Ростелеком
Солар

Исследование «Нарушения в части управления доступом в российских компаниях»

Октябрь – ноябрь 2021

МОСКВА, 2021

Содержание

1. Ключевые цифры и факты

- **72,5%** компаний регистрируют у себя случаи нарушений прав доступа в информационные системы: **40%** – более 3 раз в год, **32,5%** – свыше 5 раз в год
- Почти **90%** опрошенных отметили, что число таких нарушений в компаниях в 2021 году выросло
- В **55%** случаев нарушения доступа приводят к утечке конфиденциальной информации компании
- **40%** нарушений вызваны передачей сотрудниками своих логинов-паролей от внутренних систем компании коллегам, подрядчикам, друзьям; в **30%** случаев персонал использует ненадежные пароли и еще в **22,5%** случаев – небезопасно их хранит.
- В **50%** компаний доступы уволившихся сотрудников ко внутренним системам так или иначе остаются незаблокированными (о части уволившихся забывают, блокируют их доступ не во все системы либо не блокируют вовсе)

2. Методология

Данное исследование проведено методом электронных опросов аудитории наиболее популярных интернет-изданий по тематике информационной безопасности Securitylab.ru, Anti-Malware.ru, по ИТ-тематике – TAdviser и ComNews.

В опросе приняли участие представители компаний более 8 отраслей экономики, в том числе из финансовой сферы, ИТ/Телекома, производства, госсектора, сферы услуг, ретейла, ВПК и др. Для целей исследования были отобраны компании в категориях с численностью персонала до 500 сотрудников, от 500 до 1000 сотрудников и свыше 1000 сотрудников. География респондентов представлена 7 федеральными округами России, в число опрошенных не вошли представители Дальневосточного ФО.

Всего в исследовании приняли участие около 100 представителей компаний. Опросы проводились в период с октября по ноябрь 2021 года.

В ходе опросов респондентам предлагалось выбрать один из предложенных вариантов ответа или указать свой вариант ответа в свободной форме.

3. Введение

К сожалению, инцидентам, вызванным различными нарушениями прав доступа в информационные системы компаний, не уделяется широкого внимания в публичном поле. Об этой проблеме редко говорят в СМИ, она, как правило, остается во внутренней кухне специалистов по информационной безопасности.

Однако по данным исследования «Итоги защищенности российских компаний, июнь 2020 – июнь 2021» компании «Ростелеком-Солар», второй наиболее вероятной точкой проникновения злоумышленников в корпоративную сеть являются системы удаленного доступа. Например, получение доступа через VPN-подключение с использованием ранее украденного пароля.

А самой распространенной веб-уязвимостью при тестировании защищенности российских компаний оказалась некорректная настройка прав доступа. Например, высокой степенью критичности была отмечена некорректная настройка прав доступа к API GraphQL. Доступ к программному интерфейсу позволил создать учетную запись с правами администратора и тем самым получить контроль над внешним приложением. Если бы это была реальная атака, то у злоумышленника в руках оказалась бы вся обрабатываемая в системе информация, а также функциональность конфигурирования системы и управления пользователями.

В связи с актуальностью проблемы нарушения прав доступа в корпоративные информационные системы эксперты «Ростелеком-Солар» подготовили данное исследование. Его результаты будут полезны как специалистам по информационной безопасности российских компаний, так и широкому кругу читателей, интересующихся проблематикой контроля и управления доступом и учетными данными в организациях.

4. Результаты исследования

4.1 Динамика нарушений доступа

В рамках данного исследования аналитики «Ростелеком-Солар» спросили представителей российских организаций, насколько часто их компании сталкиваются с нарушениями доступа в инфраструктуру. Результаты оказались неутешительными: **почти три четверти** компаний регистрируют случаи нарушений доступа достаточно часто – более 3 раз в год – либо очень часто (свыше 5 раз в год). Еще около **30%** организаций сталкиваются с такой проблемой не чаще 2 раз в год. При этом **ни один (!) участник опроса** не указал, что его компания не сталкивалась с подобными нарушениями.

