УДК 004.056

АНАЛИЗ РИСКОВ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Беребин А.Ю., Капарбек уулу Б., Курманбекова А.К.
Кыргызский государственный университет строительства, транспорта и архитектуры имени Н. Исанова

В статье рассматриваются процедуры проведения анализа рисков и угроз информационной безопасности на предприятия. Приводятся основные источники угроз и зоны риска информационной безопасности. В процессе анализа рисков проводится оценка критичности идентифицированных уязвимых мест и возможности их использования потенциальным злоумышленником для осуществления несанкционированных действий**.**

Ключевые слова: информационная безопасность, угроза информационной безопасности, информационные риски, анализ рисков, защита информации, анализ угроз.

ИШКАНАДАГЫ МААЛЫМАТТЫК КООПСУЗДУК ТОБОКЕЛДИКТЕРИН ЖАНА КОРКУНУЧТАРЫН ТАЛДОО

Беребин А.Ю., Капарбек уулу Б., Курманбекова А.К.
Н. Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт жана архитектуры университети

Макалада ишканадагы маалыматтык коопсуздук тобокелдиктерин жана коркунучтарын талдоо жүргүзүү процедуралары каралат. Маалыматтык коопсуздуктун коркунучтарынын негизги булактары жана тобокелдик зоналары келтирилет. Тобокелдиктерди талдоо процессинде, аныкталган аялуу жактарга критикалык баа берүү жана потенциалдуу чабуулчу тарабынан уруксатсыз аракеттерди жасоо үчүн аларды пайдалануу мүмкүнчүлүгү бааланат.

Баштапкы сөздөр: маалыматтык коопсуздук, маалыматтык коопсуздук коркунучу, маалыматтык тобокелдиктер, тобокелдиктерди талдоо, маалыматты коргоо, коркунучтарды талдоо.

ANALYSIS OF RISKS AND THREATS TO INFORMATION SECURITY AT ENTERPRISES

Berebin A.Yu., Kaparbek uulu B., Kurmanbekova A.K.
Kyrgyz State University of Construction, Transport and Architecture named after N. Isanov

The article discusses procedures for conducting analysis of risks and threats to information security at the enterprise. The main sources of threats and information security risk zones are given. In the process of risk analysis, the criticality of identified vulnerabilities and the possibility of their use by a potential attacker to carry out

Keywords: information security, information security threat, information risk, risk analysis, information protection, threat analysis.

В век информатизации автоматизация бизнес-процессов предприятия, использование различных информационных сервисов для обработки информации – это залог эффективности и конкурентоспособности на рынке.

Внедрение различных информационных систем на предприятии позволяет решить вопросы полноты, достоверности и конфиденциальности получаемой информации.

Использование таких систем на предприятии сопровождается усложнением задач по управлению информационными ресурсами. Наиболее важными из них являются внедрение системы защиты информации и минимизация появляющихся рисков, связанных с информационными процессами на предприятии.

Построение систем защиты информации начинается с создания модели угроз. Для предприятий риски зависят от сферы деятельности и готовности информационной системы к отражению атак. Модель необходимо строить, с учетом результатов анализа угроз информационной безопасности (ИБ) и после классификации типов нарушителей.

Под угрозой ИБ понимается совокупность условий и факторов, реализация которых приводит к ситуации, в которой информационная

безопасность организации оказывается в зоне риска. Результатом реализации риска оказывается событие, наступление которого имеет экономические или иные неблагоприятные последствия для человека, организации или государства. Формат ущерба для информации может быть трояким – утечка, изменение или нарушение уровня доступности. Но последствия оказываются разнообразными – от техногенных аварий до потери средств с карточных счетов или разглашения компрометирующей информации.

В процессе анализа угроз информации необходимо оценить:

- источник риска;
- зону риска;
- гипотетическую фигуру злоумышленника;
- вероятность реализации риска;
- степень ущерба от его реализации;
- соотношение расходов, необходимых для минимизации риска, и убытка, причиняемого в случае его реализации.

Традиционно основным источником угроз считаются международные или национальные хакерские группировки. Однако на практике ситуация иная, все чаще на первый план выходят криминальные группировки или иностранные технические разведки. Эксперты выделяют три группы источников:

- антропогенные (внутренние и внешние);
- техногенные;
- стихийные.

Антропогенные источники угроз информационной безопасности – это граждане или организации, случайные или намеренные действия или бездействие которых приводят к реализации рисков ИБ.

Техногенные угрозы сложнее спрогнозировать, но проще предотвратить. К ним относятся технические средства, внутренние и внешние.

К внутренним относятся:

- несертифицированное и нелицензионное программного обеспечения (ПО);
- лицензионное ПО, имеющее известные хакерам изъяны или незадекларированные возможности;
- средства контроля за работоспособностью информационных сетей со слабыми возможностями мониторинга, отказ от своевременного и четкого реагирования на их сигналы;
- некачественные средства наблюдения за помещениями и сотрудниками;
- неисправное или некачественное оборудование.

Внешние источники:

- каналы связи;
- инженерно-технические сети;
- провайдеры интернет-услуг и облачных технологий.

При анализе зоны риска нужно установить объект, на который направлена гипотетическая угроза. С технической точки зрения объектами становятся информация, оборудование, программы, каналы связи, системы управления и контроля.

