Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №2**

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

Выполнила:

Студентка 2 курса 1 группы ФИТ

Быско Елизаветы

Цель: разработать проект политики информационной безопасности бизнес-компании.

**Введение**

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

**Политика безопасности** организации образует совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области **безопасности**, которые регулируют управление, защиту и распределение ценной информации. Кроме этого в политику безопасности входят требования в адрес субъектов информационных отношений и излагается политика ролей субъектов информационных отношений

Из-за возможности утечки информации или неосторожного поведения сотрудников компания теряет свою конкурентоспособность на рынке. Благодаря разработке различных систем защиты это можно минимизировать или вовсе избежать. При разработке системы защиты необходимо опираться на различные стандарты, которые позволят взаимодействовать с разными государственными органами в соответствующем правовом поле, а также успешно сотрудничать с зарубежными партнёрами.

Основная задача политики безопасности — это задокументировать правила работы на предприятии в области информационной безопасности. Без нее взаимодействие работников с различными ресурсами будет регулироваться лишь неформально и поэтому возрастет риск нарушений и утечек данных. Поэтому минимизация рисков компании приведёт к повышению её прибыльности.

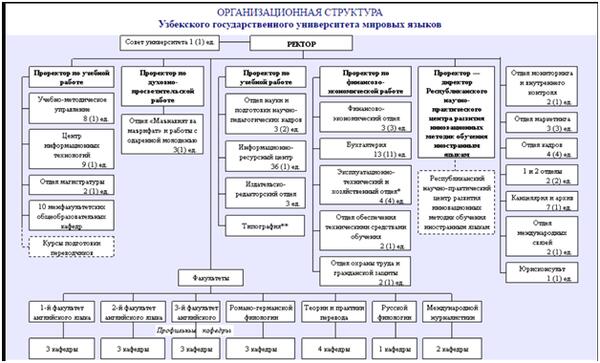
**Описание структуры компании**

**Организационная структура компании** — это, по сути, руководство для пользования, которое объясняет, как организация выстроена и как она работает. Если говорить конкретнее, то организационная структура описывает, как в компании принимаются решения и кто является ее лидером.

**Почему необходимо разрабатывать организационную структуру предприятия?**

* Организационная структура дает четкое понимание того, в каком направлении движется компания. Ясная структура — это инструмент, с помощью которого можно придерживаться порядка в принятии решений и преодолевать различные разногласия.
* Организационная структура связывает участников. Благодаря ей люди, присоединяющиеся к группе, имеют отличительные черты. В то же время и сама группа обладает определенными особенностями.
* Организационная структура формируется неизбежно. Любая организация по определению подразумевает какую-то структуру.

Организационная структура университета.



Основные положения, которые положены в основу информационной системы управления ВУЗом:

1. Наличие единой корпоративной сетевой инфраструктуры и единого центра управления разработками, обеспечивающих разработку информационных подсистем, которые направлены на автоматизацию задач, стоящих перед ВУЗом;
2. Разработка системы, включающей доступ ко всем информационным ресурсам ВУЗа;
3. Управление учебным процессом с помощью информационных ресурсов;
4. Управление персоналом;
5. Поддержка всех основных процессов сферы деятельности ВУЗа и поднятие их качества на новый уровень;
6. Использование современных технологий для разработки, управления и сопровождения всех используемых ВУЗом сетевых ресурсов, а также корректное их использование, редактирование и заполнение;
7. Поддержка информационных ресурсов для комфортной работы персонала и студентов;
8. Управление документооборотом;
9. Выделение достаточного количества ресурсов для корректной работы всей сети ВУЗа;

Информационная системы ВУЗа позволяет собирать, анализировать и систематизировать данные о приёме абитуриентов: количество абитуриентов, количество баллов, специальность на которую поступает абитуриент, топ абитуриентов по количеству баллов и так далее. Некоторые функции программы единой информационной системы ВУЗа позволяют отслеживать успеваемость студентов, количество пропусков по уважительной и неуважительной причине, также ведётся табель с оценками. Эта область соприкасается с большинством участников образовательного процесса.

Возможности информационный системы ВУЗа позволяют чётко представить структурную организацию отдельных подразделений и всего ВУЗа в целом. Это помогает грамотно и своевременно готовить приказы о приёме на работу, начислению заработной платы и т.д.

Также с информационной системой вуза пересекаются информационные ресурсы, электронные образовательные ресурсы, различные технологические средства, всё это и не только обеспечивает освоение обучающимися образовательных программ в полном объёме и позволяет обучаться студентам вне зависимости от места нахождения.

**Основные угрозы и их источники**

Способы нанесения вреда информационным системам модифицируются и усложняются с каждым годом. Всё чаще используются специально написанные программы, эксплуатируются скрытые угрозы, а традиционные методы атак всё чаще исправляются при разработке программ и в итоге не используются для эксплуатации. Все этим угрозы проникают внутрь сети — на уровень ядра, уровень доступа пользователей, где защита от угроз может находиться на минимальном уровне. С этой позиции угрозы без проблем могут перейти на новый уровень и в итоге добираются до своей цели — конкретные ресурсы в сети или информация. Цель современных кибер-угроз чаще всего заключается в захвате ценной информации и дальнейшей её эксплуатации или продаже, также целью может быть шантаж или вымогательство.