Также участникам исследования был задан вопрос, выросло ли в российских компаниях за последний год количество нарушений, связанных с управлением доступом. Чуть менее **90%** (!) опрошенных признают, что число подобных происшествий в их компаниях в 2021 году выросло, причем **почти половина** из них утверждает, что **значительно**! Еще 10% респондентов полагает, что ситуация с такими нарушениями осталась на прежнем уровне.

4.2 Последствия нарушений доступа

Утечка конфиденциальной информации из компаний названа самым частым последствием, к которому приводят различного рода нарушения доступа в инфраструктуру организации – так полагает **более половины** опрошенных. Это неудивительно – конфиденциальные данные являются одним из наиболее дорогостоящих активов

современного бизнеса. Поэтому при проникновении в информационные системы организации злоумышленники почти всегда стремятся собрать побольше секретных данных, которые впоследствии можно выгодно продать.

Вторым по популярности негативным последствием нарушений доступа признана **временная недоступность информационных систем** компании – сайтов, клиентских сервисов и т. п. Действительно, практика «Ростелеком-Солар» в направлении защиты российского бизнеса от угроз несанкционированного доступа показывает: проникнув в сеть компании, злоумышленники нередко выводят из строя наиболее критичные бизнес-системы.

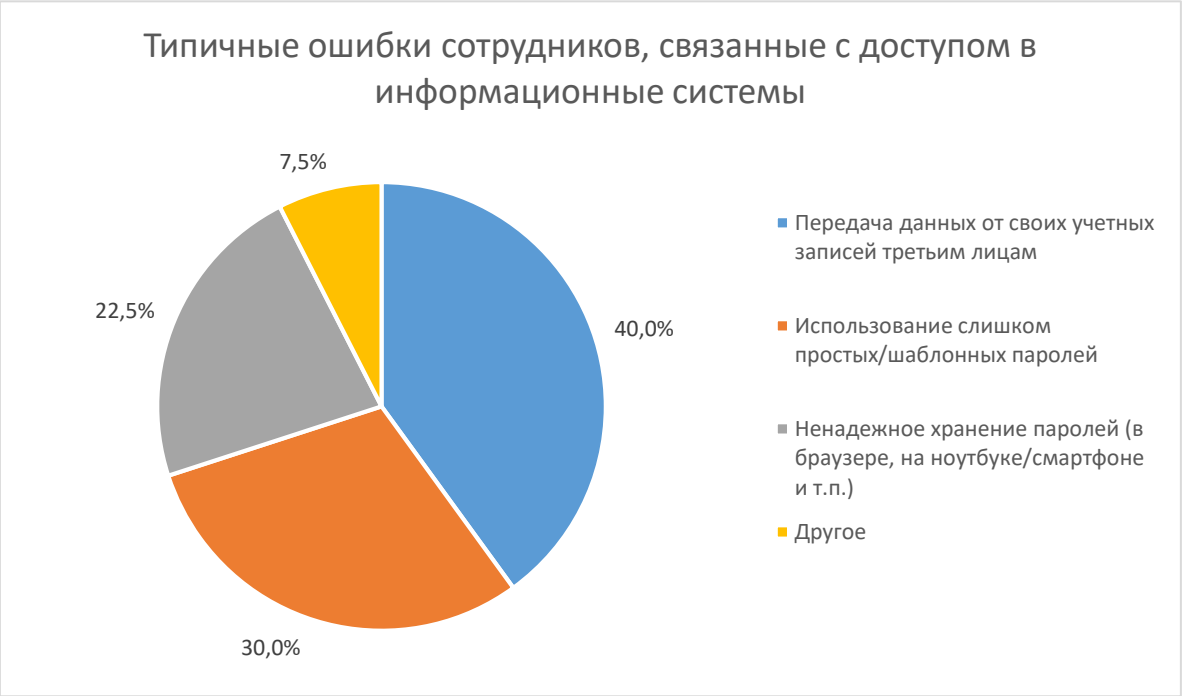
Особого внимания заслуживают несколько ответов респондентов, попавших в категорию «Другое». Так, некоторые отметили, что частым последствием нарушений доступа в инфраструктуру компаний является уничтожение ценных данных организации. Эксперты «Ростелеком-Солар» подтверждают – такая ситуация не редкость. Например, покинувший компанию обиженный сотрудник через незаблокированный доступ уничтожил важную информацию компании, а также исказил ряд данных, чтобы подвести бывшего руководителя. Или же действующий сотрудник из-за наличия избыточных прав доступа случайно удалил документ с важной информацией смежного подразделения.

