

Политика информационной безопасности “ION MEDIA”

(Подготовил Мирошниченко Георгий,

учащийся группы БСБО-09-18)

**Москва 2019**

**Содержание**

**Содержание.................................................................................................................... 2**

**Основные положения.................................................................................................... 3**

**Список терминов и определений.................................................................................. 4**

**Описание объекта защиты............................................................................................. 6**

**Цели и задачи деятельности по обеспечению информационной безопасности.................................................................................................................. 6**

**Угрозы информационной безопасности.................................................................................................................. 7**

**Модель нарушителя информационной безопасности.................................................7**

**Основные принципы обеспечения информационной безопасности.................................................................................................................. 8**

**Организационная основа деятельности по обеспечению информационной безопасности................................................................................................................. 10**

**Заключительные положения........................................................................................11**

**1.Общие положения**

1.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права

1.2. Настоящая Политика является документом, доступным любому сотруднику Медиа и пользователю его ресурсов, и представляет собой официально принятую руководством “ION MEDIA” (далее – Медиа) систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Медиа.

1.3. Требования информационной безопасности, которые предъявляются Медиа, соответствуют интересам (целям) деятельности Медиа и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Медиа имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности.

1.4. Стратегия Медиа в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

* российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных, банковской тайны и других правовых актов;
* нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности;
* закона РФ от 27.12.1991 N 2124-1 (ред. от 06.06.2019) "О средствах массовой информации"

1.6. Необходимые требования обеспечения информационной безопасности Медиа должны неукоснительно соблюдаться персоналом Медиа и другими сторонами как это определяется положениями внутренних нормативных документов Медиа, а также требованиями договоров и соглашений, стороной которых является Медиа.

1.7. Настоящая Политика распространяется на бизнес - процессы Медиа и обязательна для применения всеми сотрудниками и руководством Медиа, а также пользователями его информационных ресурсов.

1.8. Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности в дочерних и аффилированных организациях.

**2.Список терминов и определений**

2.1. **Бизнес-процесс** – последовательность технологически связанных операций по предоставлению медиа продуктов и/или осуществлению конкретного вида обеспечивающей деятельности Медиа.

2.2. **Информационная безопасность Медиа(ИМ)** – в настоящей Политике состояние защищенности технологических и бизнес - процессов Медиа, объединяющих в своем составе сотрудников Медиа, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

2.3. **Информационная система Медиа** – совокупность программно-аппаратных комплексов Медиа, применяемых для обеспечения бизнес - процессов Медиа.

2.4. **Инцидент информационной безопасности** – это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

2.5. **ИТ-блок** – совокупность самостоятельных структурных подразделений Медиа, ответственных за развитие, эксплуатацию и сопровождение информационных банковских систем

2.6. Конфиденциальная информация (далее – КИ) – информация, в отношении которой Медиа установлен режим конфиденциальности

2.7. Модель угроз – описательное представление свойств или характеристик угроз безопасности информации.

2.9. Модель нарушителя – описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИМ, необходимых им для реализации угрозы ИМ, и возможной мотивации действий

2.10. Пользователь информационной системы - физическое лицо, обладающее возможностью доступа к информационной системе Медиа.

2.11. Ответственное подразделение – Служба (департамент) безопасности Медиа. Основные функции в указанной сфере – внедрение настоящей Политики, разработка, внедрение и поддержка систем обеспечения информационной безопасности Медиа.

2.12. Режим конфиденциальности информации – организационно-технические мероприятия по защите информации, позволяющие обладателю КИ при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, и реализующие меры по охране КИ, включающие в себя:

• ограничение доступа к КИ путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

• учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;

• регулирование отношений по использованию КИ работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений

2.14. Угроза информационной безопасности – операционный риск, влияющий на нарушение одного (или нескольких) свойств информации – целостности, конфиденциальности, доступности объектов защиты.

2.15 Пользователь - физическое лицо, обращающееся к услугам Медиа.

2.16 Контент - данные(информация), произведенные сотрудником Медиа в интересах Медиа.

**3. Описание объекта защиты**

Основными объектами защиты системы информационной безопасности в Медиа являются:

* информационные ресурсы, содержащие коммерческую тайну.
* любой вид контента(данных), сгенерированный или произведенный сотрудником (не противореча трудовому договору).
* информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц (как сотрудников, так и физических лиц, являющихся клиентами Медиа)
* информационные каналы, средства, с помощью которых происходит обеспечении безопасности Медиа, данные о взаимодействии сотрудников Медиа.
* данные, направленные в медиа независимыми лицами, желающими скрыть свою причастность к отправленному
* архивные записи контента, доступ к которому не был открыт широкому кругу лиц.
* Основной сайт Медиа предоставляет его пользователям доступ к открытому контенту, запрашивая следующие данные пользователя, которые также являются объектами защиты:

1. IP адрес;
2. информация из cookies;
3. информация о браузере (или иной программе, которая осуществляет доступ к показу рекламы);
4. время доступа пользователя;

**4. Цели и задачи деятельности по обеспечению информационной безопасности**

Целью деятельности по обеспечению информационной безопасности Медиа является снижение угроз информационной безопасности до приемлемого для Медиа уровня.

