ПАО «Группа Ренессанс Страхование»
www.renins.ru
info@renins.com
115114, г. Москва, Дербеневская набережная, дом 11, этаж 10, пом. 12
Тел.: 8 495 725-10-50
Факс: 8 495 967-35-35

Приложение №1

УТВЕРЖДЕНА

Приказом Генерального директора
Гадлиба Ю. О.

№ ..... от ..... 20 ..... г.

Политика

предотвращения утечек информации в ПАО «Группа Ренессанс Страхование»

Москва
2024

Оглавление

1. Область применения

1.1. Настоящая Политика определяет требования к порядку планирования, реализации, контроля и совершенствования процессов и систем, направленных на предотвращение утечек информации, составляющей коммерческую тайну ПАО «Группа Ренессанс Страхование» (далее – Общество), включая персональные данные работников, клиентов и контрагентов, а также конфиденциальной, инсайдерской и иной информации ограниченного распространения.

1.2. Настоящая Политика разработана с целью формирования единого подхода к противостоянию угрозам информационной безопасности, связанным с несанкционированным распространением информации конфиденциального характера, и способным оказать негативное влияние на операционный риск Общества.

1.3. Пересмотр настоящей Политики (в том числе, с целью актуализации) осуществляется по мере необходимости, но не реже одного раза в год.

2. Термины, определения и сокращения

Корпоративная сеть ПАО «Группа Ренессанс Страхование» (в рамках данной Политики) – объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех функций Общества, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов.

Общество – ПАО «Группа Ренессанс Страхование».

Пользователь – лицо, которому был предоставлен доступ к информационным системам Общества.

Отдел ИБ – Отдел информационной безопасности.

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

СВТ – средство вычислительной техники.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Работники ИТ – работники Департамента информационных технологий и стратегических инициатив.

Система предотвращения утечек (Data leak prevention, DLP) – подсистема информационной безопасности, предназначенная для обнаружения и (или) предотвращения неконтролируемого Обществом распространения информации конфиденциального характера.

Субъект доступа – работник Общества или иное лицо, осуществляющий физический и (или) логический доступ, или программный сервис, осуществляющий логический доступ.

Регистрация событий защиты информации (регистрация) – фиксация данных о совершенных субъектами доступа действиях или данных о событиях защиты информации.

URL (Uniform Resource Locator) – единый указатель ресурса, адрес информационного ресурса (файла) в сети Интернет.

3. Основные положения

3.1. Применяемые в Обществе меры по предотвращению утечек информации конфиденциального характера должны обеспечивать:

- Блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации;
- Контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации;
- Организацию защиты машинных носителей информации (МНИ);

- Регистрацию событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации.

3.2. С целью предотвращения утечек информации конфиденциального характера Обществом могут приниматься организационные и технические меры, в том числе с применением систем обнаружения и предотвращения утечек информации (DLP) и иных средств защиты информации, обладающих соответствующими функциями.

3.3. В ходе реализации мер, направленных на обнаружение и предотвращение утечек информации конфиденциального характера в Обществе, осуществляется:

- Блокирование неразрешенной и контроль (анализ) разрешенной передачи информации конфиденциального характера в сеть Интернет с использованием информационной инфраструктуры Общества, отправки на внешние адреса электронной почты, а также вывода такой информации на печать и её записи на переносные (отчуждаемые) носители информации;

- Контроль содержания информации (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), передаваемой за периметр ЛВС Общества по сетям связи (с применением электронной почты, сервисов обмена сообщениями (мессенджеров), IP-телефонии и видеоконференцсвязи, веб-сайтов и иных каналов и средств передачи данных), а также записываемой на переносные (отчуждаемые) носители информации, и выводимой на печать с применением основных и вспомогательных технических средств Общества;

- Ведение единого архива электронных сообщений с архивным доступом на срок не менее шести месяцев и оперативным доступом на срок не менее одного месяца;

- Ограничение перечня форматов файлов, допущенных к передаче за периметр ЛВС Общества, и размеров передаваемых файлов в зависимости от способа передачи (электронная почта, SFTP, облачные хранилища, машинные носители);

- Ограничение перечня протоколов сетевого взаимодействия, используемых для взаимодействия с сетью Интернет и передачи сообщений электронной почты;

- Классификация ресурсов сети Интернет с целью разграничения доступа к сайтам или типам сайтов и блокировки тех из них, которые запрещены к использованию в соответствии с установленными правилами;

- Блокирование неразрешенных к использованию портов ввода-вывода информации СВТ;

- Учёт, маркирование и контроль машинных носителей информации, предназначенных для хранения конфиденциальной информации, а также документарное определение порядка доступа к таким носителям и их использования;

- Блокирование возможности использования незарегистрированных (неразрешенных к использованию) переносных (отчуждаемых) носителей информации в информационной инфраструктуре финансовой организации;

- Стирание информации конфиденциального характера с машинных носителей информации средствами гарантированного стирания, или способом (средством), обеспечивающим невозможность их восстановления, или средствами, обеспечивающими полную перезапись данных, при передаче (перезакреплении) машинных носителей информации между работниками и (или) структурными подразделениями финансовой организации;

- Шифрование информации конфиденциального характера при ее хранении на машинных носителях информации, выносимых за пределы финансовой организации.