Однако следует признать, бывают и организации, в которых проблематика информационной безопасности не является критически важной для ее существования. Скажем, завод по производству железобетонных конструкций скорее волнуют вопросы своевременного предоставления доступа, чтобы не создавались задержки в поставках. Представители именно такой категории компаний (отрасль – производство) при ответе на вопрос о том, каковы последствия нарушений доступа в сеть, указали вариант: «Как

правило, никакие, обычно информация дублируется на бумажных носителях и восстанавливается. Правда, необходимо потратить на это трудовые ресурсы».

4.3 Ошибки сотрудников при доступе в информационные системы

В целом самые частые ошибки корпоративных пользователей участники опроса связывают с банальным разгильдяйством. Сотрудники передают свои логины-пароли от внутренних систем компании коллегам, подрядчикам, друзьям, используют ненадежные пароли или небезопасно их хранят. Аналитики «Ростелеком-Солар» отмечают: эта проблема актуальна для всех компаний без исключения, и ее трудно изжить. Наиболее уязвимым звеном информационной безопасности является человеческий фактор – низкая ответственность людей и осведомленность в вопросах ИБ.



Здесь также стоит обратить внимание на ряд ответов в категории «Другое». Один из респондентов посетовал: некоторые сотрудники компании отключают антивирусы и запускают программы, добытые из сомнительных источников. Несмотря на то что речь идет о довольно крупной организации со штатом в диапазоне 500–1000 чел., такая вольница для сотрудников скорее характерна для небольших предприятий с незрелыми ИБ-процессами. В крупных и зрелых организациях автоматизированная политика безопасности не позволит сотрудникам совершить такие действия.

Если же к подобным мерам прибегают привилегированные пользователи, например сами ИТ-специалисты, то такая практика может довести компанию до беды. Скачиваемое из ненадежных источников ПО нередко содержит уязвимости, которые злоумышленники не

преминут использовать для проникновения во внутренний контур компании и кражи конфиденциальных данных. Возрастают риски утечек информации и заражения компьютеров вредоносным ПО, которые способны парализовать работу компании.

Похожий сценарий может развернуться и в случае, если сотрудники «не закрывают сессию после окончания работы» (еще один популярный ответ в категории «Другое»). Опять же если политикой безопасности не предусмотрена автоматическая блокировка экрана компьютера после окончания работы пользователя, а, скажем, главный бухгалтер не закрыл сессию, то сотрудник-злоумышленник может этим воспользоваться и провести от его имени какую-либо сомнительную операцию.

При этом почти **38%** участников исследования считают, что снизить число нарушений доступа со стороны сотрудников поможет лишь применение автоматизированных средств управления доступом, включающих предварительно настроенные политики безопасного доступа. Немногим менее **28%** опрошенных являются сторонниками введения в компаниях жестких мер безопасности при работе с учетными данными пользователей, а именно принудительного использования сложных паролей, многофакторной аутентификации, автоматического блокирования «учеток» отсутствующих сотрудников и т. п. За регулярное обучение и аттестацию сотрудников по правилам доступа в информационные системы выступают еще **20%** респондентов.

