2. «Специальные требования по технической защите конфиденциальной информации (СТР-К)» / Утверждена Гостехкомиссией 2002 г.
3. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждёна ФСТЭК от 15.02.2008 года.
4. *Миронова В.Г., Шелупанов А.А.* Сети Петри как инструмент анализа системы защиты конфиденциальной информации // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 64-70.
5. *Шелупанов А.А., Миронова В.Г. и др.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – Ч. 1. – 2010. – № 1 (21). – С. 14-22.
6. *Миронова В.Г., Шелупанов А.А.* Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – Ч. 1. – 2010. – № 2 (22). – С. 257-259.
7. *Миронова В.Г., Шелупанов А.А.* Анализ этапов предпроектного обследования информационной системы персональных данных // Вестник СибГАУ им. М.Ф. Решетнева. – 2011. – № 2 (35). – С. 45-48.
8. *Миронова В.Г., Шелупанов А.А., Югов Т.Н.* Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – № 2 (24), Ч. 3. – С. 206-211.

Статью рекомендовал к опубликованию к.ф.-м.н. Г.И. Афонин.

Миронова Валентина Григорьевна – Томский государственный университет систем управления и радиоэлектроники; e-mail: mvg@security.tomsk.ru; 634050, г. Томск, пр. Ленина, 40; тел.: 89234151608; руководитель аттестационного цента института системной интеграции и безопасности ТУСУРа.

Шелупанов Александр Александрович – e-mail: saa@udcs.ru; тел.: +83822514302; проректор по научной работе ТУСУРа; д.т.н.; профессор.

Mironova Valentina Grigor'evna – "Tomsk State University of Control Systems and Radio Electronics"; e-mail: mvg@security.tomsk.ru; 40, Lenin avenue, Tomsk, 634050, Russia; phone: +79234151608; the head of the appraisal institute cents systems integration and security TUSUR.

Shelupanov Alexander Alexandrovich – e-mail: saa@udcs.ru; phone: +73822514302; vice-rector TUSUR; dr. of eng. sc.; professor.

УДК 004.056

А.П. Стефаров, В.Г. Жуков

ФОРМИРОВАНИЕ ТИПОВОЙ МОДЕЛИ НАРУШИТЕЛЯ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ*

Рассмотрено решение задачи построения типовой модели нарушителя правил разграничения доступа в автоматизированных системах. Проанализированы существующие подходы к построению неформальной модели нарушителя правил разграничения доступа в автоматизированных системах. Описаны критерии классификации нарушителей и оригинальная методика классификации нарушителей. На основе выявленных критериев предложены семь категорий нарушителей правил разграничения доступа в автоматизированных системах. Сформирована таблица, показывающая наличие угроз информационной безопас-

* Работа выполнена при поддержке Минобрнауки в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007-2013 годы», ГК № 07.514.11.4047 от 06.10.2011 г.

ности, которые могут быть реализованы нарушителем на определенном уровне воздействия. Описанный подход построения модели нарушителя позволяет однозначно классифицировать нарушителей.

Модель нарушителя; модель угроз; автоматизированная система; информационная безопасность.

A.P. Stefarov, V.G. Zhukov

STANDARD ATTACKER`S PROFILE CREATION IN COMPUTER-BASED SYSTEMS

An article consider task solution of attackers` profile creation in computer-based systems. Modern approaches to informal attackers` profile creation in computer-based systems are examined in the article. There are classification criteria and unique methodology of attackers` classification introduced in article. Based on classification criteria seven attackers` profiles has been proposed. Information security`s threats that can be realized by attackers on their impact levels are shown in summary table. The described approach of attackers` profile creation allows to definitely classifying attackers.

Attacker`s profile; threat model; computer-based systems; information security.

Автоматизированные системы (АС), в настоящее время, играют ключевую роль при решении задач эффективного выполнения бизнес-процессов любой организации. Вместе с тем повсеместное использование АС для хранения, обработки и передачи информации приводит к повышению актуальности вопросов, связанных с защитой информации, циркулирующей в АС.

