DOI 10.37882/2223–2966.2020.04.26

# СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ

## INFORMATION SECURITY TOOLS FOR CORPORATE CLIENTS

***L. Makshanova***
***T. Toktohoeva***
***T. Tsybikova***

*Summary.* The article deals with the problem of cybercrime and means of information security, as ways to solve it. Types of cyber attacks and their statistics on enterprises and public authorities are given. It describes the laws of the Russian Federation, which must be complied with in the implementation of information security measures. The article also presents examples of information security tools, in particular, products and principles of operation of Rostelecom PJSC Solar, as well as the results of using these tools.

*Keywords:* information security, the problem of cybercrime, Rostelecom Solar, hacker attacks, information protection, hacking, phishing, DDos attacks.

***Макшанова Лариса Михайловна***
*К.т.н., доцент, ФГБОУ ВО «Бурятский государственный университет имени Доржи Банзарова», Улан-Удэ*
*lorimak@list.ru*
***Токтохоева Татьяна Александровна***
*Старший преподаватель, ФГБОУ ВО «Бурятский государственный университет имени «Доржи Банзарова», Улан-Удэ*
*totaal@mail.ru*
***Цыбикова Туяна Сандаликовна***
*К.п.н., доцент, ФГБОУ ВО «Бурятский государственный университет имени Доржи Банзарова», Улан-Удэ*
*cts2001@mail.ru*

*Аннотация.* В статье рассматриваются проблема киберпреступности и средства информационной безопасности, как пути ее решения по размещению оборудования. Представлен расчет размещения серверов, приводятся типы кибератак и их статистика на предприятия и органы государственной власти. Описываются законы РФ, которые должны быть соблюдены в ходе реализации мер по информационной безопасности. Также в статье приводятся примеры средства информационной безопасности, в частности — продукты ПАО «Ростелеком» Solar возможности и принципы работы, а также результаты, которые дает использование данных средств.

*Ключевые слова:* информационная безопасность, проблема киберпреступности, Ростелеком Solar, хакерские атаки, защита информации, хакерство, фишинг, DDos-атаки.

## Введение

В эпоху телекоммуникационных технологий и тотальной цифровизации информации во всех сферах жизни: образование, бизнес, власть, развлечения и так далее, появилась такая проблема, как киберпреступность. Чем сложнее сфера преступности, тем более сложно и изощренно действуют преступники. Тем более, что с возрастающим поглощением всех областей жизни машинами, растут возможности и масштабы для подобного вида преступлений. Теперь жулики не ограничиваются простыми манипуляциями в сети типа взлома страниц. Хакерам высокого уровня не составляет труда нанести урон крупным компаниям, и шантажировать их, взламывать правительственные базы, обнародовать компрометирующую информацию, не говоря уже о воровстве денег со счетов (фишинге) и прочих преступлениях.

Так как данная проблема стоит остро, появилось такое направление деятельности, как информационная безопасность. Это целый спектр средств защиты от хакерских атак, а также непрерывная работа специалистов в этой сфере, которые адаптируют защиту для отражения и предупреждения возможности взломов, повреждений и краж информации, вредоносного программного обеспечения, промышленного шпионажа и прочих возможных противоправных действий.

В нашей стране существует Федеральный закон «Об информации, информационных технологиях и о защите информации» 149-ФЗ от 9 августа 2006 года. В нем описываются понятия и определения в области информационной технологии, принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, а также регулируются отношения при осуществлении права