Примечателен подход, озвученный представителем крупной (свыше 1000 сотрудников) производственной компании, расположенной в Южном федеральном округе. В этой компании применяются меры наказания за нарушения правил безопасного доступа в информационные системы: лишение премии или бонусов, а также занесение нарушений в личное дело сотрудника. По наблюдениям экспертов «Ростелеком-Солар»в ее компаниях-заказчиках, наказание рублем является очень действенной мерой соблюдения правил информационной безопасности.

4.4 Незаблокированные «учетки» ушедших сотрудников – дыра в безопасности компаний

Несмотря на то что почти **43%** представителей компаний утверждают, что все учетные данные сотрудников, уволившихся из компании, сразу же автоматически блокируются, ситуация с незаблокированными «учетками» не выглядит обнадеживающе.

Дело в том, что **ровно такой же процент** респондентов признает: в компаниях либо блокируются не все «учетки», а только те, о которых вспомнили (оформили заявку), либо автоматической блокировкой охвачены не все информационные системы. А это значит, что в обоих случаях уволившиеся уносят с собой действующую «учетку», доступ к которой

может оставаться незаблокированным месяцами! А еще почти **8%** опрошенных откровенно заявляют: в их компаниях доступы ушедших сотрудников остаются незаблокированными.

Такие ситуации не редкость не только в небольших заурядных компаниях, но и, например, в крупных российских организациях банковской сферы! Также этим, как ни странно, страдают даже крупные предприятия ИТ-сферы, хотя их уровень зрелости в части информационной безопасности вроде бы должен быть высоким.

В категории «Другое» примечателен ответ «Блокировка доступа вручную после получения выгрузки по принятым и уволенным сотрудникам». Такой подход может быть эффективным только при высокой частоте выгрузки, как минимум ежедневной. Если же данные актуализируются, скажем, раз в неделю, в этом случае риски несанкционированного доступа значительно возрастают.

Бывают ситуации, особенно в крупных компаниях, когда сотрудников очень много и учетных записей на всех не хватает. Тогда при увольнении работника его доступ передается другому сотруднику – происходит перерегистрация ID на другое лицо. Похоже, именно такая практика реализована у одного из участников исследования – крупного (свыше 1000 чел. в штате) столичного предприятия сферы ВПК.

Такой сценарий управления доступом допустим при условии, что данные обо всех действиях с «учеткой» логируются. Зная, когда и на основании чего произошла перерегистрация, вплоть до минут и секунд, можно будет понять, от чьего имени происходили операции в ИТ-системе. При этом все же хорошей практикой для обеспечения дополнительной безопасности является передача учетной записи через

блокировку/разблокировку и введение моратория на использование данного ID в течение нескольких месяцев.

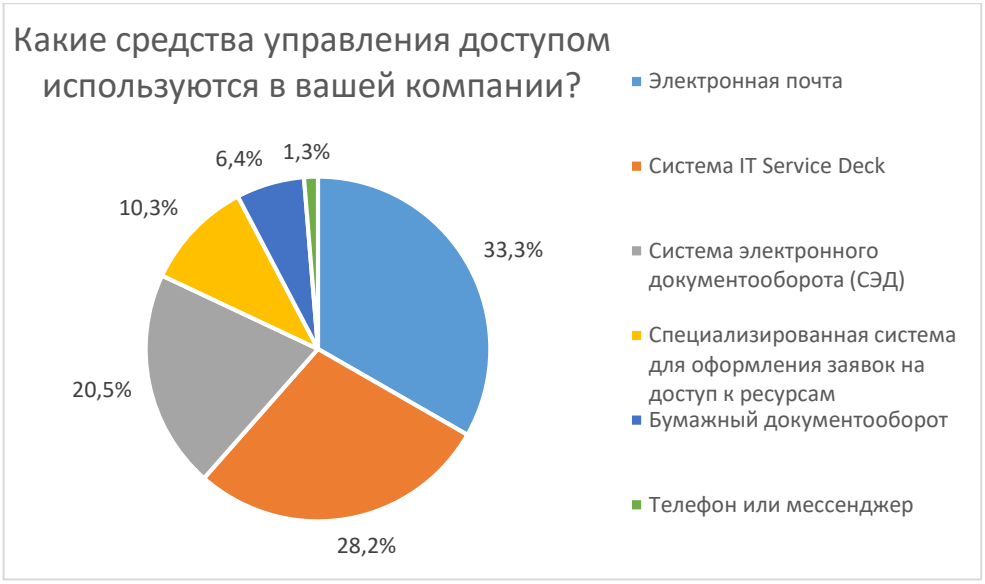
4.5 Инструменты управления доступом в компаниях