С целью исключения или существенного затруднения получения нарушителем защищаемой информации, обрабатываемой в АС, а также исключения или существенного затруднения несанкционированного и/или непреднамеренного воздействия на защищаемую обрабатываемую информацию и ее носители строится система защиты информации (СЗИ). Для построения системы защиты информации необходимо рассматривать как модель угроз, так и модель нарушителя.

Под моделью нарушителя, согласно [14], понимается абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

На сегодняшний день модель нарушителя носит неформальный характер. Различные методы классификации нарушителей описываются как в научно-технической литературе, так и в нормативно-методических документах.

Анализ научно-технической литературы показал, что подходы к построению модели нарушителя у разных авторов различны, хотя и имеются общие классификационные признаки. В результате анализа научно-технической литературы было определено, что при построении модели нарушителя используются следующие критерии: выделяют внутренних и внешних нарушителей, учитывают уровень профессиональной подготовки нарушителей, учитывают уровень знаний нарушителей об объектах атак, учитывают преследуемые цели нарушителей, учитывают наличие доступа у нарушителей к штатным средствам АС, учитывают возможность использования нарушителями различных средств для проведения атак, учитывается возможный сговор нарушителей разных категорий.

Подходы к построению модели нарушителя, описанные в нормативно-методических документах, имеют ряд отличий от подходов, представленных в научно-технической литературе. В частности, помимо критериев, описанных в научно-технической литературе, при построении модели нарушителя следует классифицировать внутренних нарушителей в соответствии с уровнем их полномочий.

Полученные данные показали, что на сегодняшний день отсутствует единый подход к построению модели нарушителя. Предложенные подходы, несмотря на то, что имеют ряд общих классификационных признаков, неполно описывают нарушителей, а категории нарушителей, описанные в различных источниках, не являются коррелированными.

Индекс цитирования классификационных признаков, представленный в виде нормированной гистограммы на рис. 1, позволяет выявить наиболее распространенные классификационные признаки, применяемые при построении модели нарушителя.

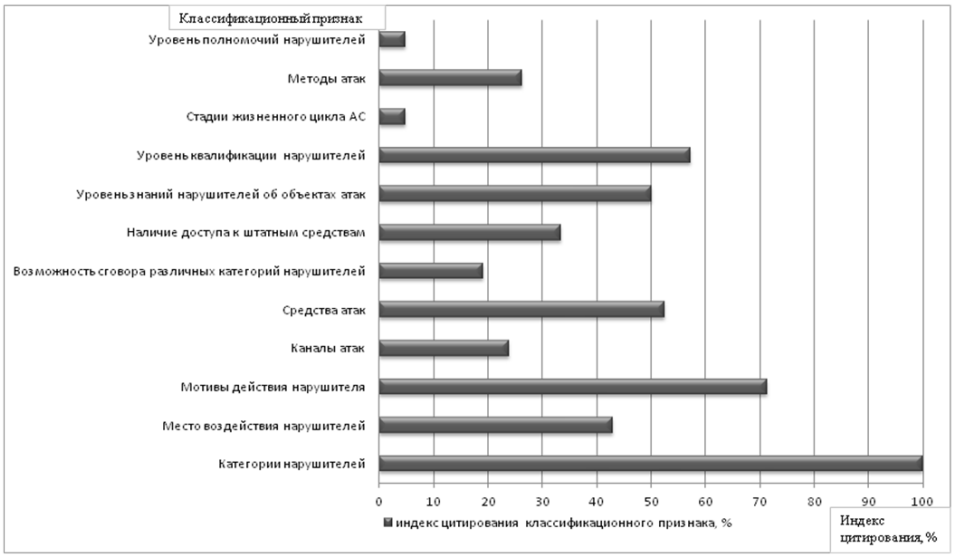

Рис. 1. Нормированная гистограмма индекса цитирования классификационных признаков

В соответствии с полученными в результате анализа данными о критериях классификации нарушителей, при построении модели нарушителя целесообразно использовать следующие классификационные признаки: место воздействия нарушителей, мотивы действия нарушителя, каналы атак, средства атак, возможность сговора различных категорий нарушителей, наличие доступа к штатным средствам, уровень знаний нарушителей об объектах атак, уровень квалификации нарушителей, уровни воздействия нарушителей и стадии жизненного цикла АС.