3.4. Меры по регистрации событий защиты информации, связанных с реализацией мер по предотвращению утечки информации, применяемые в Обществе, включают:

- Регистрацию использования портов ввода-вывода: события подключения или извлечения устройств, тип выполняемых операций (чтение, запись, передача данных), результат выполненных операций (успешно или неуспешно), состав и содержимое переданных или

полученных посредством портов ввода-вывода данных;

- Регистрацию результатов выполнения контентного анализа, включая содержимое проанализированных данных;
- Регистрацию операций, связанных с осуществлением доступа работниками финансовой организации к ресурсам сети Интернет, включая URL, текст запроса, состав и содержимое переданных или полученных данных.

3.5. В целях своевременного реагирования на события информационной безопасности, связанные с потенциальными или действительными утечками информации, работниками Отдела ИБ Общества осуществляется периодический мониторинг сообщений, сохранённых в едином архиве, и журналов регистрации, описанных в п. п. 3.4 настоящей Политики.

4. Права и ответственность

4.1. Работники Общества несут ответственность за соблюдение требований настоящей политики, а также других нормативных документов в области защиты информации.

4.2. Работники Отдела информационной безопасности Общества в пределах своих полномочий и должностных обязанностей контролируют конфиденциальность обрабатываемой информации ограниченного распространения, несут ответственность за функционирование подсистем разграничения доступа, технических средств, реализующих меры, приведённые в п. п. 3.4 настоящей Политики, а также средств регистрации и учета событий информационной безопасности и других средств защиты информации,

4.3. Планирование изменений в системе предотвращения утечек конфиденциальной информации Общества и внесение предложений по её совершенствованию осуществляется работниками Отдела информационной безопасности.

4.4. Работники обязаны хранить в тайне сведения конфиденциального характера, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации, и немедленно информировать о таких фактах, а также о других причинах или условиях возможной утечки конфиденциальной информации своего непосредственного руководителя и работников Отдела информационной безопасности.

4.5. Прекращение доступа к сведениям конфиденциального характера не освобождает работника от взятых им обязательств по неразглашению таких сведений.

4.6. При работе с конфиденциальной информацией работники обязаны:

- Строго соблюдать установленные правила обеспечения безопасности информации при работе в ИС Общества;
- Выполнять требования администраторов безопасности ИС, касающиеся защиты информации;
- Знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на СВТ Общества;
- Использовать для работы только учтенные съемные накопители информации (флэш-накопители, гибкие магнитные диски, компакт диски и т.д.);
- При необходимости передачи сведений конфиденциального характера через Интернет, использовать только корпоративные адрес электронной почты, облачное хранилище или SFTP-сервер.

Запрещается:

- Передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения конфиденциального характера;
- Использовать сведения конфиденциального характера при подготовке открытых публикаций, докладов, научных работ и т. д.;

- Записывать и хранить конфиденциальные данные на неучтенных носителях информации (флэш-накопителях, гибких магнитных дисках, компакт-дисках и т. д.), а также в личных и общедоступных облачных хранилищах информации;
- Использовать для передачи или получения сведений конфиденциального характера личные учётные записи в сервисах электронной почты, социальных сетях или программах мгновенного обмена сообщениями (мессенджеров);
- Умышленно создавать и использовать недокументированные возможности и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности информации. Об обнаружении такого рода ошибок ставить в известность работников Отдела информационной безопасности;
- Осуществлять фотографирование и видеосъёмку средств отображения конфиденциальной информации, документов и иных материальных носителей, содержащих такую информацию в форме, позволяющей визуальное ознакомление с ней.

За разглашение конфиденциальной информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

5. Исключения и ограничения

5.1. В целях выполнения Правил внутреннего трудового распорядка Общества использование оборудования и любого иного имущества Общества в личных целях запрещается как в рабочее время, так и вне его пределов.

5.2. В случае нарушения Пользователем требований п. 4.1 настоящей политики, Общество не гарантирует исключение личной информации (в том числе сведений о частной жизни, личной и семейной тайны) из общего массива информации, обрабатываемой (включая в том числе: сбор, запись, систематизацию, накопление, хранение, обновление, изменение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) в ИС Общества при реализации п. 3 настоящей Политики.

6. Требования по контролю

6.1. Задачи общего контроля выполнения требований настоящей Политики, а также поддержания данного документа в актуальном состоянии, возлагаются на Отдел ИБ.

6.2. Соответствующие требования настоящей Политики должны реализовываться в виде настроек ИС, позволяющих централизованно управлять средствами обнаружения и предотвращения утечек информации с применением автоматизации.

6.3. Обо всех нарушениях требований настоящей Политики требуется незамедлительно информировать работников Отдела ИБ.

6.4. Совершение операций с базами данных, журналами событий и архивами сведений, содержащими информацию, накопленную в процессе реализации мер по предотвращению утечек информации, допускаются исключительно после получения согласования руководителя Отдела ИБ.