УДК 005.21:334.012.42

Авраменко Т. О. ,
ассистент кафедры экономической информатики, учёта и коммерции,
Гомельский государственный университет имени Ф. Скорины,
Республика Беларусь, г. Гомель

АНАЛИЗ КРУГА СУЩЕСТВУЮЩИХ ПРОБЛЕМ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ

Аннотация

В статье рассмотрены потенциальные угрозы безопасности в информационной сфере, выделены объекты угроз информационной безопасности, дана классификация угроз, а также выделены основные виды преднамеренных угроз информационной безопасности компьютерных систем и приведён перечень основных угроз в зависимости от уровня их вероятной реализации в коммерческой организации.

Ключевые слова: информационная безопасность, компьютерная система, информационные угрозы, преднамеренные угрозы информационной безопасности, стратегическое управление.

T. Avramenko,
Assistant, Department of Economic Informatics, Accounting and Commerce,
Gomel State University named after F. Skorina,
Republic of Belarus, Gomel

ANALYSIS OF THE RANGE OF EXISTING PROBLEMS IN ENSURING INFORMATION SECURITY IN THE PROCESS OF STRATEGIC MANAGEMENT

Annotation

The article considers potential security threats in the information sphere, identifies objects of information security threats, gives a classification of threats, and also identifies the main types of deliberate threats to information security of computer systems and provides a list of the main threats depending on the level of their likely implementation in a commercial organization.

Key words: information security, computer system, information threats, intentional threats to information security, strategic management.

В результате проведённого анализа существующих проблем при обеспечении информационной безопасности в коммерческих организациях Республики Беларусь, в том числе в процессе стратегического управления ими, было определено что основным объектом риска в современном мире выступает компьютерная система (далее - КС) организации.

Под угрозой информационной безопасности КС следует понимать потенциальную либо реально существующую угрозу преднамеренного или непреднамеренного на информацию КС, которая прямо или косвенно способно навредить текущей или будущей деятельности организации, пользователям информации и (или) владельцам информации.

С позиции воздействия полагаем возможным разделить угрозы информационной безопасности КС на два основных вида:

1 Форс-мажорные факторы – угрозы физического воздействия на КС организации из вне, которые невозможно предсказать, т.е. угрозы, которые не зависят от деятельности человека (например, стихийные бедствия).

2 Искусственно созданные угрозы – условно предсказуемые угрозы, являющиеся следствием человеческой деятельности.

В свою очередь искусственные угрозы логично разделить на намеренные и случайные в зависимости от вызвавших их мотивов и действий.

Среди случайных можно выделить:

– ошибки и неточности в разработке архитектуры КС;

– ошибки и неточности при разработке программного обеспечения КС;

– любые сбои, вызывающие некорректную работу технических средств КС, линий связи и электроснабжения;

– ошибки пользователей КС;

– возможное воздействие на технические средства КС электромагнитных полей расположенных рядом устройств и другие.

Случайные угрозы информационной безопасности реализуются непреднамеренно и решаются при помощи обновления протоколов безопасности разработки и использования КС. В то же время, с преднамеренными угрозами дело обстоит сложнее: вероятности их реализации значительно выше, а последствия куда серьёзнее. Преднамеренные угрозы можно разделить на три основных вида [1]:

1 Угрозы конфиденциальности информации.

Под конфиденциальностью понимается указание на необходимость введения ограничений на круг лиц, имеющих доступ к информации. Соответственно под угрозой конфиденциальности следует понимать нарушение установленных ограничений на доступ к информации.

2 Угрозы целостности информации.

Целостность информации – это такое её свойство, которое состоит в существовании информации в изначальном неискажённом виде, т.е. неизменном по отношению к некоторому фиксированному состоянию. В качестве угрозы в данном случае будет выступать преднамеренное искажение информации.

3 Угрозы доступности информации.

Под доступностью информации подразумевается свойство КС, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость. Угрозой в данном случае будет выступать несанкционированная блокировка доступа к информации. Блокирование может быть постоянным или временным, в зависимости от того, насколько быстро информация потеряет свою ценность для пользователей и (или) владельцев.

Выделяют четыре уровня взаимодействия пользователя с информационными ресурсами КС. В свою очередь каждый уровень имеет свои угрозы информационной безопасности в зависимости от вида угроз. Рассмотрим их подробнее:

I уровень физических носителей информации:

– угроза параметрам системы – риск определения типа и параметров носителей информации;

– угроза конфиденциальности – риск хищения, копирования, перехвата информации с физических носителей;

– угроза нарушения целостности – нарушение устройства или полное уничтожение физического носителя информации;

– угроза доступности – выведение из строя технических носителей информации.

II уровень средств взаимодействия с пользователем КС:

– угроза параметрам системы – доступ к данным о программно-технической среде, доступ к данным о функциях системы, получение информации об используемых средствах защиты и системе безопасности;

– угроза конфиденциальности – несанкционированный доступ к информационным ресурсам КС, совершение пользователем нарушающих систему безопасности действий, несанкционированное копирование программного обеспечения, проведение перехвата информации по каналам связи;

– угроза нарушения целостности – внесение изменений в программное обеспечение и информацию, самовольная установка и применение нештатного программного обеспечения, заражение КС вирусами;

– угроза доступности – выявление ошибок и неточностей проектирования архитектуры и разработки КС, обход или отключение встроенных механизмов защиты КС.

III уровень средств представления информации пользователю КС:

– угроза параметрам системы – несанкционированное изменение условий представления информации;

– угроза конфиденциальности – визуальное наблюдение при представлении информации лицами, не имеющими к ней доступ, несанкционированное раскрытие представления информации;

– угроза нарушения целостности – искажение способа представления информации, уничтожение информации;

– угроза доступности – искажение согласования между семантическими и синтаксическими нормами и конструкциями языка.

IV уровень содержания информации:

– угроза параметрам системы – несанкционированное изменение качественного содержания информации;

– угроза конфиденциальности – несанкционированное раскрытие данных третьим лицам;

– угроза нарушения целостности – частичное искажение информации, дезинформация;

– угроза доступности – запрет на использование информации пользователями.

Использованные источники:

1. Киреенко, А. Е. Современные проблемы в области информационной безопасности: классические угрозы, методы, средства их предотвращения / А.Е. Киреенко // Молодой учёный. – 2012. – № 3 (38). – С. 40 - 46.