Рассмотрим предложенные классификационные признаки подробно.

Ввиду того, что нарушители могут воздействовать на АС не только в пределах контролируемой зоны (КЗ), но и за ее пределами, целесообразно разделить нарушителей на субъектов, не имеющих права доступа в контролируемую зону, и субъектов, имеющих право постоянного или разового доступа в контролируемую зону.

Таким образом, согласно п.1 [10], потенциальных нарушителей можно разделить:

- на внешних нарушителей, осуществляющих воздействие за пределами контролируемой зоны (Нвнешн);
- внутренних нарушителей, осуществляющих воздействие, находясь в пределах контролируемой зоны.

Констатируется, что внешними нарушителями могут быть как субъекты, не имеющие права доступа в контролируемую зону, так и субъекты, имеющие право постоянного или разового доступа в контролируемую зону, внутренними нарушителями могут быть только субъекты, имеющие право постоянного или разового доступа в контролируемую зону.

Мотивы действия нарушителя могут быть различны. В общем можно выделить непреднамеренные и преднамеренные действия, согласно п.2 [3].

Непреднамеренные (случайные) действия могут быть спровоцированы недостаточной надежностью штатных средств АС, ошибками обслуживающего персонала, природными явлениями и другими объективными дестабилизирующими воздействиями.

Преднамеренные действия могут быть активными, пассивными и не преследующими целей, что отражено в п. 5.11 [11].

Активные действия потенциального нарушителя предусматривают вмешательство в работу АС, нарушение режимов ее функционирования вплоть до полного прекращения работоспособности.

Пассивные действия потенциального нарушителя предполагают доступ к хранимой, передаваемой и обрабатываемой в АС информации путем использования выявленных уязвимостей АС, но не наносящий прямого вреда АС.

Под действиями, не преследующими целей, следует понимать действия без злого умысла, не ставящие перед собой цели нанесения вреда АС или доступа к информации ограниченного распространения, циркулирующей в АС, например, действия потенциального нарушителя с целью самоутверждения.

Основными каналами атак являются:

- канал НСД, согласно п.1 [10], п.4.5 [5];
- технические каналы, согласно п.3.4 [4], п.1 [10], п.4.5 [5].

Нарушители могут реализовывать атаки по каналу НСД через каналы передачи данных, в том числе выходящие за пределы контролируемой зоны, через автоматизированные рабочие места (АРМ), в том числе подключенные к сетям связи общего пользования, через штатные средства АС, в том числе через те, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны, через АС взаимодействующих ведомств, организаций и учреждений при их подключении к АС.

Следует отметить, что внешний нарушитель реализует атаки по каналу НСД с использованием протоколов межсетевого взаимодействия.

Среди технических каналов, согласно [3], выделяют каналы акустической (речевой) информации, видовой информации, информации по каналам побочных электромагнитных излучений и наводок.

Реализация атак по техническому каналу возможна как в пределах контролируемой зоны, так и за ее пределами.

В качестве средств атак нарушитель может использовать как штатные средства, к которым он имеет доступ, так и все необходимые для проведения атак по доступным ему каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну.

Среди средств атак можно выделить:

- применение пассивных средств (технические средства перехвата без модификации объектов АС);
- применение штатных средств и недостатков системы защиты для ее преодоления;

- применение средств активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

Следует учесть, что средствами атак могут являться доступные в свободной продаже технические средства и программное обеспечение, согласно п.3.4 [4], специально разработанные технические средства и программное обеспечение, согласно п.3.4 [4], п.1 [10], штатные средства, согласно п.3.4 [4], п.1 [10].

Следует учесть возможность сговора нарушителей разных категорий. Сговор нарушителей осуществляется для получения дополнительных привилегий, которые могут использоваться для подготовки и проведения атак.

Жизненный цикл АС, согласно [14], представляет собой совокупность взаимосвязанных процессов создания и последовательного изменения состояния АС от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации АС.