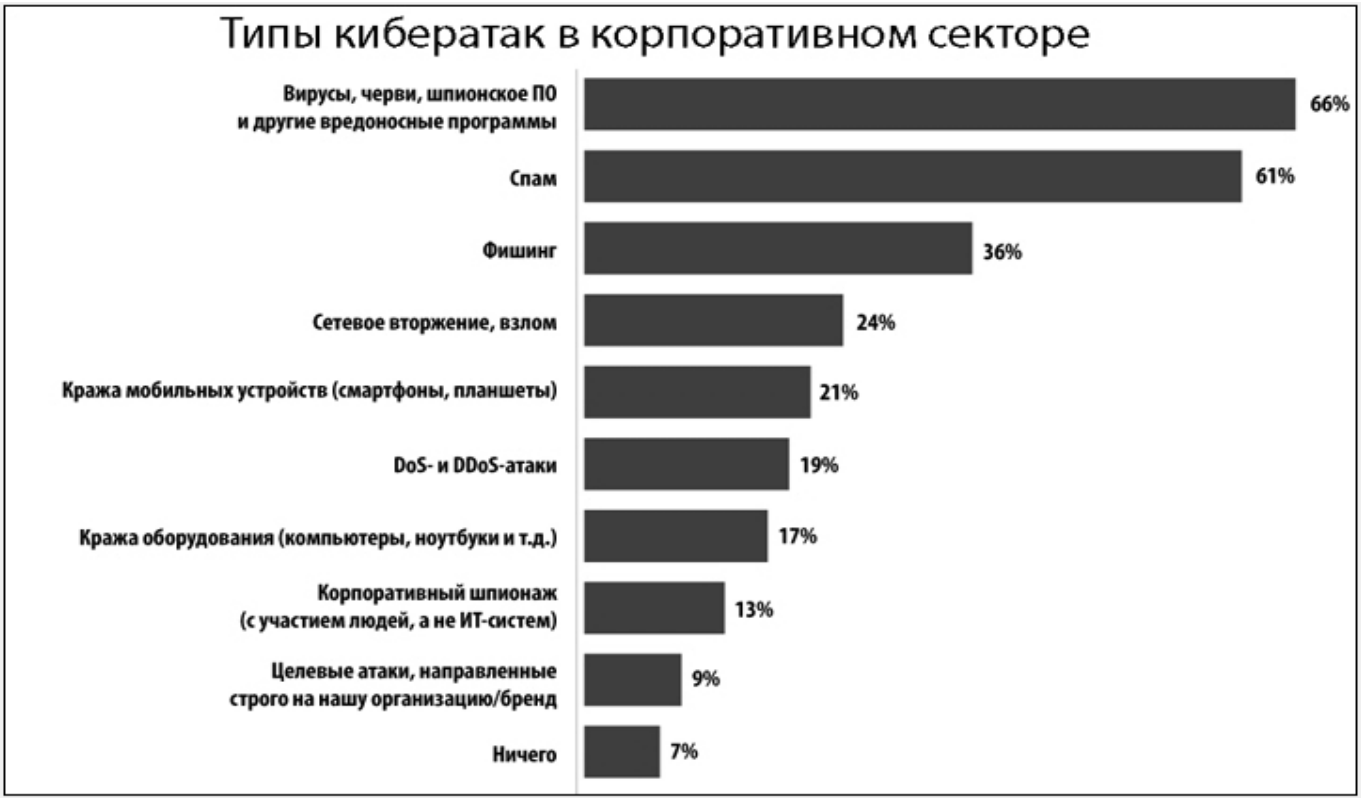


Рис. 1. Типы кибератак в корпоративном сегменте

на поиск, получение, передачу, производство и распространение информации при применении информационных технологий. Также существуют национальные стандарты в области информационной безопасности — это Перечень Государственных стандартов Российской Федерации в области защиты конфиденциальной информации и персональных данных. Конкретно этот документ регламентирует работу, к примеру, с информацией о гражданах, получающих какую-либо государственную услугу, либо медицинскую помощь. Все мы когда-либо заполняли соглашение на обработку персональных данных в поликлинике или еще каком-либо учреждении/компании. Безусловно, есть еще ряд других документов, которым подчиняется вся структура информационной безопасности в России, но перейдем к описанию средств информационной безопасности на примере продуктов компании «Ростелеком».

У этой телекоммуникационной компании существует целое направление по осуществлению информационной безопасности, и она является национальным провайдером сервисов и технологий кибербезопасности в России.

В основе технологий компании лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами информационной безопасности. Этот принцип реализован в продуктах и сервисах Ростелеком. Среди клиентов организации есть как государственные учреждения, так и бизнес-гиганты российского рынка. Но надежная защита в киберпространстве, безусловно, нужна абсолютно всем. Рассмотрим подробно и максимально доступно решения, которые разработала данная компания.

**Безопасность из облака (ЕПСК)** — это набор сервисов по информационной безопасности, предназначенных для защиты информационной инфраструктуры и приложений заказчиков от различных сетевых угроз и вредоносного ПО. Применяется для защиты периметра информационных систем и приложений, расположенных на площадках заказчика, либо размещенных в облаке, в том числе: межсетевое экранирование, обнаружение и предотвращение вторжений, мониторинг и реагирование на инциденты ИБ, защита от атак на веб-приложения, защита электронной почты, защиты от фишинговых атак, контроль приложений, антивирусная защита, защита от DDoS атак.

