7. Клебанович, Н.В. Химическая мелиорация почв: практикум для студентов географического факультета / Н.В. Клебанович. – Минск: БГУ, 2018. – 47 с.

8. Пат. RU 2551569 C1. Косилка-измельчитель сидеральных культур/И. М. Курочкин, А. И. Кадомцев. – № 2014103380; заявл. 31.01.2014; опубл. 27.05.2015, Бюл. № 15.

9. Курочкин, И.М. Косилка-измельчитель сидеральных культур с наклонными роторами / И.М. Курочкин, А.И. Кадомцев.– Сельский механизатор. – 2016. – №6. – С.40.

10.Анализ кинематических схем погрузочного оборудования одноковшовых фронтальных погрузчиков / А.Н. Смирнов [и др.] // Техническое и кадровое обеспечение инновационных технологий в сельском хозяйстве : материалы Международной научно-практической конференции, Минск, 24–25 октября, 2019 г. : в 2 ч. Ч. 1. – Минск : БГАТУ, 2019. – С. 270–271.

УДК 004.056

ЗАЩИТА ИНФОРМАЦИИ В СЕТИ

Острый М.А. – 7 мпт, 3 курс, АМФ
Толочко А.А. – 7 мпт, 3 курс, АМФ
Научный руководитель: ст. преподаватель Подашевская Е.И.
УО «Белорусский государственный аграрный технический университет», г. Минск, Республика Беларусь

Каждому человеку нужны средства защиты информации в интернете, поскольку похищение или получение доступа к личным данным посторонними лицами может вызвать самые разные последствия. К примеру, распространены случаи построения фиктивной личности, занимающейся криминальной деятельностью в интернете и постоянно оперирующую идентификационной информацией другого индивидуума.

Еще одна опасность – намеренное нанесение ущерба репутации, материальных потерь путем продажи личной недвижимости, оформления кредитов и так далее.

Поэтому защита личной информации в интернете сегодня регламентируется законодательными актами.

Однако больше всего система защиты информации в интернете нужна производственным и коммерческим компаниям, поскольку

при несанкционированном доступе к данным, их похищении, намеренном изменении могут происходить самые разнообразные опасные случаи.

1. Нанесение ущерба качеству товара в результате изменения ключевых параметров процесса производства или исходного сырья.

2. Нарушение взятых на себя обязательств вследствие нарушения логистики поставок, изменения качества, срывов договорных сроков.

3. Прямой ущерб вследствие промышленного шпионажа, прямой продажи разработок конкурентам.

4. Косвенный ущерб из-за раскрытия планов развития и других стратегических данных.

5. Комплексный ущерб при краже, шифровании данных с целью шантажа, вымогательства, что ведет к прямым финансовым потерям, чревато последствиями промышленного шпионажа, нарушения рабочих процессов и многим другим.

Конкретный список принимаемых мер и выбранные технологии защиты информации в сетях интернет зависит от множества факторов.

Это может быть характер информации, методика ее разделения и хранения, формат используемых технических средств и многое другое. Однако на практике все решения условно формализуются и делятся на крупные категории.

1. Аппаратные средства. Они применяются на всех организационных уровнях. Однако особенно важно правильно организовать хранение информации.

Задача аппаратных средств при этом:

· обеспечивать нужную скорость доступа к данным;

· гарантировать надлежащую скорость систем проведения расчетов;

· обеспечивать целостность данных и гарантию их сохранения при выходе из строя отдельных средств хранения;

· организовывать резервное копирование, быстрое восстановление информации при сбоях;

· обеспечивать взаимодействие со средствами связи;

· реагировать и минимизировать ущерб при аварийных ситуациях (пожар, затопление);

· сохранять работоспособность основного оборудования во время отключения основного источника энергии (генераторы, источники бесперебойного питания).

· обрабатывать запросы подключенных пользователей.

2. Программные. Область программных средств – самая обширная. Выбор конкретного списка пакетов зависит от используемых платформ и операционных систем, принятых механик доступа.

Среднестатистический список защитных мер включает:

· систему обнаружения сетевых атак и попыток несанкционированного доступа на узел в составе программно управляемого оборудования;

· комплексы шифрования (программные или аппаратные);

· средства подтверждения подлинности, электронные ключи и системы для работы с ними;

· средства управления доступом, которые могут включать и аппаратные средства.