Как видно на диаграмме ниже, лишь чуть более **10%** компаний применяют специализированные системы для создания заявок на доступ к ресурсам компании и управления этим доступом. То есть системы, в которых заложены правила предоставления и ограничения доступа пользователей к ИТ-ресурсам компании и которые автоматизируют этот процесс, а значит, максимально снижают риски со стороны человеческого фактора (ошибки, злонамеренные действия и т. п.).

Электронная почта является самым популярным способом создать и выполнить заявку на предоставление доступа к ресурсам в российских компаниях – ею пользуется более **33%** опрошенных. **Почти половина** компаний использует для управления доступом системы электронного документооборота и IT Service Desk. Следует отметить, что применение только этих систем свидетельствует не о полной автоматизации, а лишь об автоматизации в части оформления и согласования заявок на доступ. При этом выдача прав непосредственно в ИТ-системах остается в ручном режиме, а значит, сохраняются риски, связанные с человеческим фактором, – ошибками, злоупотреблениями и т. п.

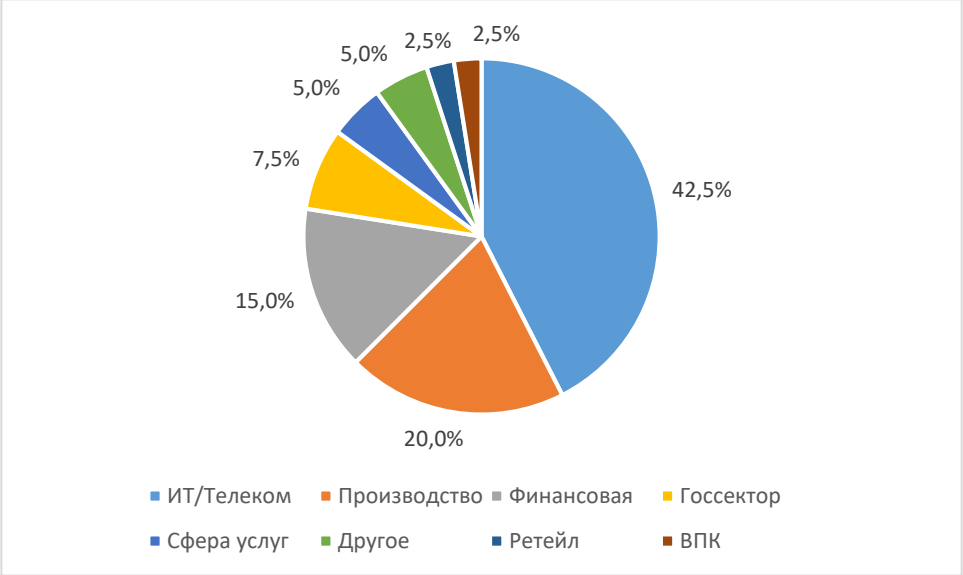
Более 6% компаний продолжают жить в прошлом веке и выдают разрешение на доступ по бумажной заявке, со всеми вытекающими последствиями: очередями на доступ, длительными задержками в предоставлении прав (тормоз для бизнеса), перегрузкой ИТ-специалистов (как следствие, появление ошибок и рост рисков несанкционированного доступа).

