ПРОБЛЕМЫ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Руденя В.Ю.

Магистрант кафедры проектирования информационно-компьютерных систем, Белорусский государственный университет информатики и радиоэлектроники (БГУИР), г.Минск

Аннотация

Статья посвящена проблеме защиты данных в информационных системах, описываются основные требования и свойства для защиты информационных сетей и систем.

Ключевые слова: Защита данных, информационные системы.

Вследствие активного развития информационных технологий, огромную ценность на сегодняшний день представляет информация. Любая сфера общественной жизни может быть описана информацией, потеря или модернизация которой может привести к большим убыткам. Таким образом, информация становиться стратегическим ресурсом государства и бизнеса всех уровней, которые заинтересованы в её сохранности. Кроме естественных рисков потери информации (отказ техники, стихийные бедствия и т. д.), присутствует также стремление криминальных структур осуществить незаконной похищение или модернизацию информации. В свете сказанного проблема защиты информации является чрезвычайно актуальной на сегодняшний день [1].

Требования по обеспечению безопасности в различных информационных системах (далее – ИС) могут существенно отличаться, однако они всегда направлены на достижение трех основных свойств:

- **целостность,** информация, на основе которой принимаются решения, должна быть достоверной и точной, защищенной от возможных непреднамеренных и злоумышленных искажений;
- **доступность,** информация и соответствующие автоматизированные службы должны быть доступны, готовы к работе всегда, когда в них возникает необходимость;
- **конфиденциальность,** информация должна быть доступна только тому, кому она предназначена.

Все сказанное позволяет сделать вывод о том, что ИС ввиду присущей им специфики целесообразно рассматривать только в комплексном порядке совместно с обеспечением информационной защиты всей системы обработки информации в целом. При рассмотрении ИС следует обратить внимание на такие их особенности, как [2]:

– широкораспространенность использования персональных данных при регистрации пользователей на сайтах глобальной информационной сети Интернет;

– присутствие риска утечки персональных данных при регистрации пользователем;

– отсутствие единого набора полей форм персональных данных;

– прямая возможность использования мошенниками персональных данных в целях личного обогащения и причинения денежного ущерба их владельцу и ИС в целом;

– рост технических возможностей и числа путей обхода средств защиты информации со стороны мошенников;

– неосведомленность пользователей о возможности и последствиях угроз утечки информации;

– существование автоматизированных систем сбора персональных данных мошенниками в обход средств защиты персональных данных.

Для решения проблем информационной безопасности необходимо сочетание законодательных, организационных, технологических и стандартизационных мероприятий [3].

В последнее время проблема защиты персональных данных серьезно обострилась наряду с изменением хозяйственных механизмов, а также широкомасштабной автоматизацией сбора и обработки данных социально-экономического характера. Первое условие привело к появлению большого количества новых субъектов в виде независимых от государства юридических лиц, занимающихся сбором, обработкой и хранением информации. Второе условие существенно упростило процессы копирования, распространения и использования информации любого характера, в том числе персональных данных. Все это способствовало появлению нового вида криминальной деятельности - хищения и противоправного оборота персональных данных. В связи с повсеместным внедрением глобальной информационной сети Интернет, где до сих пор до конца не решена проблема идентификации пользователей, данный вид преступного бизнеса получил широкое распространение [4].

Практика расследования киберпреступлений показывает, что большую угрозу для общества и государства представляют деяния, связанные с незаконным копированием, модификацией или уничтожением компьютерной информации. При этом по статистике до 2/3 фактов несанкционированного проникновения в компьютерные сети совершается по вине неаккуратных пользователей или при непосредственном участии обслуживающего персонала пострадавшей организации. Подобные тенденции характерны не только для России, но и для всех развитых государств, где ключевую роль в жизни общества играют средства информатизации и массовых коммуникаций [5].

Причиной нарушения правил информационной безопасности (далее – ИБ), как правило, становится халатность сотрудников, либо корыстный и преступный умысел нарушителей. Подобные случаи опережают по своей массовости даже количество атак, в результате которых происходит внедрение в компьютер специальных программ и утечка данных через Интернет. Все

также опасны и актуальны хакерские нападения, целью которых является несанкционированный доступ и взлом ресурсов с приватной информацией [6].

Таким образом, можно утверждать, что, как и прежде, в 80% случаев утраты закрытой информации необходимо искать источник внутри самой организации.

Конечно, нельзя утверждать, что внутренние риски ИБ опаснее внешних, однако факт, что угроза со стороны служащих компаний и организаций сегодня вызывает гораздо больше беспокойства, чем вирусы, хакеры и спам. Проблема состоит в том, что от внутренних нарушителей нельзя защититься также легко, как, например, от вредоносных программ с помощью антивируса. С внутренними угрозами дело обстоит гораздо серьезнее. Это комплексная, но вполне решаемая проблема[7].

Использование различных систем для защиты от внутренних нарушителей становится все более популярным. Но, как уже отмечалось ранее, к решению проблемы защиты от внутренних угроз необходимо подходить комплексно. Техническими средствами взять под контроль все каналы утечки, а административными - ограничить доступ к тем, которые контролировать невозможно. Необходимо уметь обходить такие препятствия на пути внедрения защиты от утечки, как психологическая неготовность и бюджетные ограничения. Важно сочетать административные меры с подготовкой и воспитанием квалифицированного персонала, наряду с внедрением технологических решений и стандартов [8].

СПИСОК ЛИТЕРАТУРЫ

1. Бормотов, В. Е. Проблемы защиты информации в компьютерной сети / В.Е. Бормотов. – М.: Молодой ученый №11(115). – 2016.

2. Основы информационной безопасности // НОУ ИНТУИТ [Электронный ресурс]. – 2018. – Режим доступа: http://www.intuit.ru/studies/courses/3627/869/lecture/31759. – Дата доступа: 26.02.2018.

3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: уч. пособие / В.Ф. Шаньгин. – М.: МИЭТ, 2010.

4. Андрончик, А. Н. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург: УГТУ-УПИ, 2008.

5. Замкова Т.В. Проблемы защиты информации в современных информационных системах / Т.В. Замкова. – М.: Современные наукоемкие технологии №3, 2005.

6. Проблемы защиты информации // Студфайлс [Электронный ресурс]. – 2018. – Режим доступа: https://studfiles.net/preview/5443793/page:47/. – Дата доступа: 05.03.2018.

7. Латыпова, Э.Р. Проблемы защиты информации / Э.Р. Латыпова. – М.: Уфа, 2017.

8. Федотов А.М. Проблемы защиты информации в *WWW* информационных системах / А.М. Федотов. – Новосибирск: ИВТ СО РАН, 2009.