

Информационная безопасность в компании: как защищать конфиденциальную информацию

Полезные материалы из системы:

1. [Статья: Защита информации \(Подготовлен для системы КонсультантПлюс, 2023\) {КонсультантПлюс}](#)
2. [Готовое решение: Как организации защитить конфиденциальную информацию \(КонсультантПлюс, 2023\) {КонсультантПлюс}](#)
3. [Готовое решение: Как учреждению защитить свою конфиденциальную информацию \(КонсультантПлюс, 2023\) {КонсультантПлюс}](#)

Согласно **ч. 4 ст. 6** Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее - Закон об информации) обладатель информации обязан принимать меры по ее защите. К числу таких мер относятся правовые, организационные и технические.

Для защиты конфиденциальной информации нужно принять ряд мер как внутри организации, так и в отношениях с контрагентами.

Чтобы не допустить разглашения внутри организации, разработайте локальные акты, установите порядок обращения с информацией, назначьте ответственных лиц. Конкретный перечень мер зависит от того, какую информацию вы защищаете - персональные данные или коммерческую тайну.

Чтобы обязать контрагента не разглашать конфиденциальную информацию, заключите с ним соответствующее соглашение. Включите в него штраф за разглашение, чтобы не пришлось доказывать размер убытков. Обязательно фиксируйте факты передачи контрагенту документов, содержащих секретные сведения.

Тщательная разработка правил информационной безопасности для офиса и производства частично способны снизить степень риска. Обучение сотрудников основам производства частично способны снизить степень риска. Обучение сотрудников основам информационной безопасности проводят даже на АЭС, где персонал априори должен быть подготовлен к неожиданностям. Все это говорит о первоочередной необходимости

информирования сотрудников и регламентации их поведения при работе с защищаемыми информационными массивами и объектами сетевой инфраструктуры.

Правила ИБ в офисе

Правила информационной безопасности для офиса не самые сложные, но степень ответственности сотрудников не всегда гарантирует их безусловное выполнение. Это значит, что внедрение правил должно сопровождаться мотивационными мерами, стимулирующими их выполнение, и депремированием, дисциплинарной ответственностью в случае невыполнения.

Информирование

Первым правилом ИБ в офисе должно стать информирование сотрудников. Инсайдерские утечки данных не менее опасны, чем внешние нападения. Менеджеры по продажам, увольняясь, уносят с собой базы данных клиентов, а сотрудники мобильных операторов с легкостью торгуют детализацией телефонных разговоров абонентов. О размере риска говорит объем рынка даркнета, измеряемый сотнями миллионов долларов в год только для российских ресурсов.

Всем пользователям корпоративной системы должны быть известны простые правила безопасности:

- использовать и периодически менять сложные пароли, никогда не передавать средства идентификации – пароль и логин – другим сотрудникам;
- не хранить в «облаках» конфиденциальную информацию, даже если нужно поработать с годовым отчетом из дома;
- уничтожать ненужные документы в шредере;
- не передавать информацию без официального запроса;
- не смешивать корпоративную и личную почту;
- архивировать важные файлы;
- блокировать компьютер перед уходом с рабочего места;
- уметь распознавать фишинговые письма;
- ознакомиться с практиками социальной инженерии и не поддаваться им.

Тестирование в игровой форме на знание правил информационной безопасности на предприятии позволит превратить теоретические сведения в сложившиеся навыки. Вторым важным способом поддержания необходимого уровня информационной безопасности в офисе станет контроль доступа.

Контроль доступа

Это решение реализуется на физическом, аппаратном и программном уровнях. Действует правило: никто не должен иметь больше привилегий, чем допускается его должностной инструкцией. Юристу не нужен доступ к бухгалтерским программам, а программисту – к чату руководства. Системные администраторы должны реализовать дифференцированную модель доступа, назначив каждому пользователю и группе пользователей роль, при которой доступными ему окажутся только определенные файлы и ресурсы. То же относится к правам администраторов.

Комплексный подход

Это правило должно стать незыблемым для системных администраторов и разработчиков структур информационной безопасности. Невозможно устранять уязвимости и недочеты частичными решениями, латая прорехи одну за другой до тех пор, пока администрирование системы станет невозможным. Необходимо с самого начала выстраивать ИБ как единую систему с учетом возможностей ее роста и прогнозированием направлений дальнейшего развития. Система должна включать единый комплекс организационных, технических и программных средств и контролироваться как единое целое.

