, в то же время они не предлагают абсолютно никаких мер диагностики и профилактики подобного деструктивного поведения пользователей.

5. Заключение. Представленный обзор показывает, что проблема анализа защищенности пользователей информационных систем от социо-инженерных (социотехнических) атак является актуальной, необходимость поиска путей решения которой подчеркивают многие специалисты в области информационной безопасности [31, 65]. В то же время, очевидно, что данная проблема имеет междисциплинарный характер, что оказывается существенным препятствием как в развитии соответствующих теоретических положений, так и основывающихся на них методических и технологических решений. Однако можно указать серию работ [1-15, 17, 18, 20, 35-37, 41, 43-54, 61-63], с одной стороны, успешно комбинирующую подходы математики, информатики и социогуманитарных наук, а с другой стороны уже снабженную иллюстративными прототипами программной реализации методик автоматизированной оценки степени защищенности пользователей и критичной информации от социо-инженерных атак.

Литература

1. *Азаров А. А., ТулупьеваТ.В., Тулупьев А.Л., Пащенко А.Е* .Создание программного комплекса для анализа защищенности информационных систем с учетом человеческого фактора. // Современные информационные технологии и ИТ-образование. Сборник научных трудов VI Международной научно-практической конференции. М: МГУ. 2011. С. 470-477.
2. *Азаров А.А.* Анализ защищенности информационных систем от социоинженерных атак рекомпенсационного типа в отношении пользователей// VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011)» (Санкт-Петербург, 26–28 октября 2011 г.) Материалы конференции. СПб.: СПОИСУ, 2011. С. 160.
3. *Азаров А.А.* Визуальный JAVA-конструктор для формирования сцен реализации социоинженерных атак// Научная сессия МИФИ-2011. Аннотации докладов. В 3 т. Т. 3. М.: МИФИ, 2011. С. 90.
4. *Азаров А.А.* Математические аспекты применения психологического профиля уязвимостей пользователя для анализа защищенности информационных систем от социо-инженерных атак // Региональная информатика-2012 (РИ-2012). XIII Санкт-Петербургская международная конференция. Санкт-Петербург, 24--26 октября, 2012 г.: Материалы конференции / СПОИСУ. СПб., 2012. С. 78.
5. *Азаров А.А.* Прототип программного комплекса для получения агрегированных оценок вероятности ответных действий пользователя на социо-инженерное атакующее действие // XV Международная конференция по мягким вычислениям и измерениям. SCM-2012. (25–27 июня 2012 г. Санкт-Петербург). Сборник докладов. 2012. Т. 2. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2012. С. 108–111.
6. *Азаров А.А.* Разработка программного комплекса для анализа угроз безопасности информационных систем с учетом человеческого фактора // Каталог XIV Конкурса бизнес-идей, научно-технических разработок и научно-исследовательских проектов «Молодые, дерзкие, перспективные». СПб.: Лема. 2011. С. 27-28.
7. *Азаров А.А., Ванюшичева О.Ю.* Синтез агрегированных оценок вероятности реакций пользователя в ответ на социо-инженерное атакующее действие. // VI Международная научно-техническая конференция молодых специалистов, аспирантов и студентов «Математическое и компьютерное моделирование естественнонаучных и социальных проблем» (МК-70-912) (Пенза, 21-24 мая 2012 г.). П: Приволжский Дом Знаний. 2012. С. 117-120.
8. *Азаров А.А., Тулупьев А.Л., Тулупьева Т.В.* SQL-представление реляционно-вероятностных моделей социо-инженерных атак в задачах расчета агрегированных оценок защищенности персонала информационной системы // Труды СПИИРАН. 2012. Вып. 22. С. 31–44.
9. *Азаров А.А., Тулупьев А.Л., Тулупьева Т.В., Фильченков А.А.* Разработка вероятностно-реляционных моделей для представления комплекса «персонал-критичные документы-информационная система» // Региональная информатика-2012 (РИ-2012). XIII Санкт-Петербургская международная конференция. Санкт-Петербург, 24--26 октября, 2012 г.: Материалы конференции / СПОИСУ. СПб., 2012. С. 79.
10. *Азаров А.А., Тулупьева Т.В.* Разработка психологического профиля уязвимостей пользователя для анализа защищенности информационных систем от социо-инженерных атак // Региональная информатика-2012 (РИ-2012). XIII Санкт-Петербургская международная конференция. Санкт-Петербург, 24--26 октября, 2012 г.: Материалы конференции / СПОИСУ. СПб., 2012. С. 78–79.
11. *Азаров А.А., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л.* Развитие методов и моделей анализа защищенности информационных систем от социоинженерных атак на

основе применения реляционно-алгебраических представлений и алгоритмов// VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011)» (Санкт-Петербург, 26–28 октября 2011 г.) Материалы конференции. СПб.: СПОИСУ, 2011. С. 160-161.

