Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

Студент: Мамаева Д. А.

ФИТ 2 курс 6 группа

Преподаватель: Берников В. О.

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

# Введение

Потоки информации, циркулирующие в окружающем нас мире, огромны. В этих потоках имеются документы, содержащие самую разнообразную информацию. Поэтому без решения задач информационной безопасности не может продолжать работу ни одно из предприятий. В любой организации, как большой, так и маленькой, возникает проблема безопасного хранения, передачи, использования информации.

Целью обеспечения информационной безопасности автоматизированной системы управления технологическими процессами является повышение уровня устойчивости ее функционирования, стабильности исполнения реализуемых технологических процессов путем предотвращения и/или снижения возможного ущерба от несанкционированных воздействий на объекты защиты автоматизированной системы управления технологическими процессами.

Цель: разработать проект политики информационной безопасности бизнес-компании.

Задание для выполнения:

Разработать проект политики информационной безопасности бизнес-компании, оформив результаты в виде пояснительной записки. Пояснительная записка может, например, содержать следующие разделы:

1. Титульный лист;
2. Введение (обосновывается важность разработки политики информационной безопасности);
3. Описание структуры бизнес-компании (выбор компании предварительно согласовывается с преподавателем);
4. Оценка рисков;
5. Разработка мер защиты;
6. Выводы.

Электронный вариант вносится в электронную тетрадь и показывается преподавателю для предварительной проверки (объем – 10-20 страниц).

После предварительной проверки пояснительная записка распечатывается и проект политики информационной безопасности бизнес-компании защищается в указанные преподавателем сроки.

Вариант 13. Маркетинговое агентство

# 1.Общее положение.

Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

* управление доступом к средствам вычислительной техники, программа и данным;
* антивирусную защиту;
* вопросы резервного копирования;
* проведение ремонтных и восстановительных работ;
* информирование об инцидентах об области ИБ.

Определение уровней рисков и типов доступа, требуемых для каждой сети, позволяет сформировать некоторую матрицу безопасности. Эта матрица безопасности является стартовой точкой для дальнейших шагов по обеспечению безопасности, например, таких, как создание соответствующей стратегии по ограничению доступа к сетевым ресурсам.

Изменения конфигурации средств обработки и хранения информации, а также изменения сетевой инфраструктуры, конфигурации сетевого оборудования выполняются администратором. Все изменения регистрируются в соответствующих журналах. Самостоятельное изменение конфигурации средств обработки, хранения и передачи информации пользователями АСУ ТП запрещено. Использование съемных носителей информации в автоматизированной системе управления технологическими процессами запрещено. При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

В данной работе приведены термины и сокращения:

– АРМ – автоматизированное рабочее место;

– АСУ ТП – автоматизированная система управления технологическими процессами;

– ИБ – информационная безопасность;

– ИУС ПХД – информационно-управляющая система производственно-хозяйственной деятельности;

– ЛВС – локальная вычислительная сеть;

– ОС – операционная система;

– ПО – программное обеспечение;

– СУБД – система управления базами данных;

– ТЗ – техническое задание.

Под автоматизированной системой управления технологическими процессами понимается система, состоящая из персонала и комплекса средств автоматизации его деятельности и формирующая управляющее воздействие на технологические процессы.

Комплекс средств автоматизации включает:

– системы диспетчерского управления (АРМ пользователей и серверы, на которых установлено системное и прикладное ПО, а также набор сетевого оборудования для организации ЛВС и средств ее защиты (средства межсетевого экранирования, средства обнаружения и предотвращения вторжений));

– системы локальной автоматики (системы автоматического управления, концентраторы, контроллеры, пункты управления технологическими объектами, устройства сопряжения с объектами).