Правила ИБ при работе на удаленном доступе к сети

Самостоятельной проблемой становится регламентация работы сотрудников на удаленном доступе. Современному бизнесу присуще стремление к минимизации затрат, на компанию могут работать сотни разработчиков и программистов, находящихся в разных странах и на одной виртуальной площадке занимающихся разработкой программного обеспечения. Такое размывание периметра информационной безопасности очень опасно, так как конкуренты всерьез заинтересованы в несанкционированном доступе к новым разработкам. Кроме того, во многих компаниях даже штатные сотрудники зачастую работают на удаленном доступе, находясь в командировке или в отпуске.

Существуют правила, позволяющие сделать такие удаленные рабочие отношения максимально безопасными:

- исключить возможность использования удаленными сотрудниками для подсоединения к корпоративной сети открытых Wi-Fi-сетей, в которых возможен перехват трафика;

- домашние сети сотрудников должны быть защищены паролями и шифрованием как минимум уровня WPA2. В компании необходимо разработать правила информационной безопасности для удаленных сотрудников для защиты домашних сетей;
- подключение для мобильных устройств к корпоративной сети должно происходить только по каналам VPN. Компании желательно самой выбрать надежного поставщика услуг VPN и обеспечить сотрудникам на удаленном доступе возможность работать с этим сервисом;
- для работы необходимо иметь отдельное мобильное устройство и не смешивать частную и корпоративную информацию, система ИБ компании должна предусматривать меры защиты таких удаленных устройств;
- сведения о работе на удаленном доступе не должны публиковаться в социальных сетях, чтобы не вызвать интерес злоумышленников. Устное и письменное разглашение конфиденциальных данных недопустимо;
- пароли на ресурсах, связанных с работой на удаленном доступе, необходимо регулярно менять;
- плагины и программное обеспечение, содержащие известные хакерам уязвимости (например, Adobe Flash, Acrobat Reader, Java и другие), должны регулярно обновляться;
- компьютер и мобильные устройства нужно защищать паролем даже дома, чтобы гость или ремонтный рабочий не смогли похитить или случайно повредить данные.

Эти правила необходимо оговаривать с каждым работником на удаленном доступе на первом этапе сотрудничества. От компании требуется организовать собственную систему мер, позволяющую обезопасить работу с любым сотрудником на удаленном доступе, штатным или внештатным:

- внедрить механизм аутентификации пользователей (пароли, аппаратные средства-токены, биометрические данные);
- организовать единую систему управления доступом (централизованное управление доступом к IT-ресурсам компании);
- системно использовать средство организации собственных протоколов VPN (аппаратные устройства, программные решения, расширения брандмауэра);
- внедрить средства противостояния атакам (защита внутренней сети и сотрудников от атак).

Программа защиты удаленного доступа актуальна и для информационной безопасности на производстве, где многие объекты управляются по каналам беспроводной связи.

Правила информационной безопасности приобретают особую актуальность, когда касаются производства и автоматизированных систем управления (АСУ ТП). Системы управления отвечают за работу таких объектов, как доменные, прокатные станы, гидроэлектростанции. Любое внешнее вмешательство в их информационную инфраструктуру способно вызвать аварии и человеческие жертвы. Поэтому требования к ИБ АСУ строятся на собственных принципах, отличных от принципов управления информационными системами в целом. Угрозы таким системам могут исходить от террористических группировок, в том числе исламской направленности. Прямого корыстного интереса у обычных хакеров к ним не возникает. Такие системы часто поражаются специально созданными вирусами, направленными на вывод из строя объектов промышленной инфраструктуры и использующих уязвимости в классических информационных системах.

АСУ ТП требует наивысшей степени защиты в тех отраслях, аварии в которых способны причинить ущерб наибольшему количеству людей и имущества:

- электроэнергетика;
- предприятия топливно-энергетического комплекса;
- транспорт;
- металлургия;
- машиностроение.

Основной проблемой создания системы ИБ становится то, что использование современных программных решений может навредить общей надежности системы, поэтому часто основной задачей становится максимальное ограждение АСУ от контактов с внешним миром по любым типам подключений, в том числе установка межсетевых экранов и создание демилитаризованных зон на границах с офисными сетями.