Чуть более 1% компаний, наоборот, используют для решения этой задачи очень оперативные, но весьма ненадежные инструменты: различные мессенджеры (их защищенность под большим вопросом, утечки данных из мессенджеров у всех на слуху) и телефонные звонки. Что касается телефонных звонков, этот способ выдачи доступа вообще не выдерживает критики. По телефону невозможно на 100% идентифицировать звонившего – и здесь сразу обнаруживается большая уязвимость. В случае возникновения инцидента или, того хуже, расследования уголовного дела, телефонный звонок невозможно будет приложить в качестве доказательства, подтверждения и обоснования выдачи прав доступа. Неудивительно, что использование подобных инструментов отмечено в небольших региональных компаниях сферы услуг, чей уровень зрелости ИБ, очевидно, далек от удовлетворительного.

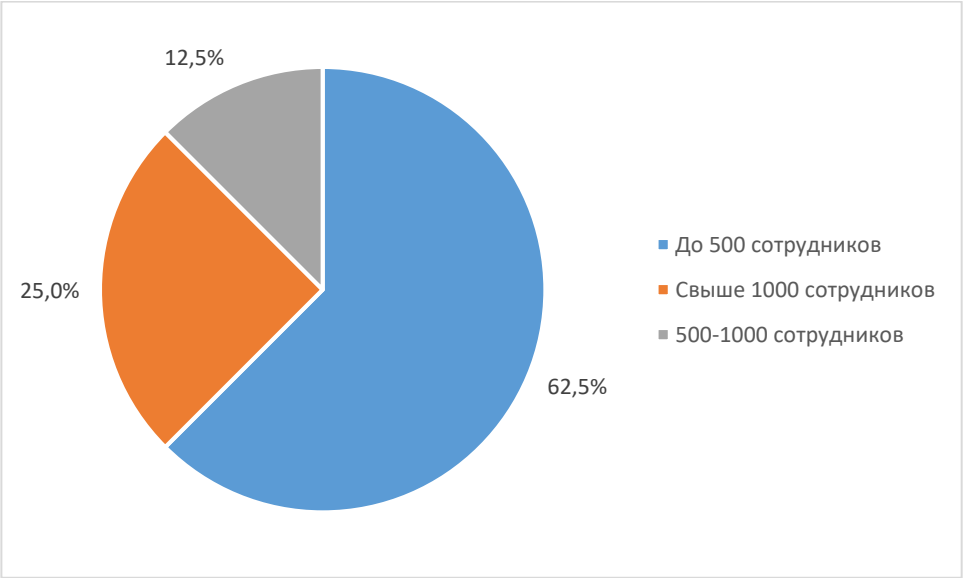

Какие средства управления доступом используются в вашей компании?
33,3%
28,2%
20,5%
10,3%
6,4%
1,3%
Электронная почта
Система IT Service Deck
Система электронного документооборота (СЭД)
Специализированная система для оформления заявок на доступ к ресурсам
Бумажный документооборот
Телефон или мессенджер