Следовательно, нарушитель может воздействовать на различных стадиях жизненного цикла АС:

- на стадии разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств;
- на стадии эксплуатации технических и программных средств.

На первой стадии обработка информации не производится, поэтому объектами воздействия нарушителей могут быть только сами эти средства и документация на них.

На данной стадии возможно внесение недекларированных возможностей в технические и программные компоненты технических и программных средств, в том числе с использованием вредоносных программ (компьютерные вирусы, "троянские кони" и т.д.), а также внесение несанкционированных изменений в документацию на технические и программные средства.

Необходимо отметить, что указанные воздействия:

- на этапах разработки, производства и транспортировки технических и программных средств могут проводиться только вне контролируемой зоны;
- на этапе хранения технических и программных средств могут проводиться как в пределах контролируемой зоны, так и вне контролируемой зоны;
- на этапе ввода в эксплуатацию технических и программных средств могут проводиться только в пределах контролируемой зоны.

На стадии эксплуатации технических и программных средств объектами воздействия нарушителей могут быть не только технические и программные средства, но и информация, обрабатываемая этими средствами.

Согласно п.4.7 [5], при разработке (модернизации) и эксплуатации АС должна быть организована разрешительная система доступа разработчиков, пользователей, эксплуатирующего персонала к техническим и программным средствам, а также информационным ресурсам АС. Пользователям предоставляется право работать только с теми средствами и ресурсами, которые необходимы им для выполнения установленных функциональных обязанностей.

Следует отметить, что согласно подпункту 5 пункта 3.1 [4], система защиты не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту полномочий.

Таким образом, наличие доступа внутренних нарушителей к штатным средствам существенным образом зависит от их функциональных обязанностей.

В соответствии с функциональными обязанностями, внутренних потенциальных нарушителей возможно представить в виде следующих категорий:

К первой категории относятся субъекты, имеющие санкционированный доступ в контролируемую зону, но не имеющие доступа к АС ($\mathbf{H_1}$).

Ко второй категории относятся зарегистрированные пользователи АС, осуществляющие ограниченный доступ к ресурсам АС с рабочего места ($\mathbf{H_2}$).

К третьей категории относятся зарегистрированные пользователи АС, осуществляющие удаленный доступ к АС по локальным и (или) распределенным каналам передачи данных ($\mathbf{H_3}$).

К четвертой категории относятся зарегистрированные пользователи с полномочиями системного администратора АС ($\mathbf{H_4}$).

К пятой категории относятся зарегистрированные пользователи с полномочиями администратора информационной безопасности (ИБ) АС ($\mathbf{H_5}$).

К шестой категории относятся разработчики прикладного программного обеспечения и технических средств и лица, обеспечивающие их поставку, сопровождение и ремонт на защищаемом объекте ($\mathbf{H_6}$).

Следует исходить из предположения, что потенциальные нарушители обладают всей информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации.

Согласно п.2.5, п.2.8 [9], пользователи обязаны не разглашать информацию, к которой они допущены, соблюдать требования к обеспечению безопасности конфиденциальной информации, сообщать о ставших им известными попытках посторонних лиц получить сведения об АС.

Таким образом, уровень знаний внутренних нарушителей об объектах атак зависит от их функциональных обязанностей.

Согласно п.2.6 [9], п.8.2.3 [15], п.7.18 [12], [13] квалификация пользователей должна быть достаточной для выполнения ими функциональных обязанностей.

Следовательно, для определения уровня квалификации внутренних нарушителей следует учитывать их функциональные обязанности.

При этом следует учесть, что реализация дополнительных защитных мер может потребовать от нарушителя более высокого уровня подготовки и значительных ресурсов для проведения результативной атаки, что отражено в [13].

Модель нарушителя должна позволять однозначно классифицировать категорию нарушителя, учитывая различные классификационные признаки. При этом в [4] указывается, что степень детализации описания параметров должна быть достаточной для выполнения задач по защите информации.

Следует отметить, что однозначно классифицировать нарушителей представляется возможным не по всем классификационным признакам, т.к. некоторые классификационные признаки характерны для нескольких категорий нарушителей. В качестве критерия классификации, позволяющего однозначно классифицировать нарушителей, предлагается использовать уровни воздействия нарушителей.