12. *Азаров А.А., Тулупьева Т.В., Тулупьев А.Л., Ванюшичева О.Ю.* Комплекс программ для анализа защищенности пользователей информационных систем с учетом их психологически обусловленных уязвимостей. // 1-й Международный симпозиум «Гибридные и синергетические интеллектуальные системы: теория и практика» (Светлогорск, 29 июня –2 июля 2012 г.) Материалы 1-го международного симпозиума. В 2 т. Т. 1 К.: БФУ им. И. Канта. 2012. С. 144-154.
13. *Азаров А.А., Тулупьева Т.В., Григорьева О.Ю., Аверьянова А.И., Тулупьев А.Л.* Методы получения агрегированных оценок вероятности ответных действий пользователя на социо-инженерное атакующее действие // XV Международная конференция по мягким вычислениям и измерениям. SCM-2012. (25–27 июня 2012 г. Санкт-Петербург). Сборник докладов. 2012. Т. 2. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2012. С. 105–107.
14. *Азаров А.А., Тулупьева Т.В., Тулупьев А.Л.* Прототип комплекса программ для анализа защищенности персонала информационных систем построенный на основе фрагмента профиля уязвимостей пользователя. // Труды СПИИРАН. 2012. Вып. 21. С. 21–40.
15. *Азаров А.А., Тулупьева Т.В., Фильченков А.А., Тулупьев А.Л.* Вероятностно-реляционный подход к представлению модели комплекса «Информационная система – персонал – критичные документы». // Труды СПИИРАН. 2012. Вып. 20. С. 57–71.
16. *Бондаренко С.В.* «Электронное государство» как социотехническая система. // Центр прикладных исследований интеллектуальной собственности. Ростов-на-Дону. 2005. 6 с.
17. *Ванюшичева О.Ю.* Прототип комплекса программ для построения профиля психологически обусловленных уязвимостей пользователя. Диплоная работа. СПб.: СПбГУ, 2012.
18. *Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л., Азаров А.А.* Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками. // Труды СПИИРАН. 2011. Вып. 19. С. 34–47.
19. Возможные угрозы информационной безопасности и их специфика. URL: http://www.e-nigma.ru/stat/possible_threats_to_information_security_and_their_ specificity/ (Дата обращения 03.10.2012)
20. *Зельтерман Д., Суворова А.В., Пащенко А.Е., Мусина В.Ф., Тулупьев А.Л., Тулупьева Т.В., Гро Л.Е., Хаймер Р.* Диагностика регрессионных уравнений в анализе интенсивности рискованного поведения по его последним эпизодам // Труды СПИИРАН. 2011. Вып. 17. С. 33–46.
21. Информзащита. URL: http://www.itsecurity.ru/edu/about/edu_main.html (Дата обращения 03.10.2012)
22. Как защитить сеть и сотрудников компании от атак, основанных на использовании социотехники. URL: http://www.networkdoc.ru/bezopasnost-seti/kak-zaschitit-set-i-sotrudnikov-kompanii-ot-atak-osnovannich-na-ispolzovanii-sotsiotechniki.html (Дата обращения 03.10.2012)
23. *Касперсикй Е.* Современные угрозы информационной безопасности: классификация, причины и способы устранения. URL: http://www.nestor.minsk.by/sr/2004/04/40413.html (Дата обращения 03.10.2012)

