## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. СЕТИ И СИСТЕМЫ

**УДК. 004.413.4:621.39**

# АНАЛИЗ РИСКОВ И ОПРЕДЕЛЕНИЕ СТРАТЕГИИ ЗАЩИТЫ В ТЕЛЕКОММУНИКАЦИЯХ

***Абляева Анастасия Николаевна,*** *магистрант группы ИТССм-1-16, направления 690300 Инфокоммуникационные технологии и системы связи, ИЭТ КГТУ им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч. Айтматова 66. E-mail: nastya-tls@mail.ru*
***Зимин Игорь Викторович,*** *к.т.н., доцент ИЭТ при КГТУ им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч. Айтматова 66.E-mail: igorzimin777@rambler.ru/*

В данной статье рассматривается полный анализ рисков информационной безопасности в сетях телекоммуникаций и основные принципы обеспечения информационной безопасности.

**Ключевые слова:** Риск, протокол, информационная безопасность, телекоммуникации, угрозы, бизнес-процесс, защитный механизм, анализ, технологии.

***Ablyaeva Anastasia Nikolaevna,*** *магистрант группы ИТССм-1-16, направления 690300 Инфокоммуникационные технологии и системы связи, ИЭТ КГТУ им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч. Айтматова 66. E-mail: nastya-tls@mail.ru*
***Зимин Игорь Викторович,*** *к.т.н., доцент ИЭТ при КГТУ им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч. Айтматова 66.E-mail: igorzimin777@rambler.ru/*

This article discusses a complete analysis of the information security risks in telecommunication networks and basic principles of information security.

**Keywords:** Risk, protocol, information security, telecommunications, threats, business process, defense mechanism, analysis, technology.

**Введение.** На сегодняшний день невозможно представить жизнь людей без использования систем телекоммуникаций. С ростом числа абонентов и быстрого развития глобальной сети Интернет, возросло количество угроз информационной безопасности сетям телекоммуникаций, как государства, так и частных лиц. В связи с этим на данный момент, вопрос защиты информационной безопасности набирает широкую популярность. Телекоммуникационные компании (ТК) - одни из самых чувствительных к надежной и безопасной работе информационных систем (ИС) - предоставляемые ими услуги практически полностью создаются на основе ИТ - решений. От этого зависит не только их качество, но и репутация операторов связи, и лояльность клиентов, а также легитимность оказания услуг. Особую важность представляют вопросы борьбы с мошенничеством и гарантирования доходов [5].

Сегодня, большинство компаний телекоммуникаций имеют достаточно хорошую оснащенность средствами обеспечения информационной безопасности (ИБ), наибольшую популярность набирают средства решения, позволяющие оптимизировать и автоматизировать процессы ИБ, повысить управляемость, обеспечить прозрачность, легитимность, а так же устойчивость в аварийных ситуациях. Также возрастает популярность относительно сохранения стабильной и бесперебойной работы компании. Одной из наиболее важных составляющих в данном вопросе является обеспечение

непрерывного (стабильного) функционирования бизнес-процессов. Однако, существуют сложности осуществления данной задачи в плане постоянного изменения процессов в компании, а также большого числа разрозненных ИС. Это приводит к тому, что существующие на данный момент способы управления правами доступа к ИТ - системам, имеющиеся в телекоммуникациях, становятся с точки зрения безопасности , а также затрат ресурсов – неэффективными.

Из-за сложной структуры ИТ- систем в телекоммуникациях уровень рисков информационной безопасности значительно увеличивается, это требует увеличения защитных механизмов и устройств. Риски возникают вследствие наличия различных уязвимостей в сетях телекоммуникаций из за широкого спектра предоставляемых услуг на рынке связи. Чтобы построить хорошую систему защиты информационной безопасности необходимо провести анализ рисков. Введем данное понятие. Анализ рисков – это действия, направленные на выявление факторов рисков, а также их оценки на определенное событие или систему. В сущности, анализ рисков – это анализ возможности того, что могут произойти определенные события, которые окажут отрицательное воздействие на работу системы. В сфере информационных технологий анализ рисков, прежде всего связан с созданием или развитием, вводом или выводом из эксплуатации информационных систем, технологий или любых других активов.