Объектами защиты автоматизированной системы управления технологическими процессами являются:

– серверное оборудование (архивные, коммуникационные и другие серверы);

– системы локальной автоматики (системы автоматического управления, концентраторы, контроллеры, пункты управления технологическими объектами);

– АРМ операторов и специалистов;

– сетевое оборудование (коммутаторы, маршрутизаторы, фронтальные процессоры, интегрирующие контроллеры, контроллеры связи с объектами);

– каналы передачи данных;

– ПО;

– технологическая информация (в том числе сигналы, команды управления, данные о параметрах (состоянии) управляемого технологического объекта (процесса)).

# 2. Структура концепции защиты

Основными разделами концепции безопасности являются:

* определение ИБ;
* структура безопасности;
* описание механизма контроля над безопасностью;
* оценка риска;
* безопасность информации: принципы и стандарты;
* обязанности и ответственность каждого отдела, управления или департамента в осуществлении защиты информационных носителей и прочих данных;
* ссылки на иные нормативы о безопасности.

Помимо этого не лишним будет раздел, описывающий основные критерии эффективности в сфере защиты важной информации. Индикаторы эффективности защиты необходимы, прежде всего, топ-менеджменту. Они позволяют объективно оценить организацию безопасности, не углубляясь в технические нюансы. Ответственному за организацию безопасности также необходимо знать четкие критерии оценки эффективности ИБ, дабы понимать, каким образом руководство будет оценивать его работу.

Политику безопасности надо формулировать с учетом двух основных аспектов:

1. Целевая аудитория, на которую рассчитана вся информация по безопасности – руководители среднего звена и рядовые сотрудники не владеют специфической технической терминологией, но должны при ознакомлении с инструкциями понять и усвоить предоставляемую информацию.
2. Инструкция должна быть лаконичной и при этом содержать всю необходимую информацию о проводимой политике. Объемный «фолиант» никто подробно изучать не будет, а тем более запоминать.

Из выше перечисленного вытекают и два требования к методическим материалам по безопасности:

* они должны быть составлены простым русским языком, без использования специальных технических терминов;
* текст по безопасности должен содержать цели, пути их достижения с указанием назначения меры ответственности за несоблюдение ИБ.

Все! Никакой технической или иной специфической информации.

В заключение мы классифицируем тех, кто может или хочет получить несанкционированный доступ к информации.

Потенциальные внешние нарушители:

1. Посетители офиса.
2. Ранее уволенные сотрудники (особенно те, кто ушел со скандалом и знает, как получить доступ к информации).
3. Хакеры.
4. Сторонние структуры, в том числе конкуренты, а также криминальные группировки.

Потенциальные внутренние нарушители:

1. Пользователи компьютерной техники из числа сотрудников.
2. Программисты, системные администраторы.
3. Технический персонал.

Для организации надежной защиты информации от каждой из

перечисленных групп требуются свои правила. Если посетитель может просто забрать с собой какой-то листок с важными данными, то человек из техперсонала – создать незарегистрированную точку входа и выхода из ЛВС. Каждый из случаев – утечка информации. В первом случае достаточно выработать правила поведения персонала в офисе, во втором – прибегнуть к техническим средствам, повышающим информационную безопасность, таким как DLP-системы и SIEM-системы, предотвращающие утечки из компьютерных сетей.

При разработке ИБ надо учитывать специфику перечисленных групп и предусмотреть действенные меры предотвращения утечки информации для каждой из них.

Антивирусы:

Компьютерные вирусы остаются в настоящее время наиболее актуальной проблемой информационной безопасности корпоративных систем.

В связи с тем, что подавляющее большинство вредоносных программ распространяется посредством электронной почты, межсетевые экраны оказываются неэффективными. В арсенале решений этого типа нет средств анализа принимаемых почтовых сообщений.

Одним из методов, применяемых системными администраторами наряду с использованием антивирусного программного обеспечения, является фильтрация сообщений, содержащих вложения определенных форматов (чаще всего, исполняемые приложения).