Основные задачи деятельности по обеспечению информационной безопасности Медиа:

* выявление потенциальных угроз информационной безопасности и уязвимостей1 объектов защиты;
* предотвращение инцидентов информационной безопасности;
* исключение либо минимизация выявленных угроз.

**5. Угрозы информационной безопасности**

Угрозы безопасности медиа подразделяются на 3 класса по природе их возникновения: антропогенные, техногенные и естественные.

5.1. Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

5.2. В качестве антропогенного источника угроз рассматривается субъект, имеющий доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта.

5.3 Антропогенные источники угроз могут быть как **внутренними**, так и **внешними**.

5.4. Техногенные источники угроз - источники угроз, определяемые технократической деятельностью человека.

5.5. Техногенные источники угроз могут быть представлены в виде технических устройств, используемых сотрудниками Медиа, программного обеспечения (далее ПО), ненадёжностью каналов связи и других используемых в процессе работы Медиа технических средств.

5.6 Возникновение естественных угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

**6. Модель нарушителя информационной безопасности**

По отношению к Банку нарушители могут быть разделены на внешних и внутренних нарушителей.

6.1. Внутренние нарушители

В качестве потенциальных внутренних нарушителей Медиа рассматриваются:

* сотрудники Медиа
* персонал, обслуживающий технические комплексы Медиа
* пользователи, зарегистрированные в системе как “отправители”
* сотрудники самостоятельных структурных подразделений Медиа

6.2 Внешние нарушители

В качестве потенциальных внешних нарушителей Медиа рассматриваются:

* Пользователи Медиа.
* Бывшие сотрудники Медиа.
* Представители спецслужб, лица, действующие в их интересах.
* Конкурирующие организации
* Иные лица, случайно или умышленно проникшие в корпоративную информационную систему Медиа из внешних телекоммуникационных сетей

**7.Основные принципы обеспечения информационной безопасности**

7.1 Основными принципами обеспечения ИБ являются следующие:

* постоянный и всесторонний анализ информационного пространства Медиа с целью выявления уязвимостей информационных активов;
* своевременное обнаружение проблем, потенциально способных повлиять на Медиа, корректировка моделей угроз и нарушителя;
* разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для
* контроль эффективности принимаемых защитных мер;

7.2 Требования об обеспечении информационной безопасности Медиа обязательны к соблюдению всеми работниками Медиа и пользователями информационных систем.

7.3 Стратегия Медиа в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Медиа, до специализированных мер информационной безопасности по каждому выявленному в Медиа риску, основанных на оценке рисков информационной безопасности.

7.4. В рамках реализации деятельности по обеспечению информационной безопасности в Банке осуществляются:

* Менеджмент инцидентов информационной безопасности
* Обеспечение защиты информации от утечки по техническим каналам

7.5. Менеджмент инцидентов информационной безопасности включает в себя:

* выявление и анализ инцидентов информационной безопасности;
* расследование инцидентов информационной безопасности;
* оперативное реагирование на инцидент информационной безопасности
* минимизация негативных последствий инцидентов информационной безопасности;

7.6. Обеспечение защиты информации от утечки по техническим каналам включает в себя:

* применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;
* применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита
* применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

7.7 В целях совершенствования деятельности по обеспечению информационной безопасности в Медиа осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Медиа).

**8. Организационная основа деятельности по обеспечению информационной безопасности**

8.1. Для обеспечения безопасности Медиа, в нём существует специальный отдел (далее Ответственное подразделение)

8.2. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Медиа осуществляются и координируются Ответственным подразделением. Основными задачами Ответственного подразделения являются:

* установление потребностей Медиа в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
* разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Медиа, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;
* выявление и предотвращение реализации угроз информационной безопасности;
* выявление и реагирование на инциденты информационной безопасности;
* пресечение несанкционированных действий нарушителей информационной безопасности;
* мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности Медиа;

8.3. Ответственное подразделение может создавать оперативные группы для проведения расследований инцидентов информационной безопасности

**9.Заключительные положения**

9.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами Медиа, которые дополняют и уточняют ее.

9.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Медиа настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Медиа. В этом случае Ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.