КИБЕРБЕЗОПАСНОСТЬ
НАШИ ДНИ
Промышленные технологии

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЧЕРА, СЕГОДНЯ, ЗАВТРА.

Комитет по информационной безопасности
Ассоциации банков России
Сергей Пазизин

#uralcyber

Причем здесь банки

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Общее, и отличия банковской ИБ и ИБ в промышленности.

Различия в мотивации киберпреступников, степени. защищенности и рисках ИБ.

Этапы развития.

ИБ часть ИТ (IT SECURITY)

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

При появлении первых многопользовательских АС необходимо было решать задачи:

- распределения памяти и вычислительных ресурсов между пользователями;
- исключения несанкционированного вмешательства в управление АС (защита от «дурака» и «продвинутого» пользователя);
- обеспечения устойчивости к вандализму.

Средства защиты (встроенные функции аутентификации, разграничения прав доступа, ведения логов) являлись частью АС и находились под управлением ИТ-подразделения.

Безопасность воспринималась как составляющая правильного функционирования АС.

ИБ часть контроля (INFORMATION SECURITY)

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Изменения конца 20-го века, начала 21-го:

- появление возможности монетизации взломов (прямой вывод финансовых средств, шантаж, выполнение стороннего заказа на хищение данных или DDOS-атаку);
- расширение круга пользователей, а следом и потенциальных злоумышленников, за счет каналов дистанционного доступа;
- осознание требований безопасности как ограничений на функциональность, процессы разработки и эксплуатации АС.

Следствия:

- формирование профессиональной киберпреступности;
- появление и развитие стандартов ИБ, обязательных к исполнению регуляторных документов;
- разработка специфических средства защиты информации (антивирусы, межсетевые экраны, прокси-сервера);
- создание подразделений ИБ, выполняющих административно-контрольные функции (обеспечение выполнения внутренних и внешних стандартов безопасности, согласование документации и прав доступа).

ИБ часть бизнес-процессов (DIGITAL SECURITY)

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Текущие процессы:

- рост электронной коммерции;
- переход к дистанционному предоставлению финансовых и государственных услуг;
- развитие электронного документооборота и необходимость обмена данными в реальном времени между организациями;
- цифровизация становится одним из основных факторов конкурентоспособности;
- обеспечение работоспособности АС, целостности и конфиденциальности обрабатываемых данных становится жизненно важным для любой организации;
- киберпреступность оформляется в высокопрофессиональные сообщества с миллиардными оборотами, развитой специализацией и сформированным рынком преступных услуг, выявление и использование слабых мест во внедряемых бизнес-процессах ставится на поток;
- происходит ужесточение нормативных требований по обеспечению ИБ и одновременное расширение области регулирования.

ИБ часть бизнес-процессов (DIGITAL SECURITY)

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

В современных условиях:

- практически любое бизнес или ИТ-решение должно приниматься с учетом необходимости обеспечения ИБ;
- ИБ должна сопровождать внедрение новых сервисов с момента постановки задачи, участвовать в проектировании, разработке, внедрении и сопровождении соответствующих АС;
- в связи с высокой конкуренцией решения необходимо принимать в кратчайшие сроки;
- сложность и разнообразие решаемых задач не позволяют свести процесс обеспечения ИБ к «механическому» соблюдению установленных правил;
- нарушение баланса между безопасностью и возможностью развития бизнеса в любую из сторон приводит к потере конкурентоспособности;
- модель взаимодействия, в которой ИБ устанавливает правила, а затем только контролирует их исполнение – становится тормозом развития бизнеса.

Возможности аутсорсинга ИБ

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Области применения:

- привлечение профильных специалистов для внедрения и настройки приобретаемых средств защиты;
- проведение тестов на проникновение, помощь в противодействии атакам, проведение расследований по взломам;
- обработка инцидентов.

Ограничения:

- недостаток полномочий у внешних сотрудников;
- наличие ограничений по доступу к коммерческой, банковской тайне и персональным данным, обрабатываемым в организации;
- недостаточность знания внутренних процессов компании;
- сложность решения вопросов разграничения ответственности и страхования рисков.

Аутсорсинг ИТ+ИБ при переходе к облачным решениям

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Преимущества облачных вычислений:

- рациональное использование оборудования в условиях неравномерной загрузки;
- быстрота получения услуги;
- экономия на капитальных вложениях;
- сокращение расходов на поддержку.

