УДК 00.056

АНАЛИЗ УГРОЗ И РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Жолдошбай уулу Э., Медетбек кызы А., Кулмурзаева А.К.
Кыргызский государственный университет строительства, транспорта и архитектуры имени Н. Исанова

В статье проводится анализ угроз и рисков информационной безопасности распределенных информационных систем (РИС). Отмечено, что особенностью защиты информации от угроз в РИС по сравнению с сосредоточенными сетями является необходимость обеспечения гарантированной передачи информации по коммуникационной подсети.

***Ключевые слова*:** информационная безопасность, риск информационной безопасности, анализ рисков, количественная оценка, качественная оценка, распределенные системы.

БӨЛҮШТҮРҮЛГӨН МААЛЫМАТТЫК ТУТУМДАРДЫН МААЛЫМАТТЫК КООПСУЗДУК КОРКУНУЧТАРЫН ЖАНА ТОБОКЕЛДИКТЕРИН ТАЛДОО МЕТОДДОРУ

Жолдошбай уулу Э., Медетбек кызы А., Кулмурзаева А.К.
Н. Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт жана архитектуры университети

Макалада бөлүштүрүлгөн маалыматтык тутумдардын (БМТ) маалыматтык коопсуздук коркунучтарына жана тобокелдиктерине талдоо жүргүзүлөт. Ал топтолгон тармактарга салыштырмалуу БМТда коркунучтардан маалыматты коргоонун өзгөчөлүгү болуп коммуникациялык түйүн боюнча маалыматты кепилденген жөнөтүүнү камсыздоо зарылдыгы санала тургандыгы белгиленген.

***Негизги сөздөр*:** маалыматтык коопсуздук, маалыматтык коопсуздук коркунучу, тобокелдиктерди талдоо, сандык баалоо, сапаттык баалоо, бөлүштүрүлгөн системалар.

METHODS FOR ANALYSIS OF THREATS AND RISKS OF INFORMATION SECURITY OF DISTRIBUTED INFORMATION SYSTEMS

Zholdoshbai uulu E., Medetbek kyzy A., Kulmurzaeva A.K.
Kyrgyz State University of Construction, Transport and Architecture named after N. Isanov

The analysis of threats and risks of informative safety of the distributed informative systems (DIS) is conducted in the article. It is marked that by the feature of defence of information from threats in DIS as compared to the concentrated networks there is a necessity of providing of the assured information transfer on of communication subnet.

Keywords: informative safety, risk of informative safety, analysis of risks, quantitative estimation, quality estimation, distributed systems.

Новые подходы и потребности безопасности информационных систем (ИС) требуют эффективного анализа ситуаций, возникающих с учетом новых потребностей предотвращения распределенных информационных атак. В первую очередь, следует разрабатывать релевантные инструментально-методологические средства, способные учесть не только критические ситуации, но и адаптивно оценивать риски, угрозы и ущерб. Требуются также и модели (профили) киберугроз, принятие решений, сценарии имитирования и изучение откликов на угрозы.

Во многих организациях распределенные системы стали основным средством обработки и хранения информационных ресурсов и нередко содержат конфиденциальную информацию.

Создание распределенной системы в организации, или внедрение новых информационных средств в существующие системы, должны сопровождаться проведением тщательного анализа с точки зрения оценки состояния информационной безопасности. Оценка состояния информационной безопасности распределенной системы заключается в оценке защищенности ее информационных ресурсов.

В настоящее время ни одна система, регулирующая потоки распределения информации, на сегодняшний день не способна гарантировать полную защищенность. Это касается не системного уровня безопасности, а в принципе практически функционирующих моделей, в которых реализуются специализированные инструменты защиты.

Адекватные меры повышения защищенности каналов снижают эффективность действий злоумышленников на разных уровнях, в конечном итоге создавая такие условия, при которых и попытки проникновения в систему становятся нецелесообразными. Средства обеспечения информационной безопасности распределенных информационных систем (РИС) должны проектироваться и встраиваться в рабочую группу только после проведения комплексного анализа потенциальных угроз. Всесторонний анализ рисков даст объективную оценку факторов и параметров возможного вторжения злоумышленников, стороннего вывода системы из строя, перехвата данных и т. д. [1, 2].

При построении безопасной распределенной информационной системы необходимо учитывать:

- сложность системы, которая определяется как количеством подсистем, так и разнообразием их типов и выполняемых функций;

- невозможность обеспечения эффективного контроля за доступом к ресурсам, распределенным на больших расстояниях, возможно за пределами границ страны;

- возможность принадлежности ресурсов сети различным владельцам.