Современные антивирусные программы, при всем их разнообразии, используют лишь два принципиально разных метода обнаружения вредоносных программ:

· Поиск по сигнатурам

· Эвристический анализ

# 3.Оценка рисков

Деятельность любой современной компании невозможно представить без активного использования информации и информационных технологий. Информация стала одним из важнейших активов, находящихся в распоряжении компаний. Все это порождает новый, принципиально отличающийся от привычных финансовых, юридических и других класс рисков для деятельности организаций – рисков нарушения информационной безопасности. А если есть риски – ими надо управлять. Такой подход заложен в основу современных международных и отечественных стандартов в области обеспечения ИБ.

Начать, пожалуй, следует с выбора методики, по которой будет проводиться оценка рисков. На сегодняшний день недостатка в таких методиках оценки рисков нарушения информационной безопасности нет. Это, к примеру, OCTAVE, CRAMM, RA2, отраслевая методика Банка России РС БР ИББС 2.2 – вот лишь немногие из них. Методики можно разделить на качественные и количественные, в зависимости от шкал, применяемых для оценки вероятности реализации угрозы и тяжести последствий от её реализации. Кроме того, отличия методик заложены в подходах (базовый уровень или детальная оценка рисков) и процедурах оценки рисков. Для некоторых методик разработаны инструментальные средства, содержащие базу знаний по рискам и механизмы их минимизации. Независимо от выбранной методики, процесс управления рисками ИБ будет включать в себя выполнение следующих задач: определение области оценки рисков; оценка рисков; обработка рисков; мониторинг и контроль; совершенствование процесса. Также перед началом работ по оценке рисков необходимо создать организационную структуру по управлению рисками, и разработать Политику управления рисками ИБ. В ней должны быть отражены такие вопросы, как цели и процессы управления рисками (в соответствии с выбранной методологией), критерии управления рисками (включая критерии оценки ущерба, оценки рисков и принятия рисков), функциональные роли по оценке рисков.

В область оценки рисков могут входить бизнес-процессы, элементы инфраструктуры, информационные активы, сервисы, персонал и т.д. На практике для организаций, которые впервые проводят оценку рисков, целесообразно ограничить область оценки, например, одним из вспомогательных бизнес-процессов или даже конкретным информационным активом. Иначе говоря, выполнить пилотный проект. Такое ограничение позволит «обкатать» и, при необходимости, доработать применяемую методику, довести до ума шаблоны документов, а также практически безболезненно наступить на все остальные грабли, разбросанные на пути внедрения системы управления рисками ИБ. Впоследствии область оценки рисков должна охватить всю организацию в целом (по крайней мере, ту её часть, на которую распространяется действие системы управления информационной безопасностью - СУИБ).

На этапе оценки рисков мы должны идентифицировать информационные активы, входящие в область оценки; определить ценность этих активов; определить перечень угроз и вероятность их реализации; произвести оценивание и ранжирование рисков. Начнем с идентификации информационных активов. Информационный актив – это любая информация, независимо от вида её представления, имеющая ценность для организации и находящаяся в её распоряжении. У каждой организации свой набор активов, относящихся к тому или иному типу, например: персональные данные; стратегическая информация, необходимая для достижения бизнес-целей; ноухау; коммерческая тайна; служебная тайна и т.д. Для каждого актива необходимо определить владельца, который несет за него ответственность.

Стоит заметить, что на данном этапе большим подспорьем может служить документированное описание бизнес-процессов организации. Это позволит нам быстро идентифицировать информационные активы, вовлеченные в конкретный бизнес-процесс, а также определить задействованный в нем персонал. Если же бизнес-процессы в организации не документированы, то самое время начать это делать. Помимо практической пользы при внедрении системы управления рисками ИБ и СУИБ, перенос бизнес-процессов «на бумагу» часто помогает увидеть возможности по их оптимизации.