Согласно [5], для гарантированного решения задач защиты информации в АС необходимо учитывать уровень технических каналов, уровень несанкционированного доступа, уровень вредоносного воздействия, уровень закладных устройств, уровень системы защиты информации.

Штатные средства, с использованием которых возможен несанкционированный доступ, могут быть различными. Следовательно, необходимо классифицировать уровень несанкционированного доступа к защищаемой информации.

Классификация уровней несанкционированного доступа к защищаемой информации может быть представлена в виде уровней стека протоколов TCP/IP [6, 7] либо в виде иных моделей, отражающих сетевые принципы правил обмена данными между субъектами [8].

При построении системы защиты информации с использованием криптосредств, необходимо соблюдать требования, описанные в нормативно-методических документах ФСБ России.

В частности, использование криптосредств должно соответствовать лицензионным требованиям и условиям, эксплуатационной и технической документации к криптосредствам [9]. В то же время должна обеспечиваться комплексность защиты информации, в том числе посредством применения некриптографических средств защиты.

Таким образом, целесообразно классифицировать уровень системы защиты информации на уровень системы защиты информации с применением криптографических средств и уровень системы защиты информации с применением некриптографических средств.

Учитывая вышеизложенное, уровни воздействия нарушителей возможно представить в следующем виде: уровень закладных устройств (**L_{10}**), уровень системы защиты информации с применением криптографических средств (**L_9**), уровень системы защиты информации с применением некриптографических средств (**L_8**), уровень технических каналов (**L_7**), прикладной уровень стека протоколов TCP/IP (**L_6**), транспортный уровень стека протоколов TCP/IP (**L_5**), сетевой уровень стека протоколов TCP/IP (**L_4**), канальный уровень стека протоколов TCP/IP (**L_3**), физический уровень стека протоколов TCP/IP (**L_2**), уровень вредоносного воздействия (**L_1**).

Уровни воздействия нарушителей и категорий нарушителей связаны между собой через наличие угроз информационной безопасности, которые могут быть реализованы нарушителем на определенном уровне воздействия (табл. 1). При этом наличие хотя бы одной угрозы, сформированной на основании факторов, воздействующих на безопасность защищаемой информации согласно [16], обозначается единицей, а их отсутствие – нулем.

Таблица 1

Соотношение категорий нарушителя и уровней воздействия нарушителя

	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}
H_1	**1**	**1**	0	0	0	0	0	0	0	0
H_2	**1**	**1**	0	0	**1**	**1**	0	0	0	0
H_3	**1**	**1**	0	**1**	**1**	**1**	0	0	0	0
H_4	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0
H_5	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0
H_6	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	**1**
$H_{внешн}$	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Как видно из таблицы, предложенная классификация нарушителей в соответствии с их уровнем воздействия позволяет однозначно классифицировать нарушителей.

Формирование типовой модели нарушителя осуществляется с учетом требований, обеспечивающих ее функциональность и практическую эффективность:

1. Типовая модель нарушителя должна представлять собой не отдельные классификационные признаки, характеризующие нарушителей, а совокупную характеристику каждой категории нарушителя.
2. Типовая модель нарушителя должна отражать тесные корреляционные зависимости выделенных в ней категорий нарушителей с различными классификационными признаками, их описывающими.
3. Типовая модель нарушителя должна обеспечивать получение достаточной информации для формирования категорий нарушителя по предложенным классификационным признакам с учетом их однозначной классификации.

4. Типовая модель нарушителя должна позволять выявить категории нарушителей для любой существующей АС.
5. Наличие типовой модели нарушителя не должно вести к стереотипности решений при создании СЗИ для конкретной АС. При создании модели нарушителя для конкретной АС необходимо применять типовую модель нарушителя как основу, но при этом следует учитывать особенности функционирования конкретной АС.