Угрозы безопасности могут быть классифицированы по следующим признакам:

1. По природе возникновения(искусственные и естественные);
2. По степени преднамеренности (случайные и преднамеренные);
3. По аспекту информационной безопасности;
4. По компонентам, на которые нацелена угроза;

Для информационной системы университета существуют следующие угрозы:

1. Несанкционированный доступ к персональным данным учеников, преподавательского состава, различным программам, а также ценным документам и бумагам;
2. Распространение нежелательного контента с использованием информационных ресурсов ВУЗа, также распространение личной информации по причине несанкционированного доступа к ресурсам внутренней сети ВУЗа;
3. Кибертерроризм, новая форма терроризма. Создание безопасной информационной технологической среды существенно снизит риск кибератаки на объекты образования, что поможет сохранить функционирование системы и последующее её восстановление;
4. Зачастую администрация университета хранит на своих компьютерах персональную информацию о преподавателях, студентах, различные приказы и иные ценные документы. Вся эта информация должна подлежать соответствующей защите от несанкционированного доступа к ней;
5. Один из возможных вариантов атаки это физический. Достаточно просто подойти к одному из компьютеров, стоящих в университете, подобрать пароль для учётной записи и скопировать все необходимые данные на переносной носитель не оставляя следов;
6. Очередная проблемы состоит в пренебрежении безопасностью. Например, чтобы пораньше уйти в работы кто-то из персонала может скопировать необходимые данные на флешку или другой переносной носитель, а после уже выполнять необходимые действия дома на своём личном компьютере. Также возможен обычный перенос необходимых данных через один из почтовых сервисов.

Основные объекты, которые нуждаются в особой защите от несанкционированного доступа:

1. Бухгалтеркие локальные сети;
2. Данные финансового отдела;
3. Сервера с базами данных;
4. FTP сервера;
5. Компьютеры, на которых храниться очень важная информация (обычно это компьютеры в кабинетах деканата и т.д.)

**Оценка рисков**

Компьютерные сети ВУЗов — совокупность сетевых ресурсов, используемых для учебной деятельности, работы персонала и устройств, благодаря которым сеть функционирует в принципе.

Источниками угроз в первую очередь могут стать учебные аудитории с беспрепятственным доступом в локальную или глобальную сеть Интернет, также источников угроз может стать лаборатория, оснащённая компьютерами с доступом в Интернет. Особую опасность представляют работники, которые халатно относятся к информационной безопасности и при этом имеют доступ к важным документам или могут косвенно повлиять на утечку данных в сети.

Анализ информационных рисков можно разделить на следующие этапы:

1. Классификация объектов, которые необходимо защитить, по важности;
2. Определение основных векторов атак, а также пути для возможного восстановления сети в случае её отказа;
3. Оценка уже существующих методов защиты, а также их модификация для корректной работы в случае попытки несанкционированного доступа;
4. Определение существующих или потенциальных уязвимостей, а также поиск способов для их ликвидации;
5. Оценка ущерба при удачной и неудачной попытке несанкционированного доступа к сети;
6. Возможность вывода оборудования из строя, а также возможность сбоев при различных случайных и непредвиденных ситуациях;

Базовый (*baseline*) анализ рисков – анализ рисков, проводимый в соответствии с требованиями базового уровня защищенности. Прикладные методы анализа рисков, ориентированные на данный уровень, обычно не рассматривают ценность ресурсов и не оценивают эффективность контрмер. Методы данного класса применяются в случаях, когда к информационной системе не предъявляется повышенных требований в области ИБ.

Полный (*full*) анализ рисков – анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ. Включает в себя определение ценности информационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности

При анализе рисков, ожидаемый ущерб в случае реализации угроз, сравнивается с затратами на меры и средства защиты, после этого принимается решение в отношении оцениваемого риска и принимается один из следующих возможных вариантов:

1. Снижен, например, за счёт внедрения средств и механизмов защиты, которые уменьшат вероятность реализации угрозы ли количество полученной информации злоумышленнику;
2. Устранён за счёт отказа от использования устройства, которое подвержено данной угрозе;
3. Перенесён, например, застрахован, в результате в случае реализации угрозы безопасности, потери будет нести страховая компания, а не владелец ресурса;
4. Принят;

**Разработка мер защиты и мероприятий по внедрению политики безопасности**

Борьба с различными видами атак должна вестись на пяти уровнях, при этом защита должна нести комплексный характер. Сейчас существует большое количество различных разработок, которые помогут построить защиту ВУЗа на необходимом уровне.

1. Внедрение антивирусного программного обеспечения

Благодаря данному программному обеспечению будет возможна базовая защита от большинства вирусов, из-за которых злоумышленник может получить несанкционированный доступ к внутренней информации.

