УВД как датчики информации на стратегию технического обслуживания по состоянию с контролем параметров. Однако необходимо отметить, что при этом обязательным условием является наличие соответствующей системы технической диагностики и контроля всех составляющих комплексов.

Список литературы

1. ГОСТ Р 51583–2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. М. : Стандартинформ, 2014.

2. *Емельянов В. Е.*, *Логвин А. И.* Техническая эксплуатация авиационного радиоэлектронного оборудования. М. : Моркнига, 2014.

3. *Левин Б. Р.* Теория надежности радиотехнических систем. М. : Сов. радио, 1988.

УДК 004.056.53

Н. С. Муравьев
Научный руководитель: д-р пед. наук, проф. Л. В. Астахова
Южно-Уральский государственный университет, Челябинск

ПРОФИЛАКТИКА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРОФИЛИРОВАНИЯ ПОЛЬЗОВАТЕЛЕЙ: ПРОГРАММНО-ТЕХНИЧЕСКИЙ АСПЕКТ

Аннотация. В статье рассмотрена проблема профилирования пользователей информационной системы как средства профилактики инцидентов в сфере информационной безопасности. Предложены направления для технической реализации профилирования.

Ключевые слова: информационная безопасность; поведение пользователя; профайлинг; профилирование; инциденты по вине пользователя.

Очевидно, что человеку отводится основная роль в процессах организации, функционирования и развития деятельности коммерческих и государственных организаций, предприятий и иных структур. При выполнении своей деятельности сотрудник располагает совокупностью информационных ресурсов организации, а также имеет доступ к средствам ее обработки, которые в свою очередь могут вызвать интерес не только у правообладателя, но и третьих лиц. В целях сохранности ключевой информации в организациях вводится режим

информационной безопасности (далее — ИБ), который состоит из правовых, организационных и программно-технических мер защиты.

Большая часть выявленных нарушений информационной безопасности происходит из-за присутствия человеческого фактора в информационной системе (далее — ИС). Под человеческим фактором мы понимаем набор преднамеренных или неумышленных (например, при неправильной эксплуатации ИС) действий внутреннего пользователя, в результате которых реализуется угроза и происходит утечка информации.

В повседневной рабочей среде при длительном периоде без инцидентов в ИБ, а также при отсутствии видимых угроз у пользователя меняется восприятие к опасностям, что приводит к успешным проведениям таких атак, как социальная инженерия, фишинг, инсайдерские утечки и т. д., которые требуют наличия человеческого воздействия на систему. Подобные угрозы усложняются тем, что внутренний пользователь имеет прямой доступ к информации и его поведение с меньшей вероятностью отличается от нормы [1].

Далее будем рассматривать событие, при котором инцидент происходит по вине пользователя информационной системы. Для решения этой задачи рассмотрим процесс профилирования пользователей и выделим критерии, по которым возможно оценить поведение человека в ИС.

Анализ российской и зарубежной литературы показал, что зачастую профайлинг рассматривается с позиций гуманитарно-психологического подхода: в деятельности кадровых служб [2], в правоохранительной деятельности [3]. Профайлингу в сфере ИБ уделяется значительно меньше внимания.

Таким образом, цель данной работы — описать критерии для оценки и прогнозирования поведения пользователя при взаимодействии с ИС для возможности последующего формирования оптимального шаблона поведения, который можно считать безопасным, а также сопоставление действий пользователя с этим шаблоном и установленной политикой ИБ.

Зарубежные специалисты рассматривают профайлинг и профилирование с позиции основанной на криминалистических подходах [4]. На наш взгляд, профилирование — процесс сбора и накопления данных о пользователях, структурированных по атрибутам согласно определенным критериям оценки с целью прогнозирования поведения пользователей. Профайл — это результат профилирования: совокупность записей в базе данных с атрибутами содержащими критерии для оценки поведения по каждому пользователю ИС.

Достижение обозначенной цели возможно путем смешения социальных и технологических решений, результаты которых должны вноситься в профайл каждого отдельного взятого сотрудника организации.

К социальным решениям относятся такие данные, как сведения о психологических, социальных, культурных и иных гранях жизни человека. Данные об

этом собираются через опросы, тесты, наблюдения и иные формы внутренних и внешних проверок. К технологическому решению относится раздел, который исследует непосредственно поведение человека в момент, когда он является пользователем ИС [4]. Идею можно рассмотреть как дополнение к различным системам мониторинга или DLP-системам. В совокупности эти данные вносятся в профайл для определения поведенческого типа каждого сотрудника. При анализе данных из профайла изучается поведение сотрудника, соответствие степени соблюдения политике безопасности организации, уровень лояльности и прочие поведенческие качества с последующим формированием шаблона по данному пользователю.

Для разработки программно-технических средств профилирования необходимо четкое определение критериев. Зарубежные специалисты выделяют такие критерии оценки поведения пользователя, как:

1. Обращение с паролями (оценка изменения пароля и его надежность в соответствии с установленной политикой безопасности).

2. Периодичность резервного копирования (своевременность резервного копирования в случае наличия таких обязанностей на пользователе [4].