24. *Кий А.В., Копчак Я.М., Саенко И.Б., Козленко А.В.* Динамическое управление доступом к информационным ресурсам в критически важных инфраструктурах на основе информационных профилей пользователей // Труды СПИИРАН. 2012. Вып. 21. С. 5–20.
25. *Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В.* Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. 2012. Вып. 21. С. 41–55.
26. *Кольдичева Ю.* Между служебным и личным. // Сети. 2005. №3.
27. *Котенко Д.И., Котенко И.В., Саенко И.Б.* Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. Вып. 22. С. 5–30.
28. *Котенко И.В., Саенко И.Б.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. Вып. 22. С. 84–100.
29. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. Вып. 20. С. 27–56.
30. *Котенко И.В., Шоров А.В.* Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода “нервная система сети” // Труды СПИИРАН. 2012. Вып. 22. С. 45–70.
31. *Котенко И.В., Юсупов Р.М.* Перспективные направления исследований в области компьютерной безопасности. Защита информации. Инсайд. 2006. № 2. С. 46.
32. *Морева О.Д.* Разработка методики оценки информационной защищенности социотехнических систем с использованием функций чувствительности: Дис. канд. техн. наук: Воронеж: ВГТУ, 2006. 162 с.
33. *Наздрачева Л.* Мобильные мошенники. URL: http://www.rusrep.ru/2009/10/news_sotovye_aferisty/ (Дата обращения 03.10.2012)
34. *Озерский К.Г.* Социотехнические методы несанкционированного доступа к информации. URL: http://stavkombez.ru/conf/2012/05/15/ (Дата обращения 03.10.2012)
35. *Пащенко А.Е., Тулупьев А.Л., Суворова А.В., Тулупьева Т.В.* Сравнение параметров угрозообразующего поведения в разных группах на основе неполных и неточных данных // Труды СПИИРАН. 2009. Вып. 8. СПб.: Наука, 2009. С. 252–261.
36. *Пащенко А.Е., Фильченков А.А., Тулупьев А.Л., Азаров А.А., Тулупьева Т.В.* Вероятносто-реляционный подход к представлению комплекса «информационная система – персонал – критичные документы» // 1-й Международный симпозиум «Гибридные и синергетические интеллектуальные системы: теория и практика» (Светлогорск, 29 июня –2 июля 2012 г.). Материалы 1-го международного симпозиума. В 2 т. Т. 2 К.: БФУ им. И. Канта. 2012. С. 30-40.
37. *Пинский М.Я., Сироткин А.В., Тулупьев А.Л., Фильченков А.А.* Повышение быстродействия алгоритма оценки наблюдаемой последовательности в скрытых марковских моделях на основе алгебраических байесовских сетей // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2011. Вып. 5. С. 69–73.
38. Политика информационной безопасности «Газпромбанк». Москва. 2008. 14 с.
39. *Разумов Л.* Основы социотехники. URL: http://www.i2r.ru/static/ 450/out_18632.shtml (Дата обращения 03.10.2012)
40. С инсайдерской активностью можно успешно бороться. URL: http://www.arinteg.ru/articles/s-insayderskoy-aktivnostyu-mozhno-uspeshno-borotsya-123099.html (Дата обращения 03.10.2012)

41. *Сироткин А.В., Тулупьев А.Л., Фильченков А.А., Пащенко А.Е., Тулупьева Т.В., Мусина В.Ф.* Особенности вероятностных графических моделей комплекса «Информационная система–персонал» для оценки его защищенности от социоинженерных атак // Научная сессия НИЯУ МИФИ-2011. (1–5 февраля 2011 г., Москва.)Аннотации докладов. В 3 т. Т. 3: Стратегические информационные технологии в атомной энергетике и промышленности. Проблемы информационной безопасности в системе высшей школы. Экономические и правовые проблемы инновационного развития атомной отрасли. Образование в Национальном исследовательском ядерном университете. М.: НИЯУ МИФИ, 2011. С. 80.
42. *Собецкий И.* Правовое обеспечение борьбы с инсайдерами. // Защита информации. Inside. 2008. №5. С. 56-69.
43. *Степашкин М.В.* Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак:Дис. канд. техн. наук: СПб.: СПИИРАН, 2002. 196 с.
44. *Суворова А.В., Пащенко А.Е., Тулупьева Т.В.* Оценка характеристик сверхкороткого временного ряда по гранулярным данным о рекордных интервалах между событиями // Труды СПИИРАН. 2010. Вып. 12. С. 170–181.
45. *Суворова А.В., Тулупьев А.Л., Пащенко А.Е., Тулупьева Т.В., Красносельских Т.В.* Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения // Компьютерные инструменты в образовании. №4. 2010. С. 30–38.
46. *Тулупьев А.Л., Азаров А.А., Пащенко А.Е.* Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Труды СПИИРАН. 2010. Вып. 2 (13). С. 143–155.
47. *Тулупьев А.Л., Азаров А.А., Пащенко А.Е.* Информационные модели компонент комплекса «Информационная система – персонал», находящегося под угрозой социоинженерных атак // Труды СПИИРАН. 2010. Вып. 3 (14). С. 50–57.
48. *Тулупьев А.Л., Азаров А.А., Тулупьева Т.В., Пащенко А.Е.* Визуальный инструментарий для построения информационных моделей комплекса «информационная система – персонал», использующихся в имитации социоинженерных атак // Труды СПИИРАН. 2010. Вып. 4 (15). С. 231–245.
49. *Тулупьев А.Л., Азаров А.А., Тулупьева Т.В., Пащенко А.Е., Степашкин М.В.* Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак // Труды СПИИРАН. 2010. Вып. 1 (12). С. 200–214.
50. *Тулупьев А.Л., Азаров А.А., Тулупьева Т.В., Пащенко А.Е., Степашкин М.В.* Генерализация моделей деревьев атак на случай социоинженерных атак // Научная сессия МИФИ-2011. Аннотации докладов. В 3 т. Т. 3. М.: МИФИ, 2011. С. 89.
51. *Тулупьев А.Л., Фильченков А.А., Вальтман Н.А.* Алгебраические байесовские сети: задачи автоматического обучения // Информационно-измерительные и управляющие системы. 2011. № 11, т. 9. С. 57-61.
52. *Тулупьева Т.В., Азаров А.А., Пащенко А.Е., Тулупьев А.Л.* Нечеткие составляющие профиля уязвимостей пользователя // Научная сессия МИФИ-2012. Аннотации докладов. В 3 т. Т. 2: Стратегические информационные технологии в атомной энергетике и промышленности. Проблемы информационной безопасности в системе высшей школы. Экономические и правовые проблемы инновационного развития атомной отрасли. Образование в национальном исследовательском ядерном университете. М.: МИФИ, 2012. С. 262.