Для небольших и средних компаний использование внешних облачных платформ это также возможность обеспечить необходимый уровень киберустойчивости при условии:

- решения технологических вопросов защиты информации внутри облака;
- обеспечения юридической защищенности обрабатываемых данных;
- развития отечественных облачных платформ, имеющих необходимые сервисы безопасности.

Актуальность моделей взаимодействия

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Несмотря на то, что исторически модели «ИБ часть ИТ», «ИБ часть контроля» и «ИБ часть бизнес-процессов» появлялись последовательно, все три модели в настоящее время имеют право на существование.

Для малых и средних предприятий, не слишком отягощенных требованиями регуляторов, модель «ИБ часть ИТ» является оптимальной, поскольку не создает искусственных проблем с резервированием функций ответственных работников и не усложняет взаимодействие.

Для предприятий с объектами критической информационной инфраструктуры и низкой динамикой изменений будет эффективной модель «ИБ часть контроля».

Аутсорсинг позволяет использовать при необходимости внешние ресурсы.

Лидерам необходимо создавать новые формы взаимодействия ИБ, ИТ и бизнеса.

Кибербезопасность vs Информационная безопасность

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Кибербезопасность (cybersecurity):

1. Способность защищать и оборонять кибепространство от кибератак. [CNSSI-4009]. Примечание. В данном случае термин «оборона» (defend) обозначает вид активных боевых действий, который предполагает, в том числе, проведение контратак, т.е. понятие «кибербезопасность» включает применение ответных и превентивных компьютерных атак для осуществления ответных воздействий на информационную инфраструктуру атакующего, в том числе расположенную на территории иностранных государств. В нормативных актах Минобороны США к оборонительным операциям относится также получение несанкционированного доступа к информационным системам иностранных государств, в том числе с применением технологий бот сетей (Cyberspace Operations Concept Capability Plan 2016-2028).

2. Свойство киберпространства (киберсистемы) противостоять угрозам намеренным и/или ненамеренным, а также реагировать на них и восстанавливаться после воздействия этих угроз [Russia-U.S. Bilateral]. Примечание. В данном случае под киберпространством понимается электронная среда, в которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается.

[CNSSI-4009] Committee on National Security Systems (CNSS) Glossary. CNSSI No. 4009, April 6, 2015.

[Russia-U.S. Bilateral]. The Russia-U.S. Bilateral on Cybersecurity — Critical Terminology Foundations, Issue 2 \ Ed. by: J.B. Godwin III, A. Kulpin, K.F. Rauscher and V. Yaschenko. 2014. East West Institute and the Information Security Institute of Moscow State University (EastWest Institute и ИПИБ МГУ).

Кибербезопасность vs Информационная безопасность

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Информационная безопасность (Information security):

1. Обобщенный термин для обозначения состояния защищенности и области деятельности по обеспечению безопасности информационных ресурсов. При этом информация может быть представлена в любой форме: печатной, электронной и т. д.

2. Защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения доступности, модификации или уничтожения с целью обеспечения:

- целостности, что означает защиту информации от несанкционированной модификации или уничтожения и включает гарантирование подлинности и невозможности отречения;
- конфиденциальности, что означает предотвращение несанкционированного раскрытия и ограничения доступности, включая средства защиты приватной и конфиденциальной информации;
- доступности, что означает гарантирование своевременного и надежного доступа и использования информации [NISTIR 7298].

3. Свойство информационного пространства противостоять угрозам, реагировать на них и восстанавливаться после нанесения ущерба [Russia-U.S. Bilateral].

4. Безопасность, связанная с угрозами в информационной сфере. Примечание. Защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) организации [СТО БР ИББС-1.0-2014].

[NISTIR 7628] Guidelines for Smart Grid Cyber Security. The Smart Grid Interoperability Panel Cyber Security Working Group. September 2010.

Кибербезопасность vs Информационная безопасность

КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ
Промышленные технологии

Тематика форума с участием промышленных предприятий:

Информационная безопасность (кибербезопасность) как способность организаций противостоять угрозам в информационной сфере, которые могут быть намеренными и ненамеренным, внешними и внутренними, воздействовать на системы управления предприятием и на производственный процесс, а также на взаимодействие с потребителям, репутацию и т.д.

КИБЕРБЕЗОПАСНОСТЬ
НАШИ ДНИ
Промышленные технологии

Спасибо за внимание!

#uralcyber