ИТ активы – это все артефакты, имеющие определенную ценность для организации, использующей их в своей деятельности. Активы могут быть выражены, как в конкретном стоимостном значении, так и не иметь четко определенной ценности, в актуальный момент времени [4].

При необходимости производят полный анализ рисков. В процессе такого анализа рассматриваются следующие факторы:

- ✓ - бизнес процессы (с точки зрения информационной безопасности);
- ✓ - ресурсы организации и их ценность;
- ✓ - угрозы безопасности – потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам и оценка их параметров;
- ✓ - уязвимости – слабые места в защите (способствуют реализации угроз);

На основе результатов вышеуказанных анализов собирают сведения относительно оценки рисков для информационной системы организации, как отдельных подсистем, так и баз данных. После полного анализа рисков при высоком показателе, необходимо минимизировать данный коэффициент, что поспособствует улучшению информационной защиты системы.

В настоящее время для проведения анализа рисков существуют специализированные программные продукты. Одним из наиболее популярных является Метод CRAMM.

Анализ рисков (методом CRAMM) включает в себя идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов. Контроль рисков состоит в идентификации и выборе контрмер, позволяющих снизить риски до приемлемого уровня. [4]

Формальный метод, основанный на этой концепции, должен позволить убедиться, что защита охватывает всю систему и существует уверенность в том, что:

- ✓ - все возможные риски идентифицированы;
- ✓ - уязвимости ресурсов идентифицированы и их уровни оценены;
- ✓ - угрозы идентифицированы и их уровни оценены;
- ✓ - контрмеры эффективны;
- ✓ - расходы, связанные с ИБ, оправданы.

После полного анализа рисков, желательно улучшить (при выявлении уязвимостей) информационную безопасность системы. Рассмотрим некоторые принципы обеспечения информационной безопасности в ТКМ.

**Обеспечение защиты информации в ТКС.** Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах: [1,3]

*Системный подход к построению системы защиты*, означающий оптимальное сочетание взаимосвязанных организационных программных, аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

*Принцип непрерывного развития системы*. Этот принцип, являющийся одним из основополагающих для компьютерных информационных систем, еще более актуален для СИБ. Способы реализации угроз информации в ИТ непрерывно совершенствуются, а потому обеспечение безопасности ИС не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования СИБ, непрерывном контроле, выявлении ее узких и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа.

*Разделение и минимизация полномочий* по доступу к обрабатываемой информации и процедурам обработки, т. е. предоставление как пользователям, так и самим работникам ИС, минимума строго определенных полномочий, достаточных для выполнения ими своих служебных обязанностей.

*Полнота контроля и регистрации попыток несанкционированного доступа*, т. е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИТ без ее предварительной регистрации.

*Обеспечение надежности системы защиты*, т. е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей и обслуживающего персонала.

*Обеспечение контроля за функционированием системы защиты*, т.е. создание средств и методов контроля работоспособности механизмов защиты.

*Обеспечение всевозможных средств борьбы* с вредоносными программами.

*Обеспечение экономической целесообразности* использования системы, защиты, что выражается в превышении возможного ущерба ИС и ИТ от реализации угроз над стоимостью разработки и эксплуатации СИБ.

Таким образом для обеспечения хорошей защиты информационной безопасности необходимо провести полный анализ рисков, выявить наличие уязвимостей и принять меры по их устранению.

**Вывод:** Таким образом, для обеспечения хорошей защиты информационной безопасности необходимо провести полный анализ рисков, выявить наличие уязвимостей и принять меры по их устранению.

## Список литературы

1. Виды анализа рисков. [Электронный ресурс] - Режим доступа: http://www.bainr.ru/article21.html

2. Емельянова Н. З. Партыка Т. Л. Попов И. И. Защита информации в персональном компьютере 2009г.

3. Информационная безопасность в сетях ТКМ [Электронный ресурс] - Режим доступа: http://5fan.ru/wievjob.php?id=21935

4. Торокин А. А Основы инженерно-технической защиты информации 1997

5. Решения для телекоммуникационных компаний. [Электронный ресурс] / Инфосистемы Джет - Режим доступа: http://www.jet.msk.su/services_and_solutions/information_security/solutions_catalog/telecom/index.php?print=y -Загл. с экрана.