Классическими «жертвами» злоумышленников становятся признаки доброкачественности информации:

- **конфиденциальность.** Этот риск реализуется при неправомерном доступе к данным и их последующей утечке;
- **целостность.** В результате реализации риска данные могут быть утрачены, модифицированы, искажены, и принимаемые на их основе решения, управленческие или технические, окажутся неверными;
- **доступность.** Доступ к данным и услуге блокируется или утрачивается.

При определении сектора реализации угрозы требуется дополнительно оценить степень важности данных, их стоимость. Это

позволит провести более точный анализ угроз информационной безопасности.

При анализе зон риска нужно также принимать во внимание:

- объем текущей зоны контроля за информационной безопасностью и перспективы ее расширения в случае увеличения организации, появления новых предприятий или сфер деятельности;
- особенности функционирования программно-технических средств и их совместимость, перспективы возникновения новых угроз, новых требований регуляторов, направлений развития рынка информационных технологий;
- возникновение зон информационного периметра, вне защитных мер;
- непредсказуемость точек атаки, их количество и рост;
- особенности управления сложными, многообъектными сетями.

Факторы реализации риска изменчивы, поэтому их анализ должен происходить с установленной в компании регулярностью.

Провести анализ угроз информационной безопасности невозможно, если не опираться на понимание типов и роли нарушителей ИБ.

Обычно классифицирует нарушителей по их потенциалу (низкий, средний, высокий). Он влияет на набор возможностей, перечень используемых технических, программных и интеллектуальных средств.

Большинство угроз генерируется **нарушителями с низким потенциалом**. Они связаны с возможностью получения ресурсов для неправомерного доступа к информации только из общедоступных источников. Это инсайдеры и взломщики, использующие интернет-ресурсы, для мониторинга работоспособности системы, распространяющие вредоносные программы.

Нарушители со средним потенциалом способны проводить анализ кода прикладного программного обеспечения, кода сайта, самостоятельно находить в нем ошибки и уязвимости и использовать их

для организации утечек. К этим группам относятся хакерские группировки, конкурентов, применяющих незаконные методы добычи информации, системных администраторов, компании, по заказу разрабатывающие программное обеспечение.

Высокий потенциал характеризуется способностью вносить «закладки» в программно-техническое обеспечение системы, организовывать научные исследования, направленные на сознательное создание уязвимостей, применять специальные средства проникновения в информационные сети для добычи информации.

К категории нарушителей с высоким потенциалом могут относятся только иностранные разведки. Практика добавляет к ним еще и военные ведомства зарубежных стран, по чьему заказу иногда действуют хакеры.

В большинстве случаев предприятию не угрожают злоумышленники с высоким потенциалом. Поэтому, анализ производится исходя из низкого или среднего потенциала инсайдеров или хакеров. Для государственных информационных систем уровень рисков окажется выше.

Иногда при анализе вероятности реализации угрозы требуется еще несколько категорий угроз конфиденциальности информации:

- по степени воздействия на информационные системы (ИС). При реализации пассивных угроз архитектура и наполнение системы не меняются, при активных они частично уничтожаются или модифицируются;
- по природе возникновения – естественные и искусственные. Первые крайне редки, вторые наиболее вероятны, при этом ущерб от реализации первых оказывается выше, часто проявляясь в полной гибели данных и оборудования. Такие угрозы при их вероятности, например, в сейсмоопасных районах создают необходимость постоянного резервного копирования;
- непреднамеренные и преднамеренные.

Целесообразно опираться на статистику, показывающую вероятность реализации того или иного риска.

Риски подразделяются по характеру на внешние и внутренние; по времени возникновения на прошлые или ретроспективные и будущие или перспективные; по фактору возникновения такие, как проектные, операционные риски, процессные, организационные; по последствиям на чистые и спекулятивные.

Так же выделяется подклассификация рисков по степени последствий возникновения и состоит из: допустимого риска, критического риска и катастрофического риска. Эта классификации является важной при принятии решений по осуществлению какой-либо деятельности, связанной с рисками.

Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков

Анализ рисков проводится для оценки реальных угроз нарушения информационной безопасности и разработки рекомендаций, выполнение которых позволит минимизировать эти угрозы.

Анализ рисков дает возможность:

• адекватно оценить существующие угрозы;

• идентифицировать критичные ресурсы ИС;

• выработать адекватные требования по защите информации;

• сформировать перечень наиболее опасных уязвимых мест, угроз и потенциальных злоумышленников;

• получить определенный уровень гарантий, основанный на объективном экспертном заключении.

При анализе рисков осуществляется:

• классификация информационных ресурсов;

• анализ уязвимостей;

• составление модели потенциального злоумышленника;

• оценка рисков нарушения информационной безопасности.

В процессе анализа рисков проводится оценка критичности идентифицированных уязвимых мест и возможности их использования потенциальным злоумышленником для осуществления несанкционированных действий.

В настоящее время разработано множество систем и методик по расчету и анализу возможных информационных рисков, которые позволяют определить новых видов рисков, которые могут составлять серьезную угрозу развитию и функционированию предприятий.

ЛИТЕРАТУРА

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.:ИД «Форум»: Инфра-М, 2012. - 416 с.
2. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность [Текст] / Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.: ил.
3. Анализ рисков информационной безопасности // securitylab.ru. [Электронный ресурс].Режим доступа:

1. https://www.securitylab.ru/blog/personal/aguryanov/30007.php/(дата обра-щения: 21.02.2020).