Мы считаем, что перечень этих критериев может быть продолжен на основе используемых сведений о пользователях, собираемых в DLP системах и других системах с возможностью мониторинга, применяемых в российской и зарубежной практике защиты информации. К таким критериям мы отнесем:

- данные о попытках доступа к сектору информации ограниченного доступа для пользователя;
- данные о сетевой активности и сопоставление просматриваемых интернет-ресурсов на предмет отношения к профессиональной деятельности;
- сведения о попытках взаимодействия со съемными носителями;
- регистрация запросов к установленным средствам защиты информации (например, данные о попытке просмотра настроек средства от НСД, антивируса и т. д.);
- иные сведения, которые могут быть получены за счет мониторинга.

Указанный перечень критериев может быть расширен в соответствии с применяемыми технологическими возможностями по каждой отдельной организации.

На основе указанных критериев предлагаем формировать так называемый «Профайл безопасного пользователя». В нем должны содержаться оптимальные показатели указанных критериев, которые соответствуют установленным требованиям политики ИБ. Например, установленная периодичность смены паролей пользователей, количество попыток несанкционированного доступа к защищаемой информации и др.

Представим общую схему профилирования, оценки и прогнозирования поведения пользователя ИС (рис. 1).

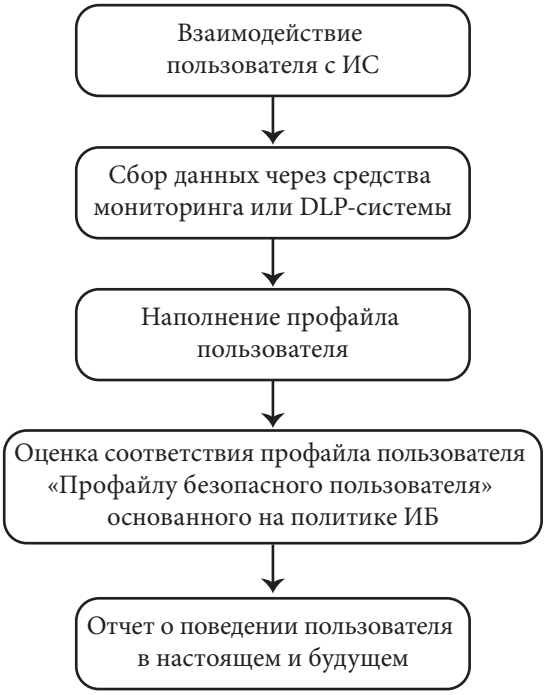

Рис. 1. Общая схема профилирования, оценки и прогнозирования поведения пользователя ИС

Таким образом, важным средством профилактики инцидентов ИБ является профилирование пользователей. Обоснованные критерии оценки поведения пользователей ИС имеют количественную характеристику. Это обеспечивает возможность автоматизации профилирования и прогнозирования возможных инцидентов ИБ по вине каждого отдельно взятого пользователя ИС. В качестве инструмента определения степени уязвимости пользователя в настоящей статье предлагается «Профайл безопасного пользователя».

Список литературы

1. *Астахова Л. В.*, *Ефремов В.* А., *Митькин А. И.* Автоматизация многофакторной оценки кадровых уязвимостей информационной безопасности // Вестн. УрФО. Безопасность в информационной сфере. 2014. № 4 (14). С. 57–61.

2. *Арпентьева М. Р.* Профайлинг как современная HR-технология // Инновационное развитие современных социально-экономических систем : материалы III Международ. заоч. науч.-практ. конф. 2016. С. 296–301.

3. *Черкасова Е. С.* Профайлинг как метод создания психологического портрета потенциального преступника на этапе организации предварительного расследования // Юр. наука и практика. 2013. С. 72–75.

4. *Fernando S. A.*, *Yukawa T.* Securing Information Sharing Through User Security Behavioral Profiling // Transactions on Engineering Technologies. 2013. С. 655–670.

УДК 004.056

А. И. Полтавец, И. П. Петров, А. С. Федотова, Н. Е. Девицкий
Научный руководитель: ст. преп. И. П. Петров
Тюменский государственный университет, Тюмень

ПРОБЛЕМЫ БЕЗОПАСНОСТИ RECAPTCHA'S

Аннотация. CAPTCHA — это первая линия защиты Интернета от автоматического создания учетной записи, автоматического спама и прочее. Google reCaptcha, одна из самых популярных captcha-систем, в настоящее время используется сотнями тысяч сайтов для защиты от автоматических ботов, проверяя, действительно ли пользователь — человек. Но возможен ли обход CAPTCHA? В этой статье мы хотели бы представить unCaptcha, автоматизированную систему, которая может решать самые сложные reCaptcha, построенную на звуковом анализе, с высокой степенью точности.

Ключевые слова: captcha; reCaptcha; антиспам; информационная безопасность; боты.

Введение

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) — полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей [1].

Captchas широко используются на различных веб-ресурсах как защита от автоматических ботов и атак Sybil [2], а также для предотвращения спама. Например, многие онлайн-платформы при покупке билетов [3] требуют, чтобы пользователь решил captcha во время регистрации для предотвращения автоматического создания поддельных счетов.

Безопасность captchas имеет первостепенное значение для защиты веб-ресурсов в Интернете от этих атак. Поскольку распространение новостей и информации все чаще зависит от пользовательского контента на сайтах, таких как Twitter, Facebook, YouTube и многих других, злоумышленники, которые могут обойти систему CAPTCHA и зарегистрировать непропорциональное