Определение ценности активов, а точнее, оценка степени тяжести последствий (СТП) от утраты активом свойств информационной безопасности - конфиденциальности, целостности или доступности - необходима нам для того, чтобы ответить на следующие вопросы: Сколько нам будет стоить «простой» системы в течение времени, требующегося на её восстановление? Каков будет ущерб, если эта информация станет известной конкурентам?

В рамках пилотного проекта по созданию системы управления рисками ИБ наиболее целесообразной является качественная оценка ценности информационного актива со стороны владельца. При этом, в зависимости от потребностей организации, её размера или иных факторов, качественная шкала оценки может использовать такие слова, как «незначительный», «низкий», «средний», «высокий», «критический», под которыми подразумевается определенный интервал количественной шкалы оценки. Например, «незначительный» - менее 10 тыс. рублей, «низкий» - от 10 до 100 тыс. рублей и т.д.

Впрочем, существуют специальные методики, используемые оценочными компаниями для количественной оценки стоимости нематериальных активов на основе рыночного, доходного или затратного подходов. Однако их применение часто требует привлечения профессиональных оценщиков, так как в подавляющем большинстве случаев специалисты подразделений ИБ не обладают подобными знаниями.

Опять же, в рамках пилотного проекта имеет смысл анализировать только высокоуровневые риски, постепенно повышая детализацию и глубину анализа в последующих оценках. Этим принципом мы будем руководствоваться при составлении перечня угроз, если в организации нет утвержденной Модели угроз, которую можно взять за основу. Угрозы могут иметь природное или техногенное происхождение, могут быть случайными или преднамеренными. Типовые перечни угроз приведены в приложениях к стандартам ISO 27005, BS 7799-3 и РС БР ИББС 2.2. Для определения степени вероятности реализации (СВР) той или иной угрозы на данном этапе можно воспользоваться качественной экспертной оценкой.

Переход на количественные шкалы, безусловно, позволяет сделать результаты оценки рисков более точными, однако предполагает наличие некоего уровня зрелости существующих процессов управления ИБ и оценки рисков и не всегда оправдан. Тем не менее, если в организации существует функционирующая система менеджмента инцидентов, фиксируются данные о частоте реализации той или иной угрозы, то грех не воспользоваться подобной информацией.

Оценивание риска, в общем случае, происходит путем сопоставления оценок СТП с оценкой СВР угроз ИБ (иногда к ним добавляется оценка уязвимостей).

По результатам оценки рисков необходимо определить способ обработки для каждого из рисков, который является недопустимым. Возможными вариантами обработки рисков являются:

* применение защитных мер, позволяющих снизить величину риска до допустимого уровня;
* уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);
* перенос риска на другие организации (например, путем страхования или передачи деятельности на аутсорсинг);
* осознанное принятие риска.

Следует помнить, что любой деятельности свойственны риски, и понизить их можно лишь до определенного остаточного уровня, а не до нуля.

Решение о применении того или иного способа обработки рисков должно приниматься исходя из стоимости их реализации, а также ожидаемых выгод от их реализации. Ведь наша цель, во-первых, добиться значительного уменьшения рисков при относительно низких затратах и, во-вторых, поддерживать принятые риски на допустимом, низком уровне.

Руководствоваться при выборе защиты лучше принципом разумной достаточности. Меры безопасности не могут быть более затратными, чем потенциальный ущерб от нарушения ИБ.

После принятия решений об обработке рисков необходимо осуществлять постоянный мониторинг и контроль СУИБ. Это позволит нам оценить эффективность защитных мер, которые мы использовали для понижения величины риска.

На данном этапе также осуществляется контроль изменения перечня активов, угроз и других факторов, влияющих на результаты оценки, проводятся аудиты и иные контрольные процедуры.

Совершенствование процессов управления рисками ИБ осуществляется по результатам, полученным в процессе мониторинга и контроля. При необходимости пересматривается Политика управления рисками ИБ, область оценки, состав угроз ИБ, оценки СВР и СТП, совершенствуется методология и т.д.

