Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Основы информационной безопасности»

Отчёт по практическому занятию №2

Студент: Арцыхович П.А.

ФИТ 2 курс 2 группа

Преподаватель: Ржеутская Н.В.

Минск 2022 г.

**Практическое занятие №2**

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

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.

|  |  |
| --- | --- |
| 1. | Университет |

# **Введение**

* **Информационная безопасность компании**, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных.

В информационную безопасность входит защита от злоумышленников данных в электронной форме и на физических носителях.

Учитывая важность информации в современном мире, защите от утечек конфиденциальной информации в адрес конкурентов необходимо уделять повышенное внимание. Возможный ущерб может быть намного большим, чем стоимость всех материальных активов предприятия.

Безопасность информационной инфраструктуры компании подразумевает защиту от случайных или умышленных действий, которые могут нанести вред владельцам данных или их пользователям. Действия лиц, несущих ответственность за эту сферу, должны быть направлены на создание защиты, препятствующей утечкам данных, а не борьбу с их последствиями. Но при этом важно сохранять простой доступ к информации тем людям, которые на законных основаниях пользуются базами данных.

Проблема сохранности конфиденциальной информации и коммерческой тайны существовала и ранее. Но по мере развития электронных средств обработки и хранения данных повышается вероятность их утечки и незаконного копирования. Если ранее для кражи чертежей нового продукта нужно было физически вынести их с завода, сейчас достаточно получить доступ к серверу через электронные каналы связи или записать их на миниатюрную карту памяти.

В большинстве случаев краже подлежат следующие данные:

* Информация о реальном финансовом состоянии компании;
* Инновационные разработки научно-технических отделов;
* Регистрационные данные для доступа к защищенным серверам;
* Персональные данные работников.

Дополнительной сложностью является то, что кража информации может негативно отразиться на компании не сразу после ее совершения, а по прошествии определенного времени. Неважные на первый взгляд данные при их обнародовании могут нанести репутационный вред компании и уменьшить ее рыночную стоимость.

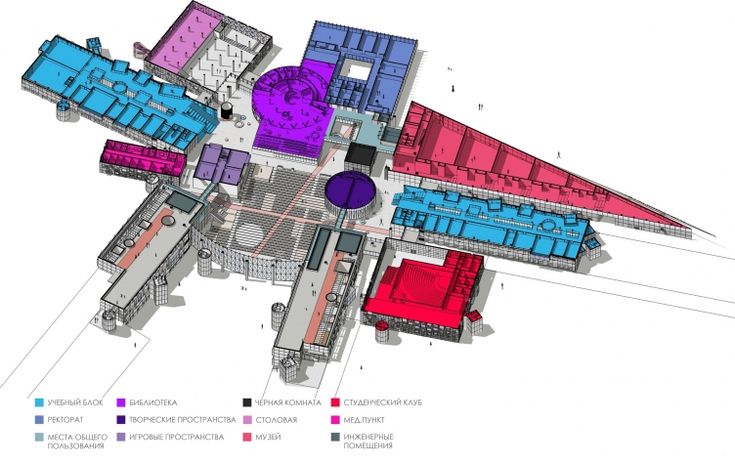
Поэтому при разработке мер по обеспечению информационной безопасности нельзя делить данные на виды. Все, что размещено в IT-инфраструктуре компании и храниться в архивах, не должно выходить за ее пределы.

# **Описание структуры Университета**

* **Структура развития университета** – это определенная совокупность компонентов для достижения целей образования, удовлетворения запросов потребителей и получения запланированного образования.

Элементами структуры университета являются:

* **Образование**. Образование определяет, что производить или предлагать, какими должны быть объем и качество этого предложения, а также условия реализации товара.
* **Ценообразование**. Выбирается уровень цен, определяется система скидок и соотношение цены и качества обучения.
* **Продвижение**. Определяются способы влияния на объем поступлений, рекламная и PR-стратегия, способы оценки их эффективности.



* **Организационная структура университета** – это совокупность отделов и подразделений здания, занимающихся разнообразной деятельностью в университете.

На выбор типа организационной структуры маркетинговой службы влияет ряд факторов:

1. Вид деятельности предприятия.
2. Цель, которую оно перед собой ставит.
3. Объем производства и номенклатуры.
4. Территориальная удаленность от конечного потребителя.
5. Система образования.
6. Другие внешние и внутренние условия.

# **Оценка рисков**

Проблемы информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

**Виды угроз информационной безопасности предприятия**

Существует несколько причин, по которым становится возможным незаконный доступ до конфиденциальной информации злоумышленниками. Среди них особенно опасными являются следующие:

1. **Халатное отношение сотрудников компании к защите цифровых данных.**

Основные причины нарушения безопасности со стороны сотрудников:

* *Переход по фишинговой ссылке с рабочего компьютера и заражение вредоносной программой корпоративной сети;*
* *Хранение конфиденциальных данных на сменных носителях информации;*
* *Пересылка информации с секретными данными по обычной электронной почте или через незащищенный мессенджер.*

1. **Использование нелицензионных программ**

Коммерческие компании часто экономят средства на приобретении ПО и позволяют сотрудникам пользоваться пиратскими версиями офисных приложений и профессиональных программ. Однако при этом возникает опасность внедрения в сеть вирусов и других вредоносных программ.

Кроме того, использование пиратского ПО влечет за собой дополнительные минусы:

* *Отсутствие периодических обновлений, которые «латают дыры» в системе защиты;*
* *Отсутствие технической поддержки со стороны разработчиков;*
* *Невозможность проверки подлинности кода приложения.*

1. **Работа вредоносных программ**

Компьютерные вирусы – распространенная угроза безопасности IT-инфраструктуры компании. Ущерб, нанесенный вредоносными программами, исчисляется миллионами долларов. В последние 3-5 лет наблюдается увеличения числа вредоносных программ и атак с их стороны, а также сумм понесенных компаниями потерь.

Дополнительная опасность в том, что помимо компьютеров пользователей и серверов, сейчас заражению подвергаются и другие элементы сетевой инфраструктуры:

* *Коммутаторы и маршрутизаторы;*
* *Мобильные устройства для доступа в сеть – компьютеры, планшеты;*
* *Элементы «умного дома».*

Наибольший ущерб причиняют вирусы, которые шифруют данные на компьютере пользователя и требуют от него денежного перевода за расшифровку. Примерами таких вредоносных утилит являются WannaCry, Petya.

1. **Действия правоохранительных органов**

В ходе расследования уголовных дел и при проведении некоторых видов проверок представители контролирующих и правоохранительных органов могут изымать компьютерную технику и документы, в том числе с конфиденциальной информацией.

Это приводит сразу к двум негативным последствиям:

* *Из-за изъятия компьютеров и серверного оборудования деятельность компании может полностью прекратиться;*
* *Информация с изъятых носителей и документов может распространиться далее, несмотря на ответственность работников следствия.*

Ущерб, причиняемый утечкой информации, невозможно спрогнозировать заранее. Он может выражаться в незначительной сумме, но в некоторых случаях приводит к полной неспособности компании заниматься хозяйственной деятельностью.

В большинстве случаев краже подлежат следующие данные:

* Информация о реальном финансовом состоянии компании;
* Инновационные разработки научно-технических отделов;
* Регистрационные данные для доступа к защищенным серверам;
* Персональные данные работников.

# **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.*

**Основные меры 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.