**Универсальный шлюз безопасности (UTM)** — услуга предназначена для снижения вероятности реализации

актуальных для клиента сетевых угроз. Услуга предполагает наличие опций:

- межсетевое экранирование на уровне сети (FW);
- межсетевое экранирование на уровне сети и обнаружение/предотвращение вторжений (FW + IPS);
- комплексное решение (UTM), включающее в себя межсетевое экранирование на уровне сети, обнаружение/предотвращение вторжений, фильтрацию трафика веб-приложений, контроль использования приложений, а также защиту от вредоносного ПО.

**Мониторинг и реагирование на инциденты ИБ —** Услуга предназначена для выявления инцидентов информационной безопасности в инфраструктуре заказчика и последующего реагирования на них с целью нейтрализации ущерба. В рамках сервиса SOC обеспечивается принятие проактивных мер, направленных на предотвращение инцидентов ИБ, обнаружение актуальных угроз и атак в области ИБ и реагирование на них раньше, чем будет оказано влияние на работоспособность и деятельность информационных систем Заказчика.

Возможности данного решения:

- выявление и реагирование на инциденты ИБ в режиме 24x7 с целью обеспечения защищенности конфиденциальной информации и сети заказчика,
- повышение устойчивости к киберугрозам за счет применения проактивных мер обеспечения ИБ по мере выявления новых атак или уязвимостей,
- выявление и нейтрализация непреднамеренной нежелательной активности или действий, носящих криминальных характер
- получение бизнес-аналитики поведения пользователей в сети Заказчика с целью формирования и определения приоритетов в стратеги развития ИТ систем Заказчика.

**Защита от DDoS —** Анализ интернет-трафика в адрес клиента и защита ресурсов от DoS- и DDoS-атак посредством фильтрации этого трафика. Результат — снижение риска как косвенных репутационных потерь, так и прямых финансовых потерь (в связи с невозможностью осуществления своей прямой деятельности) в случае недоступности или ограниченной функциональности интернет-ресурсов.

**Security Awareness** — это облачный сервис по оценке и формированию устойчивых навыков ИБ у сотрудников. Заказчику предоставляется доступ к личному кабинету платформы для самостоятельной работы, либо разовую услугу по оценке персонала.

Необходима прежде всего для сотрудников ведущих активную переписку внешними контрагентами, а также для всех остальных сотрудников с доступом к важной информационным ресурсам. Результатом является снижение риска финансовых потерь, в результате снижения ошибок персонала в распознавании атак злоумышленников через фишинговые письма и сайта.

**Аттестация информационных систем** — это мероприятия по оценке соответствия информационных систем требованиям законодательства по защите информации. Итогом оказания услуги является аттестат соответствия. Услуга необходима для информационных систем, расположенных на площадках заказчика или размещаемых в облаке, если:

- в системе обрабатываются персональные данные;
- система имеет статус Государственной/Муниципальной информационной системы;
- в системе обрабатывается информация, содержащая служебную тайну.

Услуга позволяет заказчикам подтвердить выполнение требований законодательства по защите информации.

**Тестирование на проникновение (pentest)** — Консалтинговая услуга для оценки уровня защищенности инфраструктуры и приложений организации. По результатам выполнения оценке предоставляется отчёт о обнаруженных уязвимостях и рекомендации по их устранению.

Результаты оказания услуги позволяют оценить эффективность как уже выполненных инвестиций в ИБ, так и выбрать приоритетные направления для новых инвестиций.

## Защита веб-приложений (WAF)

Web Application Firewall (WAF) — межсетевой экран уровня приложений, позволяющий детектировать и блокировать атаки, направленные на веб-приложения.

WAF позволяет создавать правила, которые способствуют защите от таких распространенных сетевых угроз как внедрение SQL-кода или межсайтовый скриптинг. Услуга используется для защиты веб-приложений расположенных на площадках заказчика или размещаемых в облаке.

## Услуга обеспечивает следующий функционал

фильтрация сетевого трафика Веб-приложений Клиента на стороне Оператора с целью его анализа на при-