Крайне желательно интегрировать процессы управления рисками в общий процесс управления информационной безопасностью. Это позволить привязать циклы деятельности по оценке рисков к общепринятому циклу выполнения деятельности по обеспечению ИБ, основанному на модели Деминга «… — планирование — реализация — проверка — совершенствование— планирование — …”, которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ИБ ISO 27001-2005.

Внедрение системы управления рисками ИБ может быть нетривиальной задачей для многих организаций, только начинающих работу над созданием системы управления информационной безопасностью. Однако оно является отправной точкой для построения эффективной системы защиты, которая будет отвечать бизнес-целям организации. В этом случае для проведения пилотного проекта может быть оправданным приглашение внешних консультантов, которые попутно разработают необходимую организационно-распорядительную документацию, адаптируют методологию и проведут обучение сотрудников организации.

Управление информационными рисками и построение комплексной системы управления информационной безопасностью – это для каждой организации шаг на качественно иной уровень корпоративного управления, а в некоторых случаях – решающее конкурентное преимущество.

# Разработка мер защиты

Методами обеспечения защиты информации являются следующие: препятствие, управление доступом, маскировка, регламентация, принуждение и побуждение.

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

Управление доступом — метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы организации (фирмы).

Управление доступом включает следующие функции защиты:

* идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);
* аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
* проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
* разрешение и создание условий работы в пределах установленного регламента;
* регистрацию (протоколирование) обращений к защищаемым ресурсам;
* реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Критерии и показатели информационной безопасности маркетингового агентства:

* конфиденциальность — доступность информации только определённому кругу лиц;
* целостность — гарантия существования информации в исходном виде;
* доступность — возможность получения информации авторизованным пользователем в нужное для него время;
* аутентичность — возможность установления автора информации;
* апеллируемость — возможность доказать, что автором является именно заявленный человек, и никто другой.

Планирование мероприятий по обеспечению информационной безопасности агентства. Построение системы защиты может выполняться в несколько этапов:

* собираются сведения о существующих информационных системах персональных сведений;
* моделируются угрозы безопасности;
* разрабатываются технические задания;
* проектируется система защиты информации;
* разрабатывается организационно-распорядительная документация, которая регламентирует процессы обработки и защиты сведений;
* поставляются, устанавливаются и настраиваются средства защиты информации;
* проводится аттестация информационных систем сведений, согласно требованиям безопасности.

К наиболее важным мерам обеспечения информационной безопасности также принято относить:

* криптографическая защита;
* выявление кибератак и формирование нескольких уровней защиты от них;
* разграничение доступа к системам с защищаемой информацией;
* использования для защиты инфосистемы межсетевых экранов;
* использование лицензионного антивирусного ПО;
* резервное копирование информации и приложения;
* обеспечение защиты от утечек информации;
* протоколирование, аудит;
* защита данных, которые передаются по проводным и беспроводным сетям.

Методами и способами защиты информации от несанкционированного доступа являются:

* реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
* ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также, хранятся носители информации;
* разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
* регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
* учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
* резервирование технических средств, дублирование массивов и носителей информации;
* использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
* использование защищенных каналов связи;
* размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
* организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
* предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

# Вывод

Политика безопасности – совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На политике безопасности нельзя экономить, так как данные, которые могут быть подвержены хищению, копированию или изменению, могут стоить дороже, чем ресурсы, потраченные на её разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность, общие меры предосторожностей, так же такие пункты как люди, и процессы, и избыточность, и непрерывность работы.

Меры по обеспечению информационной безопасности на предприятии должны разрабатываться и реализовываться постоянно, независимо от роли IT-инфраструктуры в производственных процессах.

К решению этого вопроса необходимо подходить комплексно и с привлечением сторонних специалистов. Только такой подход позволит предотвратить утечку данных, а не бороться с ее последствиями.