5. Данные об участниках исследования

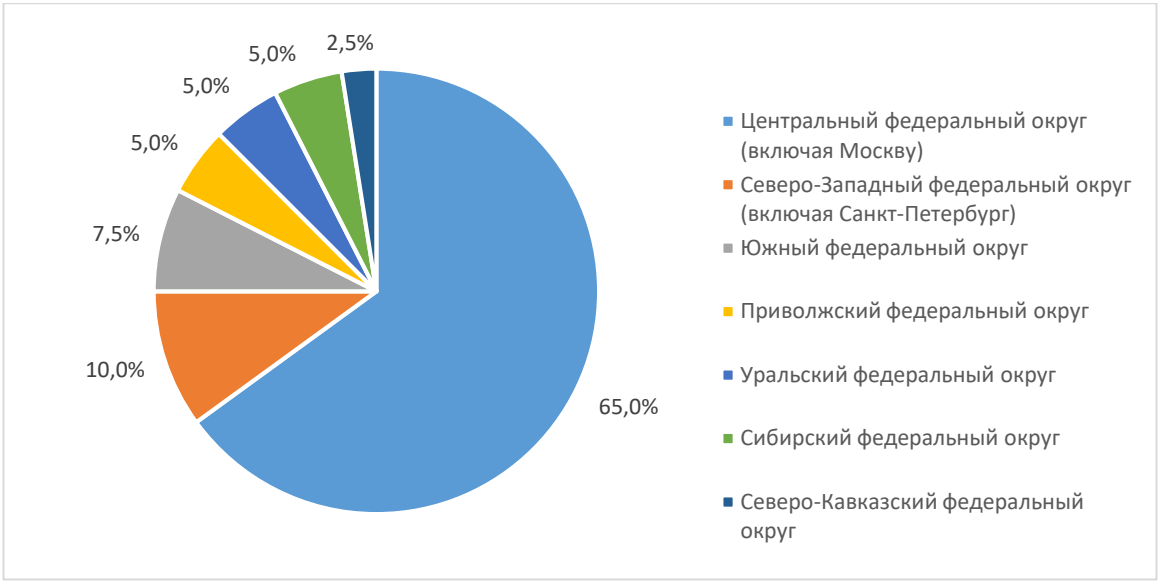
5.1 Отраслевое распределение компаний



5.2 Распределение компаний по размеру



5.3 Региональное распределение компаний


2,5%
5,0%
5,0%
5,0%
7,5%
10,0%
65,0%
Центральный федеральный округ (включая Москву)
Северо-Западный федеральный округ (включая Санкт-Петербург)
Южный федеральный округ
Приволжский федеральный округ
Уральский федеральный округ
Сибирский федеральный округ
Северо-Кавказский федеральный округ

6. Выводы

Компания «Ростелеком-Солар» подвела итоги исследования «Нарушения в части управления доступом в российских компаниях». Исследование выявило, что более 70% российских компаний часто сталкиваются с нарушениями доступа в свои информационные системы. Почти 90% участников исследования отмечают, что количество подобных происшествий в компаниях за последний год выросло. Очевидно, что проблема обеспечения безопасного доступа стоит в отечественных компаниях очень остро и нуждается в скорейшем и эффективном решении.

В процессе исследования более половины респондентов подчеркнули, что наиболее частым негативным последствием наршений доступа для компаний становятся утечки конфиденциальной информации. Этот вид ИБ-угрозы наряду с хакерской атакой является одним из самых вредоносных для компании. Ведь конфиденциальная информация – клиентские базы данных, детали секретных разработок, тендерная документация – самый ценный актив большинства современных организаций. Утечка этих данных грозит серьезным финансовым ущербом, в некоторых случаях вплоть до потери бизнеса.

Кроме того, исследование зафиксировало, что большинство нарушений сотрудниками прав доступа в информационные системы связано с небрежным или халатным отношением к вопросам информационной безопасности и низкой ИБ-грамотностью сотрудников. Это и передача учетных данных от внутренних систем компании третьим лицам, и применение ненадежных паролей, и небезопасное их хранение. Данную проблему решить непросто – единственным перспективным направлением здесь видится использование специализированных систем автоматизированного управления доступом с применением многофакторной аутентификации, биометрии и тому подобных передовых технологий.

Огромной дырой в безопасности компаний остается отсутствие автоматической блокировки учетных данных сотрудников после их увольнения. В половине компаний такие доступы либо блокируются неполностью, либо не блокируются вовсе. Успешно решить проблему, в особенности в крупных организациях, возможно лишь при условии внедрения систем автоматизированного управления доступом.

Контактная информация

Телефоны:

+7 (499) 755-07-70 – продажи и общие вопросы

+7 (499) 755-02-20 – техническая поддержка

E-mail:

info@rt-solar.ru

support@rt-solar.ru

Адреса:

125009, Москва, Никитский пер., 7, стр. 1

127015, Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд