УДК 004.056

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЯ

Абдулаев А., Кулмурзаева А.К., Курманбек уулу Н.
Кыргызский государственный университет строительства, транспорта и архитектуры имени Н. Исанова

В статье рассматриваются процедуры проведения анализа угроз информационной безопасности информационно-телекоммуникационных систем предприятия. Приводятся основные источники угроз информационной безопасности. Проведенный анализ угроз позволяет выделить составляющие современных компьютерных угроз – их источники и движущие силы, способы и последствия реализации.

Ключевые слова: информационная безопасность, угроза информационной безопасности, анализ угроз, источники угроз, информационно-телекоммуникационных систем.

ИШКАНАНЫН МААЛЫМАТТЫК-ТЕЛЕКОММУНИКАЦИЯЛЫК ТУТУМДАРЫНЫН МААЛЫМАТТЫК КООПСУЗДУГУНУН КОРКУНУЧТАРЫН ТАЛДОО

Абдулаев А., Кулмурзаева А.К., Курманбек уулу Н.
Н. Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт жана архитектуры университети

Макалада мамлекеттик ишкананын маалыматтык жана телекоммуникациялык тутумдарынын маалыматтык коопсуздугунун коркунучтарын талдоо жол-жоболору талкууланат. Маалыматтык коопсуздукка коркунучтардын негизги булактары көрсөтүлөт. Коркунучтарды талдоо заманбап компьютердик коркунучтардын компоненттерин – алардын булактарын жана кыймылдаткыч күчтөрүн, аларды ишке ашыруунун ыкмаларын жана кесепеттерин аныктоого мүмкүндүк берет.

***Баштапкы сөздөр*:** маалымат коопсуздугу, маалыматтык коопсуздук коркунучу, коркунучтарды талдоо, коркунуч булактары, маалыматтык-телекоммуникациялык тутумдар.

ANALYSIS OF THREATS TO INFORMATION SECURITY OF INFORMATION AND TELECOMMUNICATION SYSTEMS OF THE ENTERPRISE

Abdulaev A., Kulmurzayeva A.K., Kurmanbek uulu N.
Kyrgyz State University of Construction, Transport and Architecture named after N. Isanov

The article discusses procedures for conducting analysis of threats to information security of information and telecommunication systems of the enterprise. The main sources of threats to information security are given. The analysis of threats makes it possible to distinguish the components of modern computer threats - their sources and driving forces, methods and consequences of implementation.

***Key words*:** information security, information security threat, threat analysis, threat sources, information systems, telecommunication systems.

Внедрение новых информационных технологий во всех сферах деятельности человека обуславливает рост значимости информационной безопасности. Нарушения, которые могут быть вызваны несвоевременным выявлением и предотвращением угроз информационной безопасности органов государственного управления, предоставляют угрозу национальной безопасности. Вследствие этого, сфера выявления и противодействия угроз является приоритетной [1].

В настоящее время известен достаточно обширный перечень угроз безопасности информационно-телекоммуникационных систем. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для формулирования требований к системе защиты информационных систем [2. 3. 4].

Соответственно, актуальность и необходимость применения процедур анализа и управления угрозами информационной безопасности с каждым годом возрастает в связи с повышением роли информационно-телекоммуникационных систем.

Основной формой воздействия нарушителя на ресурсы информационно-телекоммуникационных систем (ИТКС) государственного предприятия (ГП) являются компьютерные атаки, представляющие собой

упорядоченные во времени действия по преодолению системы защиты и нарушению безопасности информации, реализуемые посредством программ с потенциально опасными (деструктивными) функциями. К числу таких функций относятся:

- сокрытие признаков своего присутствия в программно-аппаратной или вычислительной среде;

- осуществление сбора данных о параметрах ИТКС и ее системе защиты;

- самодублирование или перенос своих фрагментов в другие области оперативной или внешней памяти;

- ассоциирование с другими программами в вычислительном окружении; искажение или разрушение кода программ в оперативной памяти; сохранение фрагментов информации из оперативной памяти в некоторой области внешней памяти (локальной или удаленной);

- искажение, блокирование или подмена выводимого во внешнюю память или в канал связи массива информации, образующегося при выполнении прикладных программ;

- подавление информационного обмена ИТКС; искажение или фальсификация информации при обмене по каналам телекоммуникационных сетей;

- нейтрализация или нарушение работы тестовых программ и системы защиты.

В случае успеха компьютерных атак реализуются одна или несколько угроз безопасности функционирования ИТКС ГП, то есть потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или другие компоненты ИТКС ГП могут прямо или косвенно привести к нарушению безопасности информации.

В зависимости от принадлежности источника угрозы выделяют внутренние и внешние угрозы безопасности функционирования ИТКС ГП (рисунок 1).

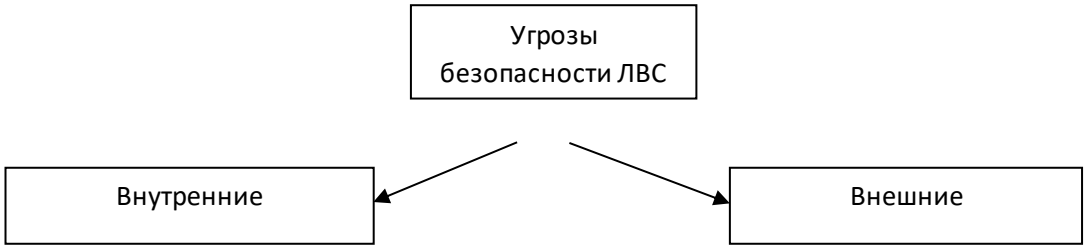

Рис. 1 - Классификация угроз безопасности ИТКС ГП

Основным источником внутренних угроз являются:

- специалисты в области разработки и эксплуатации программного обеспечения (ПО) и технических средств;

- знакомые со спецификой решаемых в ИТКС ГП задач, структурой, основными функциями и принципами работы программно-аппаратных средств защиты информации, имеющие возможность использования штатного оборудования и технических средств сети.

В зависимости от конкретных условий функционирования и особенностей ИТКС ГП в качестве источника внутренних угроз могут выступать:

- авторизованные субъекты доступа - администратор вычислительной сети, администратор баз данных, администратор безопасности, пользователи, программисты, разработчики;

- вспомогательный технический и обслуживающий персонал - служба охраны, жизнеобеспечения и др.

Источниками внешних угроз для ИТКС ГП являются:

- представители криминальных структур и террористических организаций, заинтересованные в хищении информации, составляющей государственную или коммерческую тайну, или причинении ущерба инфраструктуре организации;

- хакеры или недобросовестные поставщики телекоммуникационных услуг;

- подразделения и службы технической разведки иностранных государств.

Основным классификационным признаком угроз безопасности информации выступает их направленность. В соответствии с этим выделяют угрозы нарушения конфиденциальности, целостности или доступности информации.

При этом в качестве объекта угрозы рассматривается как оперативная информация, обрабатываемая в интересах конечных пользователей ИТКС ГП, так и технологическая, используемая для организации функционирования комплекса средств обработки информации и комплекса средств защиты информации.

К угрозам нарушения конфиденциальности информации в ИТКС ГП относятся:

- несанкционированное чтение или копирование информации, в том числе остаточной или технологической, на любом из этапов ее обработки;

- несанкционированный импорт или экспорт конфиденциальной информации;

- передача информации между элементами ЛВС органов, относящимся к разным классам защищенности.

Угрозами нарушения целостности являются:

- несанкционированная модификация либо удаление программ или данных;

- вставка, изменение или удаление данных в элементах протокола в процессе обмена между пользователями ИТКС ГП;

- потеря данных в результате сбоев, нарушения работоспособности элементов ИТКС ГП или некомпетентных действий субъектов доступа.

К угрозам нарушения доступности относятся:

- повторение или замедление элементов протокола; подавление обмена в ИТКС ГП;

- моделирование ложной тождественности узла ИТКС ГП или связи для передачи данных;

- использование ошибок или недокументированных возможностей служб и протоколов передачи данных для инициирования отказа в обслуживании;

- перерасход вычислительных или телекоммуникационных ресурсов.

В отдельный класс угроз следует выделить события, которые в зависимости от условий могут нарушить любую из составляющих безопасности информации:

- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

- несанкционированное включение в состав комплексов средств обработки информации и средств защиты информации новых элементов или изменение режимов их работы;

- доступ к ресурсам ИТКС ГП без использования штатных средств вычислительной техники (СВТ) или выполнение программ, или действий в обход системы защиты;

- подбор, перехват или разглашение (компрометация) параметров аутентификации или ключей шифрования (дешифрования); несанкционированный запуск программ;

- использование нестойких параметров аутентификации или ключей/шифрования либо их несвоевременная смена;

- навязывание ранее переданного или ложного сообщения, отрицание факта его передачи или приема;

- некомпетентное использование, настройка или администрирование комплексов средств обработки информации и средств защиты информации;

- сбои и отказы в работе комплексов средств обработки информации и средств защиты информации.

Анализ угроз безопасности функционирования ИТКС ГП в условиях информационного конфликта позволяет сделать вывод, что в зависимости от текущего уровня защищенности информации от НСД стратегии нарушителя по преодолению системы защиты будут изменяться.

Конечное число видов информационных воздействий определяет конечное число видов стратегий воздействий нарушителя. В зависимости от возможностей нарушителя по воздействию на определенные свойства защищаемой информации можно выделить следующие типы стратегий.

1. Нарушение доступности информации. Используется в случае, если нарушитель не может получить непосредственный доступ к защищаемой информации, и вынужден воздействовать на него опосредованно, путем изменения структуры, параметров, режимов работы или нарушения (снижения) качества функционирования комплексов средств обработки информации и средств защиты информации.

2. Нарушение конфиденциальности информации. Применяется в случае существования канала НСД или возможности дешифрования информации в приемлемые для нарушителя сроки.

3. Нарушение целостности информации. Используется в случае, если несанкционированное чтение или копирование информации невозможно или нецелесообразно.

4. Навязывание ложной информации. Применяется для воздействия на подсистему организационного управления с целью принятия атакуемой стороной решений, не адекватных ситуациям.

Таким образом, проведенный анализ угроз информационной безопасности позволяет выделить составляющие современных компьютерных угроз – их источники и движущие силы, способы и последствия реализации. Анализ исключительно важен для получения всей необходимой информации об информационных угрозах, определения потенциальной величины ущерба, как материальной, так и нематериальной, и выработки адекватных мер противодействия.

ЛИТЕРАТУРА

1. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.
2. Андреев Н.О. Формирование и развитие угроз в информационных системах // Прикладная информатика. - 2006. - № 6. – С. 87-100.
3. Тершуков Д.А. Анализ современных угроз информационной безопасности // НБИ технологии. - 2018. - Т. 12. - № 3.
4. Ляпидов К.В. Анализ и классификация основных угроз информационной безопасности. - Электрон. дан. – Режим доступа:
1. https://lyapidov.ru/analysis-and-classification-of-the-main-threats-to-information-security/