1. Поведенческая аналитика пользователей (UBA)

UBA собирает информацию о действиях пользователей и соотносят их поведение с базовым уровнем. Затем решения используют этот базовый уровень в качестве сравнения с новыми моделями поведения для выявления несоответствий. Затем решение помечает эти несоответствия как потенциальные угрозы.

1. Система обнаружения вторжений (IDS) и cистема предотвращения вторжений (IPS), а также firewall

IDS– это инструменты для мониторинга входящего трафика и обнаружения угроз. IPS –реагирует на трафик, который идентифицируется как подозрительный или вредоносный, блокируя запросы или завершая сеансы пользователя. Firewall поможет фильтровать трафик и передавать данные о трафике в системы мониторинга и обнаружения.

1. Морально-этические средства обеспечения информационной безопасности;

В образовательной сфере морально-этические ценности играют большую роль. Именно поэтому на ней должна основываться система мер, защищающих студента от травмирующей, незаконной и этически некорректной информации. Для защиты необходимо применять нормы закона «О защите прав ребёнка», которые определяют его права на защиту сведений, которые могут причинить ему моральную травму. Поэтому одона из основ информационной безопасности должно стать недопущение проникновения источников, которые содержат травмирующую психику ученика информацию.

1. Административно-организационные меры

Эти меры построены на создании внутренних правил и регламентов, которые определяют порядок работы с информацией и её носителями, Это внутренние методики, посвящённые информационной безопасности, инструкции, перечни сведений, которые не подлежат передаче.

Также необходимо дополнительно разработать регламент, который будет определять порядок взаимодействия с компетентными органами по запросам о предоставлении им необходимых документов, отчётов или информации.

Все методики должны определять порядок доступа студентов к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов спорного характера и запрет на использование собственных носителей информации.

1. Физические меры

За данную систему должно отвечать руководство ВУЗа и сотрудники IT-подразделений данного ВУЗа. Среди физических мер кроме невозможности копирования или отправки различной информации и документов по сети, должна быть предусмотрена пропускная система защиты помещения, организация контроля доступа посетителей, установлены различные степени допуска. Обязательно установление паролей, а также их регулярная замена.

1. Технические меры

Комплексную систему защиты всей компьютерной сети должны обеспечивать специальное программное обеспечение, которое может выявить все возможные угрозы безопасности и меры, которые необходимо предпринять по борьбе с ними. Также необходимо использовать антивирусы.

Электронная почта, к которой имеют доступ сотрудники ВУЗа и студенты, должна контролироваться. Также имеет смысл установить специальное программное обеспечение, которое запрещает копирование информации с жёстких дисков компьютеров.

Кроме всего этого необходимо установить программное обеспечение, которое ограничит доступ к сайтам с нежелательным содержанием.

Все меры обеспечения информации должны использоваться комплексно и контролироваться несколькими людьми, которые будут следить за корректной работой защиты.

Некоторые университеты используют свои сервера для выхода в Интернет, благодаря чему есть возможность блокировки сайтов с нежелательным содержанием или вовсе избежать доступа к сети посторонним лицам. Также сотрудники учебного заведения не должны разглашать внутреннюю информацию третьим лицам.

Степень защищённости ВУЗов в Республике Беларуси считается чуть ниже среднего. Основные причины из-за которых уровень безопасности считается таковым: во-первых, плохая организация мер по разработке и обеспечению политики информационной безопасности, а также недооценке важности информационной безопасности, во-вторых, недостаточное финансирование этой области, в следствие чего невозможна закупка и внедрение новых технологий, которые помогут минимизировать утечки информации.

**Вывод**

Информационная безопасность является одной из проблем, с которой столкнулось современное общество. Основная проблема в информационной безопасности заключается в нахождении различных уязвимостей ежедневно. Также не всегда есть возможность не жертвовать частью информации для сохранения какой-то более важной части. Кроме этого злоумышленнику достаточно быть правым лишь один раз, а специалисту по защите нужно быть правым всегда.

Каждый раз при построении системы защиты информации нужно определять, что нужно защищать и от чего. Кроме всего этого следует защищаться не от одной конкретной угрозы, а от целого множества угроз, при этом учитывая различные факторы, которые могут присутствовать при защите информации сети или информации от злоумышленника.

Одни из обязательных этапов является проектирование системы защиты. Для корректного проектирования необходимо поставить себя на место злоумышленника для понятия того, как может действовать злоумышленник, а также какие способы несанкционированного доступа могут быть ему доступны в данном объекте или сети. Также можно попытаться самостоятельно защитить свой объект хотя бы от базовых атак, а после переходить к более узким атакам. Или провести стресс тест для оборудования, однако данные манипуляции необходимо выполнять когда все предупреждены, иначе есть возможность из-за данного теста потеря важных документов или вовсе сбой всего оборудования по различным причинам. Кроме всего перед началом проверки следует сделать резервное копирование всей необходимой информации.

Для предупреждения успешных атак необходим постоянный поиск и анализ уязвимостей системы. Благодаря анализу уязвимостей можно обеспечить грамотную защиту необходимого ресурса. Благодаря периодическому анализу уже защищённых объектов, можно обнаружить некоторые бреши в защите или просто удостовериться в работе старых.