На практике, правильно выбранный комплекс программных средств может практически исключить прямую атаку на хранилище или отдельный узел системы обработки данных.

3. Смешанные меры защиты разрабатываются для сети хранения и обработки в том случае, когда характер действий с данными отличается для разных групп пользователей.

В перечень используемых средств могут входить программные комплексы на отдельных рабочих местах, системы разделения прав и уровней доступа в пределах одного сектора и общей структуры ответственности. Популярно применение различных схем взаимодействия исполнителей между собой, а также – методики контроля и мониторинга.

К простейшему случаю смешанных мер защиты можно отнести обязательное использование антивирусов, стандартных шифрованных протоколов передачи, системы идентификации (в том числе – аппаратной) с разноуровневым доступом к работе с информацией.

4. Организационные.К ним относится разработка оптимальных схем взаимодействия персонала с информацией и обществом. Сюда относится:

· разработка инструкций, предписаний, четких схем работы с данными для занятого персонала;

· предоставление персоналу ограниченного набора сертифицированных, надежных программных средств;

· обязательное применение принципов ответственности за разглашение конфиденциальной информации;

· разделение зон ответственности каждой трудовой единицы, ранжирование областей доступных данных, формулировка объема доступных действий;

· создание средств для предотвращения случайного, умышленного удаления информации;

· применение программных средств, полностью исключающих прямой доступ к данным;

· формулирование в виде инструкций, правил действия сотрудников, охраны – системы работы с внутренними носителями информации, регламенты выноса документации;

· применение средств проверки и подтверждения подлинности (электронные ключи).

Используя открытую, общедоступную сеть вайфай, можно запросто подхватить вредоносное ПО или потерять личные данные.

Перед тем как подключиться к открытой точке доступа, пользователю придется пройти стандартную процедуру регистрации. Обычно нужно ввести электронную почту или номер телефона в обмен на интернет. Перед этим открывается соглашение, которое нужно внимательно прочитать, чтобы удостовериться, что провайдер собирает личную информацию не для мошенничества. Нередко данные, которые вносятся для пользования вайфай, передаются службам и компаниям, использующим личную информацию для массовой рассылки спама.

Не рекомендуется скачивать и устанавливать программы из сомнительных источников. Регулярно нужно обновлять программное обеспечение и антивирус. Для каждого сайта рекомендуется использовать свой отдельный пароль. В случае утечки мошенник получит доступ только к одному аккаунту, а не ко всем сразу.

Стоит помнить: все знаменитые хакеры получали доступ к данным путем работы с людьми и использования их ошибок.

Поэтому не стоит стесняться того, что на предприятии в целях безопасности до предела ограничивается свобода персонала.

Все, что может предотвратить утечки, а также разделение доступа и ответственности способно помочь сохранить важные данные и избежать серьезных неприятностей.

Список использованных источников

1. Быков, В.Л. Информатика : учебно-методическое пособие для студентов вузов группы специальностей 74 06 "Агроинженерия" / В.Л. Быков, Н.Г. Серебрякова ; Минсельхозпрод РБ, УО БГАТУ, Кафедра прикладной информатики. – Минск : БГАТУ, 2013. – 656 с.

2. Серебрякова, Н.Г. Основы информационных технологий: пособие для студентов учреждений высшего образования группы специальностей 74 80 Научная и педагогическая деятельность / Н.Г. Серебрякова, О.Л. Сапун, Р.И. Фурунжиев ; Минсельхозпрод РБ, УО «БГАТУ». – Минск : БГАТУ, 2015. – 400 с.

3. Серебрякова, Н.Г. Методы системного анализа и компьютерного моделирования образовательных стратегий / Н.Г. Серебрякова, К. Б. Азарко // Научный поиск и инновационные преобразования в агропромышленном комплексе : сборник научных статей. - Минск : БГАТУ, 2009. – С. 221–225.

4. Особенности внедрения технологии точного земледелия / Е. В. Галушко [и др.] // Техническое обеспечение инновационных технологий в сельском хозяйстве: сборник научных статей Международной научно-практической конференции, Минск, 21-23 ноября 2018 г. – Минск : БГАТУ, 2018. – С. 44–53.

5. Серебрякова, Н.Г. Современные концепции инженерного образования: анализ в рамках компетентностного подхода / Н.Г. Серебрякова// Вышэйшая школа. – 2017. – № 6. – С. 23–27.