Таким образом, с учетом вышеописанных требований, типовая модель нарушителя будет представлена следующими категориями нарушителей:

Нарушителями первой категории ($\mathbf{H_1}$) являются субъекты, имеющие санкционированный доступ в КЗ, но не имеющие доступа к АС. Могут воздействовать на физический уровень стека протоколов TCP/IP, уровень вредоносного воздействия с целью хищения информации или самоутверждения. При этом используют технические средства перехвата без модификации компонентов системы (пассивные средства атак).

Нарушителями второй категории ($\mathbf{H_2}$) являются зарегистрированные пользователи АС, осуществляющие ограниченный доступ к ресурсам АС с АРМ. Могут воздействовать на физический, транспортный и прикладной уровни стека протоколов TCP/IP, уровень вредоносного воздействия с целью хищения информации, самоутверждения или непреднамеренно. При этом используют технические средства перехвата без модификации компонентов системы (пассивные средства атак), а так же штатные средства и недостатки СЗИ для ее преодоления.

Нарушителями третьей категории ($\mathbf{H_3}$) являются зарегистрированные пользователи АС, осуществляющие удаленный доступ к АС по локальным и (или) распределенным каналам передачи данных. Могут воздействовать на физический, сетевой, транспортный и прикладной уровни стека протоколов TCP/IP, уровень вредоносного воздействия с целью хищения информации, самоутверждения или непреднамеренно. При этом используют технические средства перехвата без модификации компонентов системы (пассивные средства атак), а так же штатные средства и недостатки СЗИ для ее преодоления.

Нарушителями четвертой категории ($\mathbf{H_4}$) являются зарегистрированные пользователи с полномочиями системного администратора АС. Могут воздействовать на все уровни стека протоколов TCP/IP, уровень вредоносного воздействия, уровень технических каналов с целью хищения информации, а так же с целью вывода из строя АС. При этом используют все возможные средства атак. Возможен сговор с нарушителями пятой и шестой категорий. Не имеют доступа к средствам защиты информации и протоколирования и к части ключевых элементов АС.

Нарушителями пятой категории ($\mathbf{H_5}$) являются зарегистрированные пользователи с полномочиями администратора ИБ АС. Могут воздействовать на все уровни стека протоколов TCP/IP, уровень вредоносного воздействия, уровень технических каналов, уровни СЗИ криптографическими и некриптографическими средствами с целью хищения информации, а так же с целью вывода из строя АС. При этом используют все возможные средства атак. Возможен сговор с нарушителями четвертой и шестой категорий. Не имеют прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Нарушителями шестой категории ($\mathbf{H_6}$) являются разработчики прикладного программного обеспечения и технических средств и лица, обеспечивающие их поставку, сопровождение и ремонт на защищаемом объекте. Могут воздействовать на все уровни стека протоколов TCP/IP, уровень вредоносного воздействия, уровень технических каналов, уровень закладных устройств с целью хищения информации, а так же с целью вывода из строя АС. При этом используют все возможные

средства атак. Возможен сговор с нарушителями четвертой и пятой категорий. Обладают возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение и технические средства АС.

Внешними нарушителями ($\mathbf{H_{внешн}}$) являются субъекты, осуществляющие воздействие за пределами КЗ. Могут воздействовать на все уровни воздействия с целью хищения информации, самоутверждения, а так же с целью вывода из строя АС. При этом используют методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

В результате проведенных исследований создана типовая модель нарушителя, учитывающая требования государственных стандартов, нормативно-методических документов ФСТЭК России и ФСБ России, что позволяет применять данную модель при защите государственных информационных ресурсов, для защиты которых требования государственных стандартов, нормативно-методических документов ФСТЭК России и ФСБ России являются обязательными для исполнения.