53. *Тулупьева Т.В., Тулупьев А.Л., Азаров А.А., Пащенко А.Е.* Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак // Труды СПИИРАН. 2011. Вып. 18. С. 74–92.
54. *Тулупьева Т. В., Тулупьев А. Л., Пащенко А. Е., Степашкин М. В.* Подход к оценке защищенности персонала автоматизированной информационной системы от социоинженерных атак // Региональная информатика-2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Санкт-Петербург, 22--24 октября, 2008 г.: Материалы конференции / СПОИСУ. СПб., 2008. С. 113–114.
55. Угрозы информационной безопасности предприятия. URL: http://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-25800.html (Дата обращения 03.10.2012)
56. Угрозы информационной безопасности. URL: http://itsecblog.ru/ugrozy-informacionnoj-bezopasnosti/ (Дата обращения 03.10.2012)
57. Угрозы информационной безопасности. URL: http://sec-it.ru/ugrozy-informacionnoj-bezopasnosti-chast-1/ (Дата обращения 03.10.2012)
58. Угрозы информационной безопасности. URL: http://www.bezzhd.ru/91_ugrozy_informacionnoj_bezopasnosti (Дата обращения 03.10.2012)
59. Угрозы информационной безопасности. Пример классификации угроз информационной безопасности. URL: http://www.interface.ru/home.asp? artId=29344 (Дата обращения 03.10.2012)
60. Угрозы на основе принципов социотехники касаются всех. URL: http://www.pcweek.ru/security/article/detail.php?ID=141030# (Дата обращения 03.10.2012)
61. *Фролова А. Н., Пащенко А. Е., Тулупьева Т. В., Тулупьев А. Л.* Анализ уровня защищенности информационных систем в контексте социоинженерных атак: постановка проблемы // Труды СПИИРАН. 2008. Вып. 7. СПб.: Наука, 2008. С. 170–176.
62. *Фролова А. Н., Тулупьева Т. В., Пащенко А. Е., Тулупьев А. Л.* Возможный подход к анализу защищенности информационных систем от социоинженерных атак // Информационная безопасность регионов России (ИБРР-2007). V Санкт-Петербургская региональная конференция. Санкт-Петербург, 23–25 октября 2007 г.: Труды конференции / СПОИСУ. СПб., 2008. С. 195–199.
63. *Фролова А.Н., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л.* Возможный подход к анализу защищенности информационных систем от социоинженерных атак // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23–25 октября 2007 г.: Материалы конференции. СПб.: СПОИСУ, 2007. С. 197–200.
64. *Харечкин П.В.* Разработка функционально-ролевой модели разграничения доступа в социотехнических информационных системах на основе среды радикалов: Дис. канд. техн. наук: Ставрополь: СГУ, 2011. 158 с.
65. *Юсупов Р., Пальчун Б.П.* Безопасность компьютернойинфосферысистем критических приложений. Вооружение. Политика. Конверсия. 2003. № 2. С. 52.
66. *Dorothy D.E.* A Lattice Model of Secure Information Flow // Communications of the ACM. 2008. Vol. 19.No. 5. p. 236–243.