Регламенты создания системы информационной безопасности АСУ ИП утверждены в виде международных стандартов и российских ГОСТов. В качестве одного из основополагающих документов эту сферу регулирует [Приказ ФСТЭК РФ № 31](#).

При разработке правил информационной безопасности промышленного производства применительно к АСУ надо учитывать, что система имеет три уровня управления:

- уровень операторского (диспетчерского) управления (верхний уровень);
- уровень автоматического управления (средний уровень);
- уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень).

Объектами защиты для АСУ, согласно нормам [Приказа № 31](#), являются:

- информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);
- программно-технический комплекс, включающий технические средства (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации.

Защита этих объектов возможна только на основе комплексного подхода, предусматривающего:

- систематический аудит степени АСУ ТП путем интервьюирования специалистов организации, изучения проектной документации, анализа структуры и архитектуры информационных систем;
- организацию технического анализа защищенности для нахождения уязвимостей при помощи программ-сканеров;
- ручной и программный анализ рисков;
- выявление и мониторинг новых типов угроз, представляющих опасность для функционирования объекта.

Стандартная архитектура АСУ ТП обычно не предполагает наличия большого количества ресурсов для размещения программ, отвечающих за безопасность. Предполагается использование только двух типов – систем мониторинга активности и обнаружения угроз и систем предотвращения угроз, подразумевающих управление доступом.

Системы мониторинга активности и обнаружения угроз

Наибольшие риски для АСУ ТП несут сотрудники-инсайдеры, допущенные к управлению и использующие съемные устройства, которые могут быть заражены вирусом. Но если система подключена к офисной, возможны внешние риски. Системы мониторинга ограничены в функционале, они не допущены к процессам управления АСУ ТП и не могут блокировать действия пользователей. Они способны только отслеживать всплески подозрительной активности и уведомлять о них по заданному алгоритму. Их функции:

- обнаружение внешних атак и аномалий в поведении элементов сети;
- мониторинг инцидентов информационной безопасности;
- пассивный анализ уязвимостей;
- анализ конфигураций оборудования, правил доступа сетевого оборудования;

- контроль целостности данных и программного обеспечения.

Системы анализируют сетевые потоки, выявляют аномалии и неизвестные IP-адреса, атаки на не запротоколированные ранее уязвимости.

Системы предотвращения угроз

Эти программные средства носят проактивный характер: они не только информируют, но и действуют. В основном они управляют доступом пользователей, имея полномочия на блокировку неавторизованных действий. В случае неопределенной транзакции они вправе запросить ее авторизацию у руководителя более высокого уровня и в его отсутствие блокируют операцию.

Ответственность за нарушение правил ИБ

Компания может применять к сотруднику за нарушение правил информационной безопасности меры дисциплинарной ответственности. Это замечание, выговор, иногда увольнение. Серьезным стимулом скрупулезно выполнять правила является депремирование. Решение о привлечении к ответственности принимает руководитель организации по представлению непосредственного начальника виновника. При выборе меры ответственности нужно предполагать, что нарушения правил информационной безопасности могут носить пассивный и активный характер.

Пассивные:

- получение информации нарушителем для использования в своих целях;
- анализ характеристик информации без доступа к самой информации.

Активные:

- изменение информации;
- внесение ложной информации;
- нарушение (разрушение) информации;
- нарушение работоспособности системы обработки информации.

Активные нарушения несут больше опасности для бизнеса и говорят о более высокой степени вины нарушителя, они должны наказываться строже. Иногда от мер корпоративной ответственности приходится переходить к гражданско-правовой, подав на нарушителя в суд с требованием о возмещении ущерба или заявление в правоохранительные органы о возбуждении уголовного дела. Утрата или намеренное разглашение конфиденциальной информации могут стать основанием для взыскания с виновника ущерба, и его размер может достигать миллионов рублей.

Целесообразным решением становится периодическое проведение проверок подразделений компании с целью определения степени выполнения правил безопасности всеми пользователями – от наладчика оборудования до генерального директора. Менеджеры чаще пренебрегают правилами, именно поэтому они являются основными источниками угроз. Результаты проверки могут стать основой для служебных расследований или переаттестации по профессиональной пригодности, поэтому они имеют дополнительный дисциплинирующий характер.

Вне зависимости от того, в каких условиях работают правила информационной безопасности предприятия, они должны соблюдаться неукоснительно. Только это приведет к тому уровню ИБ, который позволит избежать ущерба и аварий.