Кроме того, предложенная классификация нарушителей позволяет однозначно классифицировать нарушителей в соответствии с уровнями их воздействия, чего не было представлено ранее в существующих моделях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Стефаров А.П., Жуков В.Г., Жукова М.Н.* Модель нарушителя прав доступа в автоматизированной системе // Прогр. продукты и системы. – 2012. – № 2. – С. 51-54.
2. Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Рос. Федерации от 17 ноября 2007 г. № 781 // Собр. законодательства Рос. Федерации. – 2007. – № 48. – С. 6001.
3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утв. зам. дир. ФСТЭК России 15 февр. 2008 г. – М.: Аксимед, 2008. – 76 с.
4. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации: Утв. руководством 8 Центра ФСБ России 21 февр. 2008 года № 149/54-144. – М., 2008. – 20 с.
5. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения. – Введ. 2001-01-01. – М.: Госстандарт России, 2000. – 22 с.
6. *James F. Kurose.* Computer Networking: A Top-Down Approach / James F. Kurose, Keith W. Ross. - Lebanon : Addison-Wesley, 2008. – 880 p.
7. *Behrouz A. Forouzan*. Data Communications and Networking / Behrouz A. Forouzan. – 3 ed. – Columbus: McGraw-Hill Higher Edication, 2003. – 944 p.
8. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации:Руководящий документ: утв. решением гос. техн. комиссии при президенте Рос. Федерации от 30 марта 1992 г. – М.: ГТК РФ, 1992. – 12 с.
9. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных: Утв. руководством 8 Центра ФСБ России 21 февр. 2008 года № 149/6/6-622. – М.: Аксимед, 2008. – 17 с.

10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. зам. дир. ФСТЭК России 14 февр. 2008 г. – М.: Аксимед, 2008. – 8 с.
11. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения: ГОСТ Р 52448-2005. – Введ. 2007-01-01. – М.: Стандартинформ, 2007. – 15 с.
12. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники: Руководящий документ / Гос. техн. комиссия Рос. Федерации. – М.: ГТК РФ, 1992. – 29 с.
13. ГОСТ Р ИСО/МЭК ТО 15446-2008. Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. введ. 2009-10-01. – М.: Стандартинформ, 2010. – 107 с.
14. ГОСТ 34.003-90. Автоматизированные системы. Термины и определения. – Взамен ГОСТ 24.003-84, ГОСТ 22487-77; введ. 1992-01-01. – М., 1990. – 68 с.
15. Руководство по разработке профилей защиты и заданий по безопасности: Руководящий документ / Гос. техн. комиссия России. – М.: ГТК РФ, 2003. – 110 с.
16. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – Взамен ГОСТ Р 51275-99; введ. 2008-02-01. – М.: Стандартинформ, 2007. – 11 с.

Статью рекомендовал к опубликованию д.т.н. профессор В.А. Терсков.

Стефаров Артем Павлович – Сибирский государственный аэрокосмический университет им. ак. М.Ф. Решетнева (СибГАУ); e-mail: Chameleo@mail.ru; 660014, г. Красноярск, пр. им. газеты «Красноярский рабочий», 31; тел.:+79135347358; кафедра САиИО; аспирант.

Жуков Вадим Геннадьевич – e-mail: vadimzhukov@mail.ru; тел.:+79029171966; кафедра безопасности информационных технологий; к.т.н.; доцент.

Stefarov Artem Pavlovich – Siberian state airspace university named after academician M.F. Reshetnev (SSAU); e-mail: Chameleo@mail.ru; 31, Krasnoyarsky Rabochy av., Krasnoyarsk, 660014, Russia; phone: +79135347358; the department of system analysis; postgraduate student.

Vadim Zhukov Genad'evich – e-mail: vadimzhukov@mail.ru; phone: +79029171966; the department of information technologies` security; cand. of eng. sc.; associate professor.

УДК 004.056

М.О. Шудрак, И.А. Лубкин, В.В. Золотарев

СТАТИЧЕСКИЙ АНАЛИЗ БИНАРНОГО КОДА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматривается методика декомпиляции бинарного кода и возможность ее применения в сфере информационной безопасности. Основная цель работы заключается в разработке эффективного алгоритма анализа бинарного кода. Для достижения поставленной цели необходимо решить ряд задач: разработать эффективный механизм анализа низкоуровневых команд, их алгоритмического представления и провести апробацию полученной методики. Результатом работы стала эффективная методика декомпиляции и алгоритмического представления линейных участков бинарного кода, апробированная на решении таких задач как: защита программного обеспечения от несанкционированного анализа и анализе обфусцированного кода вредоносных объектов.

Декомпиляция; анализ кода; защита программного обеспечения; полиморфный код.