МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

«БЕЛОРУССКИЙ

ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЁТ**

**По лабораторной работе №1:**

**ТЕМА «РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ИЛИ УЧРЕЖДЕНИЯ»**

Минск 2022

# Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении).

*Политика информационной безопасности* (ПИБ) организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

Актуальность ПИБ состоит в том, чтобы не допустить законодательно или на основе правил утечки конфиденциальной информации в свободный доступ. Для каждой организации или учреждения необходимо иметь собственный набор правил, составленных на основе законодательства РБ чтобы уменьшить риски и наложить ответственность в ответ на противоправные действия со стороны сотрудников или сторонних субъектов.

**Цели:**

* Основной целью, на достижение которой направлена ПИБ, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

**Задачи:**

* Своевременное выявление, оценка и прогнозирование источников угроз ИБ;
* Создание механизма оперативного реагирования на угрозы ИБ;
* Предотвращение и/или снижение ущерба от реализации угроз ИБ;
* Защита от вмешательств в процесс функционирования Информационной Системы (ИС) посторонних лиц;
* Соответствие требованиям законодательства по информационной безопасности Республики Беларусь, нормативно-методических документов и договорным обязательствам в части ИБ;
* Обеспечение непрерывности критических бизнес-процессов;
* Достижение адекватности мер по защите от угроз ИБ;
* Изучение партнёров, клиентов, конкурентов и кандидатов на работу;
* Недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
* Выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
* Повышение деловой репутации и корпоративной культуры;

# Объекты защиты.

Объекты защиты:

* Коммерческая тайна издательства, данные о ее договорах, финансовых взаимоотношениях, бухгалтерская информация;
* Коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах, произошедших страховых событиях;
* Персональные данные сотрудников компании и сотрудников клиентов, эта информация иногда включает номера автомобилей, водительских удостоверений, кредитных карт;
* Все массивы информации содержатся как на бумажных, так и на электронных носителях.

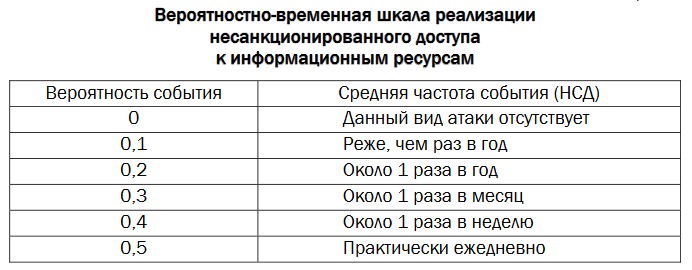
# Основные угрозы и их источники.

* Действия внутреннего или внешнего злоумышленника (несанкционированный, в том числе удаленный доступ с целью нарушения работоспособности ИВС, кражи, удаления или модификации информации, несанкционированного распространение материальных носителей за пределами организации);
* Наблюдение за источниками информации;
* Подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов;
* Перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;
* Разглашение информации компетентными людьми;
* Несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре;
* Воздействие стихийных сил (наводнения, пожары и т. п.);
* Сбои и отказы в аппаратуре сбора, обработки и передачи информации;
* Отказы системы электроснабжения;
* Воздействие мощных электромагнитных и электрических помех (промышленных и природных).

# Оценка угроз, рисков и уязвимостей.

**Условная численная шкала для оценки ущерба компании**

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации, не являющейся конфиденциальной и не раскрывающая данных о заказчиках |
| 1 | Ущерб атаки есть, но он незначителен и не связан с положением компании на рынке |
| 2 | Существует вероятность потери некоторого числа клиентов, компания теряет часть прибыли |
| 3 | Потеря весомой доли клиентов и потеря доли рынка, компания несет убытки |
| 4 | Полная потеря рынка и конкурентоспособности, долги, а так же полная потеря клиентов, банкротство |
| 5 | Полное банкротство компании и прекращение существования |

****

**Оценка рисков**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Спам | 1 | 0,4 | 0,4 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| Непреднамеренный рассказ конфиденциальной информации | 3 | 0,4 | 1,2 |
| Раскрытие основных планов и стратегий развития издательства | 4 | 0,1 | 0,4 |
| Раскрытие личных данных клиентов издательства | 3 | 0,2 | 0,6 |
| Итого | 2.8 | 0.24 | 0.58 |

# Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.

Информационная безопасность издательства должна обеспечиваться целым комплексом мер, среди которых:

* административно-правовые;
* организационные;
* программно-технические

Данные меры следует применять совместно. Опираться система защиты должна на управление персоналом компании и контроль над ним. Меры технического характера не менее важны, но не могут существовать в отрыве от организационных мер.

**Вывод:**

Комплексное применение современных технических средств в работе службы безопасности издательства может обеспечить высокий уровень защиты информации от утечек и несанкционированного доступа.

Следует учитывать, что все предпринимаемые действия должны в полной мере соответствовать требованиям законодательства. В частности, нарушение конфиденциальности данных юридической фирмы и их клиентов зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – юридическая фирма понесет ответственность – начиная от финансовой и закачивая уголовной