Особенностью защиты информации от непреднамеренных угроз в РИС по сравнению с сосредоточенными сетями является необходимость обеспечения гарантированной передачи информации по коммуникационной подсети. Для этого в РИС должны быть предусмотрены дублирующие маршруты доставки сообщений, предприняты меры против искажения и потери информации в каналах связи. Такие сложные системы должны строиться как адаптивные, в которых обеспечивается постоянный контроль работоспособности элементов системы и возможность продолжения функционирования даже в условиях отказов отдельных подсистем.

В РИС все потенциальные преднамеренные угрозы безопасности информации делят на две группы: пассивные и активные.

К ***пассивным*** относятся угрозы, целью реализации которых является получение информации о системе путем прослушивания каналов связи (злоумышленник может получить информацию путем перехвата незашифрованных сообщений или путем анализа трафика (потока сообщений), накапливая информацию об интенсивности обмена отдельных абонентов, о структуре сообщений, о маршрутах доставки сообщений и т.п.).

Активные угрозы предусматривают воздействие на передаваемые сообщения в сети и несанкционированную передачу фальсифицированных сообщений с целью воздействия на информационные ресурсы объектов РИС и дестабилизацию функционирования системы. Возможно также непосредственное воздействие на коммуникационную подсистему с целью повреждения аппаратных средств передачи информации.

Информационная угроза определяет источники возникновения информационных рисков через уязвимости системы, а факторы следует рассматривать как обстоятельства, способствующие или препятствующие реализации риска. Большинство угроз реализуется путем осуществления атак на информационные активы внутренними и внешними нарушителями и/или программными средствами с использованием уязвимостей. Управление информационными рисками заключается в согласованном воздействии на объекты и субъекты информационно-вычислительной и телекоммуникационой инфраструктуры системы мониторинга в направлении устранения угроз, уязвимостей и факторов рисков с целью предупреждения или минимизации возможных последствий от их реализации.

Подводя итог, перечислим те преимущества, которые дает проведение анализа рисков в сфере ИБ:

- выявление проблем в сфере безопасности (не только уязвимостей компонент системы, но и недостатков политик безопасности и т.д.);
- анализ рисков позволяет нетехническим специалистам (в частности, руководству организации) оценить выгоды от внедрения средств

и механизмов защиты и принять участие в процессе определения требуемого уровня защищенности КС;

- проведение оценки рисков добавляет обоснованность рекомендациям по безопасности;
- ранжирование рисков по приоритетам позволяет выделить наиболее приоритетные направления для внедрения новых СЗИ, мер и процедур обеспечения ИБ;
- подробно описанные методики анализа рисков позволяет людям, не являющимся экспертами в данной области, воспользоваться аккумулированными в методике знаниями, чтобы получить заслуживающие доверия результаты анализа.

В то же время, необходимо отметить, что оценка рисков на качественном уровне не позволяет однозначно сравнить затраты на обеспечение ИБ и получаемую от них отдачу (в виде снижения суммарного риска). Поэтому более предпочтительными представляются количественные методики. Но они требуют наличия оценок вероятности. Неправильная оценка вероятности угрозы в отношении очень дорогостоящего актива может кардинально изменить оцениваемое значение суммарной стоимости рисков.

Также необходимо отметить, что передаваемые в РИС сообщения могут несанкционированно модифицироваться или уничтожаться. Злоумышленник может размножать перехваченные сообщения, нарушать их очередность следования, изменять маршрут доставки, подменять сообщения, может предпринимать попытки несанкционированного доступа к информационным ресурсам удаленного объекта ИС, осуществления несанкционированного изменения программной структуры ИС путем внедрения вредительских программ.

В РИС, наряду с мерами, предпринимаемыми для обеспечения безопасности информации в сосредоточенных ИС, реализуется ряд механизмов для защиты информации при передаче ее по каналам связи, а

также для защиты от несанкционированного воздействия на информацию ИС с использованием ИС.

Все методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети, могут быть распределены по группам:

- обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС;
- защита информации на уровне подсистемы управления сетью;
- защита информации в каналах связи;
- обеспечение контроля подлинности взаимодействующих процессов.

В заключении можно отметить, что применение рассмотренного подхода на практике способствует выявлению основных угроз защиты безопасности, основываясь на банке данных угроз безопасности информации. Оценка рисков ИБ является приоритетным, так как может позволить функционировать системе управления рисками в режиме реального времени, при условии достаточности временных и финансовых ресурсов, в отличие от рассмотренного подхода, практическая реализация которого возможно в качестве разового или периодически проводимого мероприятия.

ЛИТЕРАТУРА

1. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность // Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

2. Губарева О.Ю. Оценка рисков информационной безопасности в телекоммуникационных сетях. // Вестник Волжского университета им. В.Н. Татищева. - 2013. № 2 (21). - С. 76–81.