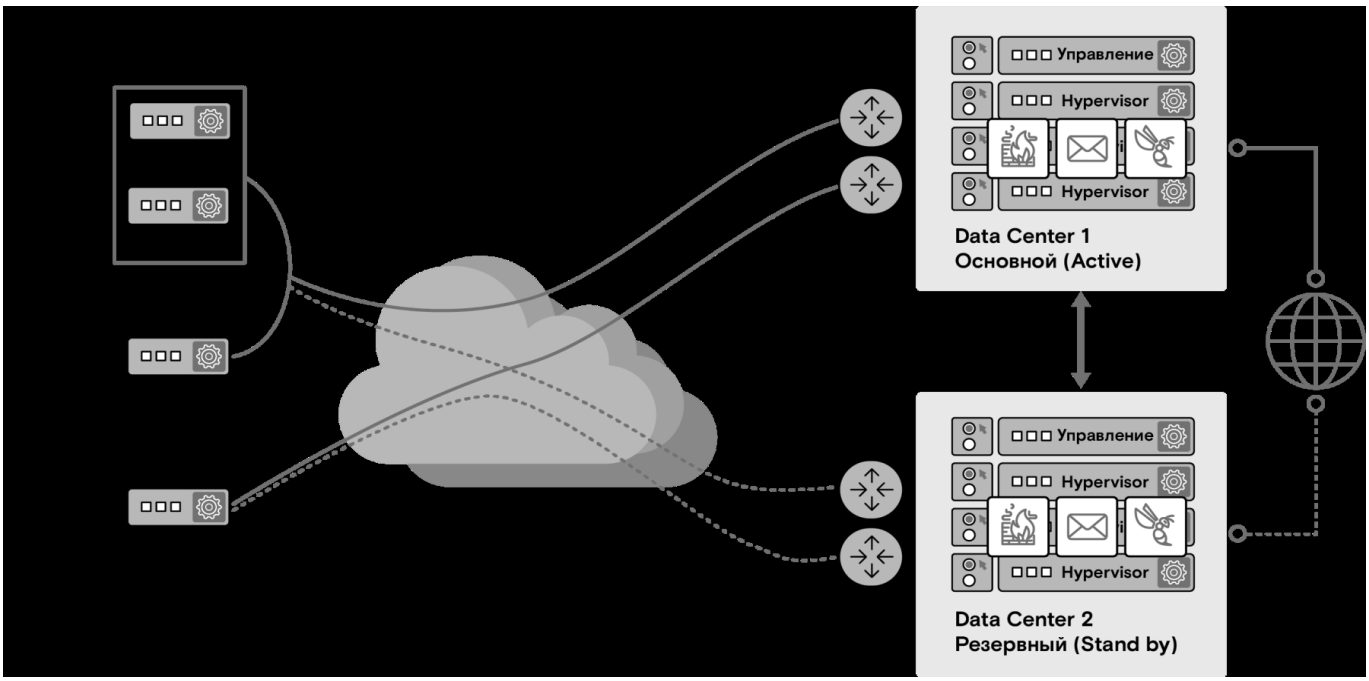


Рис. 2. Схема функционирования услуг по информационной безопасности.


Рис. 3. Схема подключения услуг по информационной безопасности.

кладном уровне, создание индивидуального профиля защиты для каждого Веб-приложения Клиента, обучение и настройка WAF для обеспечения корректной фильтрации трафика, корректировка индивидуальных профилей защиты в случае выявления некорректных срабатываний, изменения состава/функционала Веб-приложений или по запросу Клиента.

- Мониторинг и реагирование на инциденты в режиме 24x7.

**Анализ защищенности** — облачный сервис, по инструментальной оценке, защищенности ИТ-активов предприятия. Заказчик может выбрать либо готовый отчёт по сканированию требуемых узлов, либо предоставление доступа к личному кабинету платформы для самостоятельного сканирования узлов. Экономически эффективный процесс регулярного получения отчёта по защищенности нужного количества узлов с нужно периодичностью для своевременного устранения критических уязвимостей.

## Заключение

Таким образом понятно, что основной целью всех мероприятий и сервисов информационной безопасности является недопущение утечки, повреждения, раскрытия или неправомерного использования конфиденциальной информации, а также защита от проникновений злоумышленников в информационную систему, которую они охраняют.

С развитием киберпреступности развивается и направления информационной безопасности, причем не просто пропорционально, а идя на опережение, предупреждая возможность совершения данного рода преступлений, целью которых зачастую являются шантаж, деньги, получение контроля над деятельностью, либо нанесение урона репутации атакуемых организаций, либо людей.

ЛИТЕРАТУРА

1. Запечинков, С. В. Информационная безопасность открытых систем в 2-х томах т. 1 / С. В. Запечинков. — М.: ГЛТ, 2006. — 536 с.
2. Гришина, Н. В. Информационная безопасность предприятия: Учебное пособие / Н. В. Гришина. — М.: Форум, 2017. — 159 с.
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — М.: ДМК, 2014. — 702 с.
4. Ярочкин, В. И. Информационная безопасность: Учебник для вузов / В. И. Ярочкин. — М.: Академический проспект, 2008. — 544 с.
5. Описания продуктов ИБ ПАО «Ростелеком»: Пособие для сотрудников/ М.: 2018. — 6с.


Журнал «Современная наука: актуальные проблемы теории и практики»

Г. Улан-Удэ