Азаров Артур Александрович — м.н.с., лаборатория теоретических и междисциплинарных проблем информатики, СПИИРАН. Область научных интересов: защита информации, анализа защищенности информационных систем. Число научных публикаций — 30. Artur-azarov@yandex.ru, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, г.

Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450. Научный руководитель — А.Л. Тулупьев.

Azarov Artur Alexandrovich — junior researcher, Laboratory of Theoretical and Interdisciplinary Computer Science, SPIIRAS. Research interests: information protection, information system's protection analysis. The number of publications — 30. Artur-azarov@yandex.ru, www.tulupyev.spb.ru; SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450. Scientific adviser — A.L.Tulipyev.

Поддержка исследований. Исследование поддержано грантами РФФИ: проект № 10-01-00640-а, проект № 12-01-00945-а, грантом СПбГУ — проект № 6.38.72.2011, грантом Правительства СПб, ПСП №11006, стипендией Президента Российской Федерации, пр. МОН РФ № 747/4 от 21.03.2012, стипендией Правительства Российской федерации, пр. МОН РФ № 874 от 29.10.2012.

Рекомендовано лабораторией теоретических и междисциплинарных проблем информатики, заведующий лабораторией Тулупьев А.Л., д.ф-м.н., доц.
Статья поступила в редакцию 20.09.2012.

РЕФЕРАТ

Азаров А.А. **Основы мониторинга защищенности персонала информационных систем от социотехнических атак.**

Активное привлечение информационных технологий при ведении современного бизнеса выдвигает ряд требований к обеспечению безопасности используемых при этом информационных ресурсов. В связи с этим большинство специалистов в информационной безопасности занимается разработкой различных методов защиты информационных систем от технических атак. В последнее время все больше сотрудников отделов информационной безопасности начинает обращать внимание на проблемы защищенности пользователей информационных систем (ИС). Про социотехнические (социо-инженерные) атаки говорят большинство авторов рассмотренных статей, но ни в одной из них нет сведений о решении задач автоматизированной оценки степени защищенности персонала информационных систем или задач оценки эффективности мероприятий, направленных на предотвращение таких атак. Целью данной статьи является краткий аналитический обзор научной литературы по тематике информационной безопасности, который позволит перечислить как существующие потребности в области анализа защищенности пользователей информационных систем, так и выявленные автором предпосылки к развитию новых подходов такого анализа.

Представленный обзор показывает, что проблема анализа защищенности пользователей информационных систем от социо-инженерных (социотехнических) атак является актуальной, необходимость поиска путей решения которой подчеркивают многие специалисты в области информационной безопасности. В то же время, очевидно, что данная проблема имеет междисциплинарный характер, что оказывается существенным препятствием как в развитии соответствующих теоретических положений, так и основывающихся на них методических и технологических решений. Однако можно указать серию работ, с одной стороны, успешно комбинирующую подходы математики, информатики и социогуманитарных наук, а с другой стороны уже снабженную иллюстративными прототипами программной реализации методик автоматизированной оценки степени защищенности пользователей и критичной информации от социо-инженерных атак.

SUMMARY

Azarov A.A. **Monitoring bases of informational system's personnel' security from sociotechnical attacks.**

Active attraction of information technologies when conducting modern business puts forward a number of requirements to safety of information resources used thus. In this regard the majority of experts in information security is engaged in development of various methods of protection of information systems from technical attacks. In lately more and more the staff of departments of information security starts paying attention to problems of security of users of the information systems (IS). About sociotechnical (socio-engineering) attacks tell the majority of authors of considered articles, but in one of them there are no data on the solution of problems of the automated assessment of degree of security of the personnel of information systems or problems of an assessment of efficiency of the actions directed on prevention of such attacks. The purpose of this article is the short state-of-the-art review of scientific literature on subject of information security which will allow to list as existing needs for the analysis of security of users of information systems, and the preconditions revealed by the author to development of new approaches of such analysis.

The presented review shows that the problem of the analysis of security of users of information systems from socio-engineering (sociotechnical) attacks is actual, need of which search of solutions is emphasized by many experts in the field of information security. At the same time, it is obvious that this problem has interdisciplinary character that appears an essential obstacle as in development of the relevant theoretical provisions, and based on them methodical and technological decisions. However it is possible to specify a series of works, on the one hand, successfully combining approaches of mathematics, informatics and socio-humanistic sciences, and on the other hand already supplied with illustrative prototypes of program realization of techniques of the automated assessment of degree of security of users and critical information from socio-engineering attacks.